Tyro Tutorial

An Indexed Accumulation of Thirteen Years of

***Cm Tyro Grams* Columns**

For

The Young at Heart

And

Cryptogram Cipher Tips For

Seasoned Solvers as well as Tyro Novices

LIONEL

2013

TABLE OF CONTENTS

Acknowledgements

I extend a most grateful thank you to all of the ACA Krewe through the years who have provided my intellect with all of the crypto knowledge it has been capable of absorbing and in lending their wisdom, counsel, tutelage, review and editing in support of the material contained within the pages of this manuscript - Special thanks to AAJHU, BECASSE, BION, FIZZY, GGMA, HONEYBEE, LEDGE, MSCREP, PHOTON, QUIPOGAM, REAL NEO and my personal mentor, RISHU.

LIONEL

Foreword

Tyro Gram Crackers for the Young at Heart

The following crypto tutorial is an updated extraction from the American Cryptogram Association's *Cryptogram* Tyro Grams column (initially titled Kiddee Korner) from 2000 to present. The column and these extractions have been inspired by one of the ACA's foremost crypto mentors and educators, Gerhard Linz (LEDGE).

The American Cryptogram Association (ACA) is a non-profit organization, founded in 1929, devoted to the cultivation of cryptologic knowledge with members all over the world. It publishes a thirty-two page bimonthly magazine, *The Cryptogram*, full of hundreds of cipher types contributed by members for members' solving pleasure. ACA cryptologist members (Krewe) mirror an image of all walks of life, representing ages from five to ninety and all trades, professions and educational levels. Nom de Plumes (Noms) bring a degree of anonymity to all members. It is fun and cryptology that counts. The Kiddee Krewe/ Young Tyros is a division of the ACA that provides a cryptology learning experience for cipher solving aspirants and has no age limitations. More information and membership details can be found at ACA's Web site www.cryptogram.org

The Kiddee Korner had its **Cryptogram (Cm)** journal inception in January of 2000, changing its name to Tyro Grams in the Cm JF edition of 2003. Its intention was to provide an opening to those interested in pursuing the solving of codes and ciphers and was written to serve the Young at Heart Tyros of all ages.

Webster defines "tyro" as one who is in "the preliminary stage or rudiments of any study or occupation." As we watched our Kiddee Krewe grow in number and skill, observe its work in solving, constructing, authoring of articles in the *Cm*, and watched it take part in all phases of ACA conventions, we realized that these young achievers were far removed from Kiddee Land. (Two finished with scores in the top ten at our Chicago Cipher Contest.)

We felt that we performed an injustice by labeling these youngsters and **"Young at Heart"** adults, eager to work at mastering the principles of cryptology as "Kiddees." We

discouraged the young and the mature to peer at what lies beyond the Kiddee label. We also discouraged the interest of youthful membership ACA recruitment.
All of these reasons prompted us to elevate our Kiddee Krewe name to **Young Tyros (**tip of the hat to QUIPOGAM and Grandson, QUAZAR for their suggestion) and Kiddee Korner column to **Tyro Grams.** Our column objective will remain the same, that of reducing cryptology principles to their simplest terms thru a most understandable format.

Appendices, cipher solution pages and an Index follow the body of this material.

LIONEL – 2013 (Lee Melair)

INTRODUCTION

Solving Rudiments

Let's talk a bit about what our fellow hobbyists tell us has helped them develop a degree of skill and proficiency in their solving endeavors. All facets of cryptology are enjoyed – solving, constructing, writing, mentoring and above all, the friendships it generates with fellow ACA Krewe.

ANCHISES relates "I never knew LEDGE, but he took this Tyro and converted him into a solver through his excellent Novice Notes. That opus must be held in the highest regard by very many people, me included, for getting them started in the ACA with a clear exposition of how ciphers work and how one can go about solving them. Even though I solve with my computer, the solving algorithms and processes described by LEDGE for pencil and paper solving are very often the best routes for the computer to take also."

We all begin as pencil and paper solvers and learn the basic fundamentals of the various cipher types. Those with abilities in computer operating and programming go on to utilize the computer for the elimination of a lot of the manual grunt work involved in paper and pencil solving. Much the same as an engineer, who builds structural edifices or lays out complex system designs and relies on the computer for his mathematical equations, the computer is a worthless solving aid unless the foundation of basic subject knowledge has been firmly imbedded in our minds. This said, our mission is simply to learn all *we* can about the makeup and idiosyncrasies of all the cipher types.

Perhaps the best learning technique of becoming proficient in any endeavor is to cultivate an extreme interest about all of its working parts. What makes a particular "clock" or subject tick? Once you have acquired the interest and curiosity to want to know more about a subject, you will find a multitude of teachers, parents, friends, and soon to become friends, eager to impart their knowledge to you.

In our hobby, members are waiting to be of help everywhere. At the mailbox, by E-mail, at conventions and mini cons, cryptography buffs are eager to be of service. We have

international (transoceanic) learning going on as we "speak." You might be surprised at what you can learn besides cryptology.

Never underestimate the value of Google to call up our ACA Web site www.cryptogram.org or to research any term or technique which raises a question in your mind

A Young Tyros library sits awaiting your beck and call with publications available, free of charge, on most any facet of cipher solving. Simply indicate your interest to LIONEL at cryptolion@aol.com

Chapter One

Caesar Cipher (The Beginning)

We are hopeful that this column is the beginning of a long and fruitful relationship with the children (whatever the relationship) of our faithful Krewe who wish to pass this fun hobby along to another generation. We also wish for this column to be useful to all of those Young at Heart aspirants interested in developing or fine tuning their solving techniques.

Let's begin this first column with a brief explanation of the use of the term NOM by our ACA membership Krewe. NOM is short for Nom de Plume (from the French language meaning, "name of the pen" or "pen name"). ACA Krewe use NOMS to address one another while retaining their anonymity. This informality allows us to interact with each other as equals uncaring of one another's position in life — doctor, lawyer or Indian Chief. Upon registration we ask you to list the first three choices of your personal NOM. This is because once a NOM has been registered with the ACA it may never be selected again.

Caesar's Cipher

One way for someone new to cryptography to become acquainted with the substitution of one letter for another (simple substitution) is through the Caesar Cipher.

Julius Caesar (100 BC to 44 BC), Roman General, statesman and historian invented this simple cipher which still bears his name. To disguise his communications, he would shift letters so many to the right or left for each message, producing a garbled looking mass of words which we call ciphertext, disguised letters or a system of visible secret writing.

```
Plaintext:  efghijklmnopqrstuvwxyzabcd
CIPHERTEXT: ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

This alphabet has been shifted four letters. Plaintext is the original message before any encipherment (disguising) has taken place. To eliminate any confusion between plaintext

and CIPHERTEXT letters, write plaintext letters in lower case letters and CIPHERTEXT letters in UPPER CASE letters.

Someone using this Caesar Cipher shift of four letters to send the message, "I will be there at four o'clock," would simply substitute the CIPHERTEXT letters beneath the plaintext alphabet letters of the original message.

```
"I will be there at four o'clock."
"E SEHH XA PDANA WP BKQN K'YHKYG."
```

Do you see how this was done?

Unravel the disguised messages below. You will perform your first decipherment (conversion of disguised text to original text). Hint: Each message below has a Caesar Shift of four letters.

Caesar Ciphers (1)

K1. YNULPKCNWLDU EO BQJ.

K2. WYW IAIXANO WNA YWHHAZ GNASA.

K3. JKIO WNA WYW YKZA JWIAO.

K4. OAJZ EJ UKQN OKHO.

Julius Caesar may have been a great soldier and conqueror, but when it comes to ciphers, he holds no better than the rank of lead-off novice in our Kiddee Korner cryptography lessons. His ciphers (disguised messages) could be solved with a simple shift of letters between the plaintext (original message) alphabet and the CIPHERTEXT (disguised message) alphabet.

In our introduction to the Caesar Cipher, we looked at cipher messages constructed on the basis of the same shift of four letters between the plaintext and CIPHERTEXT alphabets. To increase the complexity of the disguise of a Caesar Cipher and to complicate its decipherment (changing disguised text to original text), shifts of one to twenty-five letters can be used to construct the disguised message. (Why can’t we shift twenty-six letters?)

Important note: Once the amount of the letter shift has been decided, the same number of shifts must be used for each letter in the cipher. Changing the number of the letter shift from letter to letter will make it unintelligible.

Each cipher below has been constructed with a different amount of letter shifts between the plaintext and the CIPHERTEXT. You must determine the amount of the shift for each cipher problem. Remember that the letter shifts must remain the same for each message.

A Caesar Alphabet Table appears below to help you change CIPHERTEXT to plaintext. To solve a Caesar Cipher "run down the alphabet table" with one of the CIPHERTEXT words until you find an intelligible plaintext word. You will then know the amount of letter shifts used for the rest of the message.

CAESAR Alphabet Table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
19	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
22	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
23	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
24	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
25	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Ciphertext Letters ZXBPXO
Ciphertext Letter shift - 1 aycqyp
No intelligible word here
Ciphertext Letter shift - 2 bzdrzq
No intelligible word here.
Ciphertext Letter shift - 3 caesar
Looks like a word to start Cipher K1 below.

Caesar Ciphers (2)

K1. ZXBPXO ZFMEBOP XOB BXPV.

K2. UFJBUVYN NUVFY BYFJM MIFPCHA.

K3. HKKG BKN EJPAHHECEXHA SKNZ.

K4. PCEGQRCP GL RFC IGBBCC IPCUC.

Parade of Cryptologists

It did not take long for Julius Caesar's adversaries to unravel his Caesar shift foundation of secret messages and with the unraveling, began the 2000 year battle of wits, still alive and well today, between the cryptographers (writers of secret messages) and the cryptanalysts (decipherers of secret messages).

Distinctive list of renowned cryptologists

63BC-20AD Polybius, Greek Historian
6th Century St. Boniface, Anglo-Saxon Missionary
8th Century Pope Sylvester II
11thCentury Hildegard von Bingen, German Nun
1220-1292 Roger Bacon, English Monk
1404-1472 Leon Alberti, Florentine Merchant
1501-1576 Girolamo Cardano, Milanese Physician
1523-1596 Blaise de Vigenere, French Diplomat
1535-1615 Giovanni Porta, Italian Author, Scientist
1561-1626 Sir Francis Bacon, English Statesman
1743-1826 Thomas Jefferson, American President
1774-1857 Sir Francis Beaufort, English Admiral
1791-1872 Samuel Morse, American Inventor
1805-1881 Friedrich Kasiski, Prussian Military
1846-1931 Etienne Bazeries, French Cryptologist
1891-1969 William Friedman, American Cryptologist
1892-1980 Elizabeth Friedman, American Cryptologist
1899-1993 Captain Eric Nave, Aussie Codebreaker
1908-2001 Frank Rowlett, American Cryptologist
1912-2010 Frank Lewis, U.S.A. SIS & NSA agencies
1930- David Kahn, American Author, Cryptologist
1955- Simon Singh, English Author, Cryptologist

Simple Substitution Cipher

Caesar's cryptic messaging with a simple alphabet shift soon became obvious to the least experienced cipher analysts. A fresh approach was needed. The world of the simple substitution cipher was born and letters were randomly chosen to depict other letters of the alphabet. Randomly selecting a cipher letter to represent another letter (plaintext letter) revoked the ease of simply looking for the number of shifts that a letter had been moved.

Simple substitution ciphertext is limited only by the ingenuity of the constructor (cryptographer). Its foundation may lie in an everyday medium found in the home, at work, at play or on the street. A telephone dial, computer keyboard, tic tac toe template, newspaper, book, compass, or simple street address may be the basis of ciphertext.

Chapter Two

Substitution Ciphers

Caesar's cryptic messaging with a simple alphabet shift soon became obvious to the least experienced cipher analysts. A fresh approach was needed. Let's begin to look at the world of the simple substitution cipher where letters are randomly chosen to depict other letters of the alphabet. Randomly selecting a cipher letter to represent another letter (plaintext letter) revokes the ease of simply looking for the number of shifts that a letter had been moved.

Simple substitution ciphertext is limited only by the ingenuity and imagination of the constructor (cryptographer). As mentioned in Chapter One, its foundation may lie in an everyday substance found in the home, at work, at play or on the street. A picture, book, dictionary, newspaper, keyboard, or computer internet text may be the basis of ciphertext.

In our computer age of today, we use codes for many every day activities. Your zip code is a simple method of identifying your state, city and street address where you live. Bar codes on labels speed the supermarket checkout line with pricing information. A Personal Identification Number (PIN) allows us to do banking at automated tellers. Our social security number identifies who we are, where we work and reports annual earnings to the Internal Revenue Service. (Perhaps not all codes are pleasantly used.)

Finally, there are thousands of persons like us who construct and decipher codes and puzzles for the everyday enjoyment of it. It provides a relaxing escape from our busy daily activities.

When all the letters in the ciphertext (disguised message) are exactly the same as those in the plaintext (original) message, but simply rearranged, we refer to it as a transposition cipher. The letters are all the same. Only their order has been altered or changed.

When the plaintext is changed to a different letter or symbol, the cipher is called a substitution cipher. The symbols or letters have been substituted for the plaintext. Once a plaintext letter is assigned a ciphertext letter or symbol it must use the same substitution throughout the cipher. (We refer to this as a simple substitution cipher.)

We are going to have some fun in this issue with a substitution cipher with a date back to the middle ages in Europe (500 AD to 1500 AD), also popular in the American Civil War (1861 to 1865). Today it is commonly known as the Pigpen Cipher, most likely because the cipher symbols look like penned areas.

Most important in the communication of cryptography is a KEY set up by the correspondents in advance that determines the steps to be followed in the enciphering (constructing the disguised message) and deciphering (retrieving the original message) processes. The Pigpen Cipher Key might be set up in a grid as shown below.

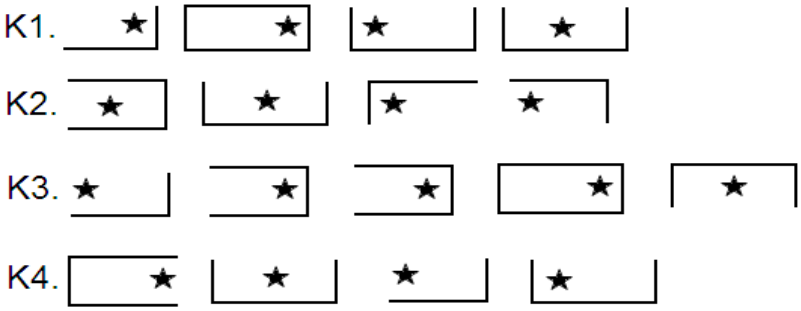
A B C	D E F	G H I
J K L	M N O	P Q R
S T U	V W X	Y Z

This shape of the grid would indicate the letter group: 

 Indicates the letter "T":

"Send" would look like this:

Pig Pen Ciphers



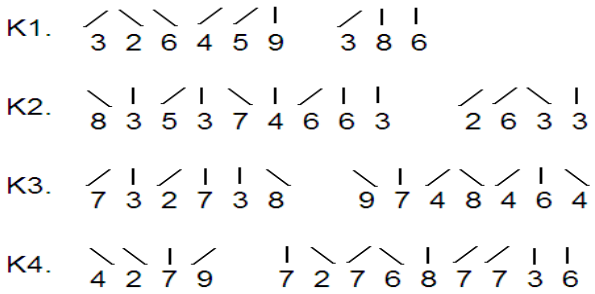
An interesting phenomenon has occurred while putting this column together for the reading and ciphering pleasure of the younger generation. There is a young at heart generation out there that has been reaping its own ciphering harvest from these basic fundamentals of cryptography principles. A group, not exactly eligible for the Kiddee Krewe, but somewhat interested in the mysterious, fascinating, and compelling force causing grown persons to eagerly await each issue of the Cm, has been prompted to find out what this cryptography fuss is all about. Welcome aboard. We will try to make the ride a pleasurable one. I invite you to make this column available to all family members.

If you have found the first two cipher types we have reviewed to be fun, you will find many more like them in the following books:

• *Secret Codebreaker Handbook*, Robert Reynard
• *Codes & Ciphers*, Christina Ashton
• *Cryptography, the Science of Secret Writing,* Laurence Smith.
• *Codes Ciphers and Secret Writing*, Martin Gardner

You will find many substitution type coding devices described in these books that are found in your own home. The ciphers below have been constructed with the help of the ordinary telephone dial. Each telephone digit can be represented with up to three letters of the alphabet. See if you can build upon the knowledge you have already gained to work on their solutions. (Hint - remember the Pig Pen Cipher.)

Telephone Ciphers



Chapter Three

Steganography

A court stenographer is a person who records proceedings in a form of shorthand (a code in itself) that permits the stenographer to keep pace with those that are speaking in the courtroom. It is mentioned here to distinguish it from a look alike term that we will be talking about today —steganography.

Steganography is another fun type of coding device that was first used by the Greeks in 500 BC and also put to great use by the Germans in World Wars I & II. It is used to conceal the very existence of a disguised message being at all present.

There are many ways steganography was performed with the everyday newspaper, book or periodical. The cipher constructor would make use of any number of devices to allow the plaintext of a book, newspaper, or periodical to carry the hidden message.

Invisible ink marks, micro dots or micro holes visible only to an individual with special reading or magnifying devices were used to conceal the existence of a hidden message. The author of the hidden message would simply mark the letters or words of the original text that he needed to convey the special message.

Another method of steganography and one that you can easily adopt is a numbering system that will point out the appropriate text letters or words to convey the concealed message. To

use this method with a friend you need only to be certain that you and the receiver are reading from the same text edition.

Let's try this methodology out with cipher S1 below. It is using a numbering sequence that relates to the letters in the words of paragraph one, line one in the Foreword of this Tutorial.

Steganography Ciphers

S1. 215 7212 32315

S2. True or false.
Steganography is used in today's courts.

S3. True or false.
Steganography is a form of coding system.

S4. True or false.
Friends in Dallas, TX and Denver, CO can use a daily fixed signal to conceal a message which appears in their own daily local newspaper.

Chapter Four

Cipher Keys (Keyboard Cipher)

Webster defines 'kid' as the informal reference to a child. I like to think of a child as an analogy to the search for knowledge and wisdom.

The child's unquenchable thirst for answers to its never ending list of questions supports the beginning of life's journey on the endless path of learning. “The kid in all of us” never loses the inquisitiveness for the world around us or the curiosity for what the future may hold.

This column is dedicated to such a spirit of learning and the interest in one another's leisure pursuits. Dare that I hint that the family that crypts together may develop a bonding in a mutually interesting form of recreation?

As we approach the threshold of classical cryptology, it will serve us well to develop a firm understanding of the device which allows us to communicate with one another in a disguised encrypted form. The key to this type of communication is appropriately called a “key.”

Most all encrypted messages are based upon a key that allows the receiver of the message to turn garbled disguised ciphertext into original plaintext form. It is these keys that we attack through time tested decipherment methods that allow us to read disguised text. When the cipher key is not provided, our work and fun as a cryptanalyst (solver) begins.

In Chapters Two and Three, we have mentioned the fact that there are many coding devices around the house. We are going to use the computer keyboard as the keying device to the cipher problems that appear in this month's column.

Seek out a computer keyboard at home or school and carefully copy the three rows of letters exactly as they appear on the keypad. Copy them in upper case letters as they are going to be our CIPHERTEXT letters.

Now write the letters of the alphabet in lower case letters beneath the computer keypad letters from “a to z.” You have created the key to decipher the problems that appear below and can use this key to convert CIPHERTEXT (keyboard letters) to your plaintext key.

Keyboard Ciphers

KB1. EGDHXZTK ATNWGQKR ATN RTCOET

KB2. EQF EKTQZT DQFN ROYYTKTFZ ATNL

KB3. IGV EQF VT YOFR ZIT HKGHTK ATN

KB4. LTT FTBZ EIQHZTK YGK ATN EGFLZKXEZOGF

Chapter Five

Keyword Alphabet

ACA Conventions are a good time to begin lifetime friendships with many people who have similar interests. They are also a wonderful opportunity to pick up a lot of information and education about cryptography. It is not coincidental that many of the Krewe solution scores have increased greatly with convention attendance.

Our ACA convention sites allow a great opportunity for ACA Krewe to plan their summer vacation setting. Conventions provide a great opportunity to get to know other members of the Young Tyros and adult members of the ACA and the cultivation of lifelong friendships.

In our last chapter, we related how most ciphers (disguised messages) are based on a key that allows both the sender and the receiver to communicate in ciphertext.

Here is a simple way to construct a substitution cipher alphabet with the use of a keyword. Pick a keyword that is easy to remember. Write the alphabet in a row of upper case letters. Write a keyword directly above it in lower case letters followed by the rest of the alphabet that does not appear in the keyword. We refer to this procedure as a Key 1 Alphabet.

```
zcipherabdfgjklmnogstuvwxy
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

You will notice that we begin our keyword over the upper case (ciphertext) letter ‘B’. If we had started our keyword above the upper case letter 'A', the lower case or plaintext letter 'e' would be substituted for by the upper case letter 'E' .

A letter may never be substituted for itself under ACA rules for simple substitution ciphers. When placing a plaintext keyword over the ciphertext alphabet, no identical letters may appear above or beneath each other. No letter may stand for itself (self-encryption).

A keyword may be started at any point over the ciphertext alphabet as long as it does not cause a letter to be substituted for itself.

It is equally important that duplicate letters in a keyword not be repeated, to avoid duplicate ciphertext letters standing for the same plaintext letter. Keeping these principles in mind, each keyword selected will produce different ciphertext.

The knowledge of this keyword between the sender and the receiver allows the disguised ciphertext to be converted to an easily read plaintext message. When this key is not provided the work of the cryptanalyst is ready to begin.

Indicate whether each keyword alphabet below is correct.

```
KW1. crazybdefghijklmnopgstuvwx
KW2. cipherabdfgjklmnogstuvwxyz
KW3. vwxyzcipherabdfgjklmnoqstu
KW4. uvwxcryptogrambdefhijklnqs
     ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Chapter Six

Aristocrat Substitution Cipher

We are ready to begin having fun with classic cryptography. Let us begin to discuss the tools and techniques that allow the cryptanalyst (that's you) to find the ciphertext message without possessing the actual key.

The classical substitution type cipher, which retains word breaks and is seen most often in your local daily newspaper, is called the Aristocrat cipher.

In real life cryptography we have some knowledge and probably a lot of ciphertext to analyze. Newspapers and magazines such as our own Cm have space restrictions which limit the amount of ciphertext they can print. In place of large amounts of text which aid solving, subject titles and tips (also known as cribs) are provided. Tips are often given in Caesar format that require determining the number of letter shifts (see Chapter One) to identify the plaintext word to be placed in the message.

Analysis of the Aristocrat cipher begins by checking the title for thoughts of words that might appear in the plaintext. If a tip appears, look for its proper spot in the cipher. Look for common short words (in, it, is, of, no, on, and, the). 'The" often starts of a sentence. One letter words most always are "a" or "I."'. (Rare exceptions are "O," "X" marks the spot.)

Letter frequency counts may lead us to the most often used letter "e". Pattern words are those words having repeat letters. We think of the common pattern word "that" in terms of 1-2-3-1, meaning the first and last letter of the word are the same.

Try these deciphering tools on the following cipher example and check your answer on our Solutions Pages at the end of this Tutorial.. Keep in mind that once a cipher text letter is used for a given plaintext letter, it must always be used for the same letter.

A-Example. Cryptography lesson. (AFPDRFPBA – Caesared tip.)

DNO KPIMDAUPQMNOP LC QXGQIC

KNOKWLZU TAP CYQXX GAPSC AP

CLZUXO XODDOP GAPSC DNQD MPAFLSO

Q UAAS OZDPI MALZD LZDA DNO

SLCUELCOS YOCCQUO.

A-1. Solvers delight. (ABIFDEQBA – Caesared tip.)

TROWFGT HGF JFOCLEUFJ XEFQ UEFZ JCTBRWFG UEF GFDFHUFJ VTF RK

UEF PRTU KGFSVFQU WRXFO CQ H BCDEFG .

A-2. What is the crib of A-1?

A-3. What is the most frequent letter in A-1?

A-4 . How many pattern words are in A-1?

Are you having fun yet? We are going to spend many columns talking about the Aristocrat cipher, the cipher that your daily newspaper holds synonymous with 'cryptogram'. Let's continue our discussion with some of the many tools that are helpful in solving Aristocrats as well as many other cipher types.

Titles and tips. Do not overlook cipher titles as good leads to plaintext words. Each plaintext word correctly placed provides valuable letters to other words in the cipher.

Caesar Cipher tips. Remember your alphabet training to convert any ciphertext tip to plaintext. Placing the tip in a message generates leads to many other words in the plaintext.

Frequency count. The first step in solving by most cryptanalysts is a simple tally of how often each ciphertext letter appears in the message. This is called a frequency count and is used to compare each ciphertext letter of appearance with that of the normal frequency of letters in the English language. Such a comparison allows us an educated guess of what a ciphertext letter may be. The "ACA and You Handbook" provides the following values:

ENGLISH LANGUAGE FREQUENCY TABLE
(Percent occurrence)

e	t	ao	nir	sh	ld	cupf	mwy	bgy
13	9	8	7	6	4	3	2	1

kqxjz - less than one percent

Senorita

Letter frequency counts are a most effective tool in cipher solving. **Senorita** is the key to frequent letter repetition. It contains most all of the frequently used letters. Align the most and least used letters with the frequencies of letters appearing in the above table. It will be a significant aid in providing a breakthrough to your solving process.

Short words - Look for these short words in a cipher: “a” and “I” (the only single letter words), an, in, is, it, on, of, the (often starts a sentence and often appears more than once in a cipher), was, why you .

Pattern words -These are words with repeating letters . Look for these common pattern words: All, off, too, see, good, poor, that, there, where, these, little, people.

Cross Checking

The phenomenon of cross checking pattern words in an Aristocrat cipher, also referred to as cross-correlation, cross-matching, cross-reduction and cross-referencing, is a valuable tool in uncovering much of an Aristocrat’s plaintext. The following examples will demonstrate its usefulness.

JF 11. A-11. The marrying kind. DYETI

A check of our pattern word list for the plaintext (pt) equivalent of ciphertext (CT) **IOSHUPZKQO** (Pattern 1234567892) found in this cipher reveals the words “admonished, centigrade, despicable, neutralize personable and persiflage” as being represented by the same pattern.

CT letters **ISOPOSH** (pattern 1234325) would reveal the words “brewery, granary, prefers, revived, synonym and utility” as plaintext pattern fits.
A simple check of the like ciphertext letters in each ciphertext word (ISOPH) will lead you to the correct pattern plaintext word for each, “persiflage and prefers” and generate more leads to the cipher’s plaintext.

See our MJ10 Tyro Grams column for a discussion of pattern word lists. The pattern word “people” would be defined as a word having a pattern of “123142.” The “1’s and 2’s” indicate the repeating letter position of the letters “p and e.”

JF 11. A-13. Isn’t that special? ANGO-KA

Pattern ciphertext word DUVWFXVW yields plaintext pattern words “**aluminum**, bungling, distrust, hastiest and sometime” as potential word solutions while the ciphertext pattern word MFUDHFZX yields the words “absorbed, **dilution**, fidelity, feathers and mahogany” as possibilities. A simple check of like letters in each ciphertext word will identify the proper fitting plaintext letters and lead to more plaintext words in the cipher.

Here is another cross check which will lead to much more plaintext recovery.

MA 11. A-14. Music. DUMPSTER

Cross-check **PNWJRBZKNZM** with pattern words, “dipsomaniac, discounting,

dismounting, miscounting and **realignment**" versus **APRZHRAWJ**, pattern words, "coatracks, convinced, **principal,** principle and traumatic" for the proper plaintext fit of each. See how many additional words of plaintext become identifiable with the letters you have distinguished.

Pattern Word List Reference

Google, Design215 **Word Pattern** Finder - Find **Words** with Similar **Patterns ...** for word lists that will reveal words by pattern numbers.

Abridged paperback list of pattern words such as included in Norma Gleason's book of *"Cryptograms and Spygrams"* provide the most often used words in the English language and is much easier to peruse than those long lists of all inclusive words in the English language that may be found on the Internet.

The non-pattern word list is a great aid in performing word cross matching. This technique is served by comparing the like letter positions in ciphertext words and finding the word fit on the non-pattern word list which will provide you with two plaintext words to assist you in the solving process.

Crib Dragging

Crib dragging is a stimulating manual exercise and great time filler for those long waits at the doctor's office or waits on significant others at shopping malls. A given crib needs to be simply placed in each ciphertext position to observe those plaintext letters that are generated as a result of each position placement.

Miscellany

Each ciphertext letter may stand for only one other plaintext letter. Each plaintext letter must be replaced by a ciphertext letter not equal to itself. (ACA simple substitution ciphers do not allow "self-encryption," (the act of allowing a letter to stand for itself.) An asterisk indicates the use of a proper noun which may, or may not, be part of the English dictionary.

Let's put these tools to use in solving the cipher and answering the questions below.

A-5. Solving tools. (CXJFIFXO)

EOP *YMUUPP *YCQBPQ LCZFAB MR S

WCCU HSJ EC ZPSQB SBU TPLCAP

VSAMZMSQ HMEO ASBJ CV EOP ZMEEZP

ECCZR EOSE SQP OPZNVFZ MB RCZGMBW

*SQMRECLQSER.

* Proper noun or name.

A-6. What plaintext letter appears most?

A-7. What plaintext letter appears least?

A-8. How does the frequency of the most and least plaintext letters in this cipher compare to their frequency in the English language?

Let's apply many of the principles of cryptanalysis which we have been discussing to a simple substitution Aristocrat Cipher that appear below.

A-9. Corn harvest. [105] (for) LIONEL

PDA YKNJ BWNIANO EJ PDA

YAJPNWH WJZ JKNPDANJ LWNPO

KB PDA *QJEPAZ *OPWPAO HKKG

BKN YKNJ OPWHGO PK XA GJAA

DECD XU PDA BKQNPD KB *FQHU.

Solving Principles

Title note: A harvester of corn may appear in the plaintext, a farmer or comedian, perhaps?

Look for the best fit position of the three letter crib, "for." It would seem unlikely to begin the cipher.

We note the ciphertext letters, **PDA**, at the start of our cipher, repeating three more times in this cipher; a good candidate for the most used three letter word in our English language

Nine ciphertext letters appear at least five times, all candidates for our **senorita** plaintext letters.

There are six, two letter ciphertext words that may fit frequently used plaintext letters "in, is, it, on, of, to, be."

Many proper nouns (*) with repeat letters appear in pattern word lists. Look for *OPWPAO.

Digraphs and Trigraphs

Let's discuss some additional principles that prove helpful in converting ciphertext (CT) to plaintext (pt). Webster defines digraph as "two letters portraying a single sound" and trigraph as "three letters depicting a single sound." These two and three letter groupings lend an aid to the solving process. Recognizing the most frequently used digraphs and trigraphs allows us to consider additional adjacent plaintext letters.

Awareness that "th" is the most frequently used digraph, that "er" and "re" the most frequently reversed digraphs and that "the, ing, and" are the most often used trigraphs is a most helpful aid to plaintext recovery.

Most Frequent Digraphs and Trigraphs

TH ER RE IN AN HE AR EN TI TE AT ON ED ND HA

THE ING AND THA ION ENT FOR TIO ERE HER ATE VER TER

Solving Lucidity

One's solving logistics, plaintext insight and ease of continuity will be helped by the use of UPPER CASE letters for ciphertext, lower case letters for plaintext, letter certainties in red.

A-10. Aristocrat. Holiday Fun. K1 (seem) LIONEL

IZDL RSD LYZDL TUC RSLIMXS RSD NIIC, TUC WRLTYXSR RSLIMXS RSD ATLUPTLC XTRD. ND WDDH RI XI DORLDHDGP WGIN, YR YW WI STLC RI NTYR. IZDL RSD LYZDL TUC RSLIPXS RSD NIIC, UIN XLTUCHIRSDL 'W BTJ Y WJP! SMLLTS EIL RSD EMU! YW RSD JMCCYUX CIUD? SMLLTS EIL RSD JMHJVYU JYD. GPCYT BSYGC

A-11. Aristocrat. Peace on Earth. K2 (161) LIONEL

*QWSXBCLNB, *WNIEHHNW, NIR *HGNIMNN, QDIT PEC DIQT N KTNS. GWTI CWTK QDLT, CWTK PSXIV VSTNC QWTTS. N WNFTI CWNC ATNQT LNK VSNQT, LNK GTOO PT GXCWXI DES DGI TLPSNQT, BWDEOR VDDRGXOO DQQEAK DES ATSBDINO BANQT.

See Appendix I – Few Pocket Tips

Chapter Seven

The Null Cipher

How do you like your sample tasting of classical cryptography so far? You say that you had no idea that there were so many variables involved? You had no idea that your parents were so smart? You ask what happened to all that fun stuff that we used to do before things got a bit more complicated.

Well, let's take a breather and get another look at some more of the fun stuff. We're going to look at another type of cipher (there are literally hundreds of different cipher types) in this chapter called the Null Cipher. . (I can see my fellow ACA members wincing as I define the Null Cipher as fun stuff. Not all of them feel that the Null is great fun.)

The Null Cipher is used by its practitioners to conceal the very existence of a cipher. The only cipher that cannot be solved is the one that no one knows exists. The plaintext is disguised by words looking every bit the same as ordinary text. But a key (there's that word again) allows the reader to extract the plaintext from the disguised text.

Some portion of the ciphertext, looking so much like plaintext, is null and void and used to conceal the real message with a subterfuge text of its own. It may be a letter, syllable word, sentence or even a paragraph. It is the cryptanalyst's job to find what part of the text is used for the concealed message.

If only the second word in each sentence of the following order is read, a quite different meaning is given than might be expected:

NO RETREAT IS ABLE. ATTACK IMMEDIATELY

Like and distaste for the null cipher runs the gamut from high praise to ridicule. It is heralded by its supporters to belong to a concealment cipher group wishing to negate the thought of a cipher, believing the only unsolvable cipher is one that no one knows exists. Protestors of this cipher relegate it to the realm of a puzzle or riddle without principal or class.

A null cipher may declare null and void any part of its ciphertext. It may choose to exclude letters, words, sentences or entire paragraphs of its concealment text. Null variables are limited only by the creative genius of the constructor.

Consider the creative genius of one World War II serviceman attempting to evade military censors and communicate his location of Tunis, the capitol of Tunisia, to his parents during the war. Prior to his departure from home, he had arranged to spell out the name of his location by changing his father's middle initial on his envelope. For the first letter he used a

fake middle initial T, on the second, U, the third, N, and so forth. However, he neglected to date the letters and when they arrived out of order; his frantic parents scoured their atlas for NUTSI.

Here are more examples of concealed messages covered by seemingly innocent text.

Null Concealment

John Jones can always be found
hard at work at his computer without
wasting time talking. Mr. Jones never
thinks twice about helping all and he
finishes jobs on time. John takes many
efforts to do the job and skips coffee
breaks . He has absolutely not a bit of
vanity despite his work and profound
knowledge in his field. John can be
classed as A-1, the type which can't be
dispensed with. I recommend John be
promoted at once. My proposal will be
cut as soon as possible.

Consider the real message if the receiver is instructed to read every other line. A null is born by sentence elimination and one without the key is totally misinformed

A Rib Tickler Concealment Cipher

A humorous bit of dialogue making the internet tour a short time ago went like this:

He: At last, I can hardly wait!
She: Do you want me to leave?
He: NO! Don’t even think about it.
She: Do you love me?
He: Of course! Always have and always will!
She: Have you ever cheated on me?
He: NO! Why are you even asking?
She: Will you kiss me?
He: Every chance I get!
She: Will you hit me?
He: Never! Are you crazy?
She: Can I trust you?
He: Yes.
She: Darling!

A contradictory sentiment is revealed when the message is read from bottom to top.

Creative Genius

In additional to what the Null Cipher has to offer as a concealment cipher is its infinite number of variable techniques, an invitation to our individual creativity.

Letters, words, syllables, lines, sentences, nouns, verbs, adjectives, adverbs, vowels, consonants, letter shapes, punctuation marks and counting patterns are only a few of the variables that can be used in the Null construction. The number of variables is limited only by our creativity.

All of these variables cast the Null in a non-user friendly computer analytical mode, allowing the cryptanalyst to open up that vast warehouse of personal ingenuity each and every time that a Null construction presents itself.

Null Construction

There is an infinite amount of ways to construct a null. Here are just a few ways a null's ciphertext can be keyed to disguise its plaintext:

- Every other word
- Every other letter
- First letter of every word
- Last letter of each word
- 2nd, 3rd 4th etc. letter each word
  QUINCE – ND 1994 Cm: Having problems with a Null? Making a vertical listing of the ciphertext words on squared paper helps immensely. Makes threading through" much easier, and you can keep track of the numbers (possible patterns) down the side. Actually, this is also the way to construct: write the letters of the plaintext message in a list on squared paper, then surround the desired letters with others to make words, adjusting those words as necessary to create and maintain a pattern.
- Every 2nd 3 4, etc. letter of complete ciphertext. (Periodic Null described at the end of this chapter.
- Letter following each vowel

Each null below has been constructed using one of the above methods. See if you can determine the real plaintext message from its ciphertext.

Null Ciphers

N-1. Patio furniture may stain ornately sculptured tiled mall.

N-2. Leave early route, hue truly entitles rd.

N-3. Feds see pirate bunch go blow safe via borings by deli layout. FBI apprehends.

N-4. Aware, I tie a fare in teen ad.

We have related that the null cipher is one in which only some portion of the text is read as part of the secret message. The bulk of the text is null and void and is used to conceal the real message with a subterfuge text of its own. It is the cryptanalyst's job to find what part of the text is used for the concealed message. One method that cryptanalysts use to make such an examination of the letters that make up the actual message is to construct a vertical listing of all ciphertext words to see if a message can be read in columnar order. Null messages, below, seemingly professing sadness of Holiday commercialism and one describing a winter scene will succumb to this technique.

N-5. Holiday Null. 'Tis the season. LIONEL

Once upon a time there was a glorious holiday environment present within schoolhouses amid most lands, trusting valued beliefs. Lucid thinking repeals behavior steeped in derision. Dramatic confirmation today is a most overwhelming consensual endorsement of original catechists, in avid binge of gift proliferation for much Christmas viewing of tidings amid nations.

N-6. Null. Winter Scene. LIONEL

DAYDREAMING OF ESCAPING TO AWESOME PATH OF A LAVISHLY

BLANKETED VIRGIN MANTLE OF LIGHT IVORY AGLOW. NATURES

BRIGHT LIGHT LUSTERS NIGHT. CINEMATIC PRISM OPENS HALOGENIC GLOW.

LIONEL – MA 1995 Cm: QUINCE's Notes on the Null offered sage advice on the making of a vertical listing of the Ciphertext words to thread through the chaff and extract the wheat from the linguistic prose of the null. A reverse vertical listing of the ciphertext words in a null would lead to the decipherment of nulls such as APEX DX's challenging Confucius quotation in The ND94 Cm. APEX DX's "antepenult" encipherment is easily read, as a reverse vertical listing of the Ciphertext reveals the cipher position to be the third from the last letter of each word.

Our JA 2008 Cm presented a Null that did not succumb to QUINCE's "Notes on the Null described above:

E-5. Self-violating grammar rule #1. (…ten…) THE RAT

RULE: DO NOT USE NO WORDS IF THEY WEREN'T SO HARROWING, IF A

GRAMMAR EXPERT SAYS NO, THEN IT PROBLY SHOULD BE ABANDONED.

YOU'D THINK A REAL LEARNED LEXICON MAY BE OKAY ... IT'S NOT.

When QUINCE's approach yields no logical plaintext, examine the crib letter spacing in the overall ciphertext message.

The JA08, E-5 Null crib (…ten…) reflects only one repetitive spacing of crib letters, "7," in its ciphertext, between ciphertext words, **T**HINK A R**E**AL LEAR**N**ED, which allows it to be examined as a Period Seven Null. Follow the horizontal posting of the ciphertext over seven vertical columns.

Period Seven Null

1	2	3	4	5	6	7
R	U	L	E	D	O	**N**
O	T	U	S	E	N	**O**
W	O	R	D	S	I	**F**
T	H	E	Y	W	E	**R**
E	N	T	S	O	H	**A**
R	R	O	W	I	N	**G**
I	F	A	G	R	A	**M**
M	A	R	E	X	P	**E**
R	T	S	A	Y	S	**N**
O	T	H	E	N	I	**T**
P	R	O	B	L	Y	**S**
H	O	U	L	D	B	**E**
A	B	A	N	D	O	**N**
E	D	Y	O	U	D	**T**
H	I	N	K	A	R	**E**
A	L	L	E	A	R	**N**
E	D	L	E	X	I	**C**
O	N	M	A	Y	B	**E**
O	K	A	Y	I	T	**S**
N	O	T.				

Column seven is the charm. A Period Seven Null. Who would have ever thought it?

A comprehensive list of null variables appears in Appendix V.

Chapter Eight

Construction Principles

Let's get back to classic cryptography after all of that fun we had in our last chapter with the null. We are going to focus our attention on the cipher construction process in this issue. It is the process of converting plaintext message text into disguised ciphertext. You will find the construction process to be one of the best ways of appreciating and learning the deciphering technique.

Learning construction principles allows one to become familiar with the details of a cipher type. In fact, it is the reason that there are so very few ciphers that have been left unsolved, for all of the principles that have been used to put a piece of ciphertext together can be used to unscramble and decipher the very same message.

Continuing to work with the Aristocrat cipher, let's take a look at how these ciphers are constructed by following our ACA guidelines for *The Cryptogram* (Cm) cipher publication. Where an ACA fundamental differs with real world of cryptography, we will indicate the difference.

Construction Principles

Taken from *The ACA and You Handbook*.

1. Aristocrat ciphers are simple substitution ciphers which maintain their word divisions.

2. Each ciphertext letter may stand for only one other plaintext letter.

3. Each plaintext letter must be replaced by a ciphertext letter not equal to itself.
   (This differs from some cryptography systems which allow self-encryption (allowing a letter to stand for itself.)

4 .An asterisk (*) is indicated to show the use of proper nouns which may, or may not, be part of the English dictionary (limited to 3).

5. Aristocrats intended for Cm publication should be from 75 to 100 letters in length.

6. A double hyphen (=) is used to indicate a true word hyphenation to distinguish it from a word split at the end of a line.

7. Because of space limitations in the Cm compared to the material that would be available in the real world, cipher titles and tips are used to accompany the cipher.

8. Cipher tips, also known as cribs may be in plaintext form or in an encrypted Caesar shift format.

9. No more than four letters may be used only a single time.

10. At least 18 different letters should be used in each cipher.

11. Keyword alphabets are most useful in the encrypting of plaintext to ciphertext. (See Chapter Five.

Construction Quiz

True or False:

C-1. The construction and decipherment process are totally unrelated.

C-2. Ciphertext letters may represent more than one plaintext letter in the same cipher.

C-3. ACA Aristocrat construction standards allow self-encryption.

C-4. Tips and cribs are synonymous.

We will continue our discussion of the construction of a cipher as an aid to decipherment with some discussion of keywords and the keyword alphabet as a tool in the building and deciphering of a disguised message.

In Chapter Five, we introduced you to the K1 keyword type (*ACA and You* Handbook, P. 26) where the plaintext alphabet has the key and the ciphertext alphabet is normal. In this chapter we will make you aware of another keyword type.

Keywords are used in many different cipher types. Their original and still useful purpose is to promote the ease of communication in ciphertext. Easily remembered keywords allow the ease of changing ciphertext to plaintext. The exchange of information between sender and receiver is rapidly accomplished as both are able to work with a common keyword.

Keywords transform our common everyday alphabet to a ciphertext alphabet that permits the construction of ciphertext with much more ease. One needs to only follow the keyword alphabet to avoid the repeat use of the same letter. An example will make its usage clear.

K2 Keyword Type

In the K2 keyword alphabet type, the plaintext alphabet is normal and the ciphertext alphabet has the key. The purpose, once again, is to allow an ease of construction of ciphertext as well as an ease of interpretation of the disguised message.

Continue to think of plaintext always appearing in lower case letters and CIPHERTEXT in UPPERCASE LETTERS to avoid confusion when working with two sets of alphabets.

K2 Alphabet Construction

```
pt abcdefghijklmnopqrstuvwxyz
CT XYZCIPHERABDFGJKLMNOQSTUVW
```

K2 Alphabet Construction Principles

1. Plaintext alphabet is normal

2. CIPHERTEXT alphabet has the key

3. Each alphabet must have 26 letters with no repeated letters

4. No CIPHERTEXT letter may stand for more than one plaintext letter

5. No CIPHERTEXT letter may stand for the same plaintext letter (self-encryption)

A keyword may be started at any point under the plaintext alphabet as long as we avoid any CIPHERTEXT letter falling under the same plaintext letter. For this reason the keyword CIPHER in the above alphabet cannot begin under plaintext letter plaintext letter “c.”

The above K2 alphabet construction generates the CIPHERTEXT appearing beneath the plaintext message shown below:

```
Pt: this cryptography is a lot of fun.
CT: OERN ZMVKOJHMXKEV RN X DJO JP PQG.
```

Keyword Alphabet Questions

KW-1. Can the CIPHERTEXT alphabet construction above begin its keyword under plaintext letter” a”?

KW-2. Which alphabet sequence is normal in the K2 keyword alphabet type?

KW-3. How many keyword types are described on page 26 of *ACA and You* Handbook?

Chapter Nine

The Keyword Alphabet as a Solving Tool

It is not coincidental that many of the ACA top constructors (those are the devious Krewe members who send in diabolical ciphers to the Cm) are also among the ACA's top solvers.

Cipher construction is one of the best ways of learning deciphering skills. Learning construction principles breeds familiarity with the makeup of cipher types and means to their solution.

In Chapter Eight, we spoke of using a Keyword Alphabet as a tool for the construction of a cipher. This chapter we'll show how that very same Keyword Alphabet tool can be so helpful in the solving process. Take a look at a random ciphertext to plaintext letter simple substitution cipher that uses every letter of the English alphabet (pangram):

```
BXJ CQLWZ NAGSV PGD OQUEF GHJA T ITRK YGM
The quick brown fox jumps over a lazy dog.

Plaintext -  rtqxpsovleyigbjfuzwamnchdk
CIPHERTEXT - ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

In her work, *Cryptogram, A Pleasant Diversion,* Jude Patterson, (JUDE) describes the random assignment of substitution letters as "alphabet soup." It serves little useful purpose between the author of a ciphered message (cryptographer) and the receiver. Keep in mind that the original purpose of the cryptogram or disguised message is to send a secret message. If a message is constructed with a random alphabet, it becomes much more difficult for the recipient to read the message.

Keyword Alphabet Uses

The keyword alphabet has two distinct purposes:

1) Ease of cipher construction – Keyword alphabets are easily followed and repetition of the use of the same ciphertext letter for more than one plaintext letter is more easily avoided.

2) Ease of message interpretation – A disguised message is easily read when the reader has the keyword used to construct the message.

Let's discuss two of the keyword alphabets used in simple substitution ciphers. Description of these can be found in *The ACA and You Handbook, P26*.

K1 Keyword Alphabet Keyword, "cipher."

In the K1 keyword alphabet, the plaintext alphabet contains the key. The ciphertext alphabet is normal.

```
Plaintext –  abdfg**cipher**jklmnoqstuvwxyz
CIPHERTEXT – DEFGHIJKLMNOPQRSTUVWXYZABC
```

- Plaintext alphabet contains the key.
- Ciphertext alphabet is normal.
- Each alphabet must contain 26 letters.
- Duplicate letters in the keyword are excluded.
- No ciphertext letter may represent more than one plaintext letter.
- No ciphertext letter may represent the same plaintext letter (no self-encryption).

We begin the ciphertext alphabet above with the letter "D" because starting the alphabet with either A, B or C will result in a self-encrypted letter. (Test it.)

K2 Keyword Alphabet Keyword, "HAPPYDAYS."

```
Plaintext –  abcdefghijklmnopqrstuvwxyz
CIPHERTEXT – HAPYDSBCEFGIJKLMNOQRTUVWXZ
```

- Ciphertext alphabet contains the key.
- Plaintext alphabet is normal.
- Each alphabet must contain 26 letters.
- Duplicate letters in the keyword are excluded.
- No ciphertext letter may represent more than one plaintext letter.
- No ciphertext letter may represent the same plaintext letter (no self-encryption).

The keyword(s), HAPPYDAYS, appears as HAPYDS in the ciphertext alphabet with its duplicate letters suppressed. We may begin the keyword(s) at any letter under the plaintext as long as we are careful not to have a letter represent itself.

Key word alphabets are the tools used by the senders and receivers of secret messages for ease of reading a disguised message. An agreed upon keyword eliminates the need for any cryptanalysis. In a future column, we will examine how keyword alphabets can also aid the solving process for the non-possessor of the keyword (cryptanalyst).

K2 Alphabet Construction

Let's use the same keyword alphabet as Chapter Eight with the keyword, "CIPHER."

```
Plaintext –  abcdefghijklmnopqrstuvwxyz
CIPHERTEXT – XYZCIPHERABDFGJKLMNOQSTUVW
```

KW-1. Aristocrat. It's easy. K2 (32) (SNEPA) LIONEL
RO RN IXNV OJ TMROI XGC NIGC CRNHQRNIC FINNXHIN.

Apply the principles that you have learned to convert the Caesar crib (SNEPA) into plaintext and begin designing a K2 Keyword Alphabet.

Look at what happens when we post the CIPHERTEXT letters under the plaintext letters (write) in the K2 Alphabet:

```
abcdefghijklmnopqrstuvwxyz
    I   R        M O  T
```

Our Caesar shift has provided us with CIPHERTEXT letters **TMROI** equaling the plaintext letters "**write."** The spacing of TMROI in the CIPHERTEXT alphabet tells us that N must equal s and that two of the CIPHERTEXT letters PQS must fall between CIPHERTEXT letters O and T. (R is on the left hand side of the alphabet slide and we know it to be in the keyword.)

We can also make very good educated guesses on the plaintext letters represented by CIPHERTEXT letters, UVWXYZ, because of their location in the alphabet to CIPHERTEXT letter T.

This is an example of how the Keyword Alphabet can be helpful in generating additional plaintext letters. It is an invaluable tool to the deciphering process. It is a good habit to post the Keyword Alphabet simultaneously to the solving of the cipher to gain maximum insight to more plaintext.

Continue the process through to completion for the KW Ciphers below.

Keyword Alphabet Quiz

KW-1. Generate K-1 Aristocrat plaintext.

KW-2. Identify Keyword Alphabet used.

KW-3. The Caesar shift used was equal to?

KW-4. The keyword Alphabet will be automatically complete after solving the cipher.
True or false?

Keyword Alphabet Review

```
1) abcdefghijklmnopqrstuvwxyz
   CIPHER
    CIPHER
          CIPHER
               CIPHER
```

```
2) abcdefghijklmnopqrstuvwxyz
           PETUNIA

3) abcdefghijklmnopqrstuvwxyz
   JMNOPQRSTVWXZL CK ABDEFGHI
```

Keyword Alphabet Review Quiz

KW-5. What is the correct placement of the keyword CIPHER above?
KW-6. Complete the 2nd keyword alphabet.
KW-7. What is the keyword in the 3rd keyword alphabet?
KW-8. True or False - All of the below statements are true.

a) Keywords are used in many different cipher types.
b) Keywords provide ease of communication between the sender and receiver.
c) Self-encryption allows a letter to be substituted for itself.
d) ACA practices do not allow for self-encryption.
e) The cryptanalyst's work begins in the absence of a keyword.

Chapter Ten

Patristocrat Cipher

The 2000 year old battle between encipherers and decipherers of secret messages continued to be a battle of wits. As one cipher type became solvable, another was introduced to take its place. Such is the case of the Aristocrat Cipher that we have examined over the past few chapters. As the solving techniques we have been discussing weakened one cipher's cryptic value, another cipher came upon the scene eliminating word divisions. It is termed the Patristocrat Cipher.

A Patristocrat cipher is nothing more than an Aristocrat cipher with the word divisions or spaces between words removed. You will find them in the Cm in groups of five letter ciphertext constructions. Most of the principles that we have been discussing for the Aristocrat cipher in past chapters also apply to the Patristocrat cipher. Keep these fundamentals handy for both sets of cipher types. A summary appears in Appendix II.
.
The neat thing about working with the Patristocrat cipher is the fact that a crib will usually be provided. The crib will always appear as a Caesar Cipher and be in parenthesis. A review of Chapter One will remind you how to convert a Caesar cipher to plaintext.

Our benevolent Cm Patristocrat editor always uses a Caesar shift of six with the Patristocrat constructions. Count forward in the alphabet six letters, and you will arrive at the plaintext equivalent of the ciphertext.

Let's take a look at the additional information that is provided in a Cm MJ 2002, P-1. Patristocrat, "Hidden writing" is the title of the cipher. The K2 indicates the keyword alphabet type. (91/19) indicates that the cipher is 91 letters long and contains 19 different letters of the alphabet. The second line indicates the number of times that each ciphertext letter appears in the text. (See frequency count analysis in Chapter Six.) In the absence of this information accompanying the construction it would be worthwhile to develop such information ourselves.

MJ 2002 P-1. Hidden writing. K2 (91/19) (XYNYWNCHA) ANGO-KA
12L 10I 8ES 6CJ 5NOQZ 4R 3KWY 2BGH 1PX

```
RILNE  ZCNYE  OQSJI   LJQZS  PGLRQ  EHLEK  EOILK

ICIQL  JCXOG   ILYEN   LLROL  JSEWW  BSZKL  ILJIS
                                      de  tecti
ZNJCO  BYSNQ  IHSCW  EISCZ R.
ng
```

We are now ready to make an entry into this Patristocrat cipher. Our knowledge about solving the Caesar Cipher allows us to convert the Caesar crib XYNYWNCHA to plaintext "detecting." Our next step is the determination of the proper crib placement.

"Detecting" is a pattern word (Chapter Six) with a pattern of 1-2-3-2-4-3-5-6-7. This means the second and third letters will repeat. Now look for ciphertext letters in our P-1 cipher with the same pattern.

We find this pattern only at letter positions 64 through 72 in the cipher text. Inserting the crib here will allow the recovery of much more plaintext with the known letters. Plaintext letters "h", "o" and "s" now become visible and the plaintext begins to unravel. Use of K2 alphabet recovery procedures assist in the final demise of the cipher.

Patristocrat Quiz

P-1 Define the purpose of the Patristocrat cipher's second line.

P-2. What number of letter shifts was used in the crib of this P-1 cipher?

P-3. The word "adapted" has a pattern. True or false?

P-4. What is the first plaintext (pt) word of the P-1 cipher?

Let’s continue to explore how a Patristocrat crib may be used as an entry into the cipher's solution. In our example above we were fortunate to have only one place in the cipher where the crib would fit and the entry was relatively simple. What do we do when there is more than one place in the cipher construction in which the crib can be placed?

We talked about how the K2 keyword alphabet can be used to aid the solving process. This same tool can be useful in finding the right crib placement in Patristocrat ciphers where multiple locations exist. Let's look a Cm JF 2002, P-2 cipher below.

JF 2002 P-2. Just a coward. K2 (93/20) (YUMCYL) G4EGG
12U 9Q 8O 7MX 6ELZ 5PY 4S 3HKW 2BFR lAJV

SQOQO KMOUU JAPQZ OEMLU HXKZQ LQRPU EMSMO

EYMPL KQOWU YLFSX UQBZU YHXUO EXUME XUYVU

PPMHZ BLFSX RZWWU YEXQO ZQL.

The Caesar cipher YUMCYL yields plaintext word "easier" with its six letter shift. We find that this pattern word (1-2-3-4-1-5) can fit into one of four places under ciphertext letters with the same pattern: MDEYMP, UQBZUY, UYHXUO and UMEXUY. Now what in the world is a cryptanalyst to do with such a revolting development?

K2 Keyword Alphabet Analysis

Our handy K2 Keyword Alphabet tool comes to the rescue. Let's set the K2 alphabet up with the plaintext letters across the top and list the possible ciphertext placement letters beneath the crib plaintext letters "easier.”

```
       abcdefghijklmnopgrstuvwxyz
MOEYMP O   M   Y         PE
UQBZUY Q   U   Z         YB
UYHXUO Y   U   X         OH
UMEXUY M   U   X         YE
```

What does our cryptanalytic eye detect? We look for an alphabetical sequence in our ciphertext keyword alphabet and find it only in the UQBZUY placement. The three spaces between ciphertext letters Q and U allow for a nice alphabetical ciphertext letter fit of R, S and T . The three spaces between ciphertext letters U and Z allow the placement of ciphertext letters V, W and X. What happened to the letter Y? We see it sitting over to the right-hand side next to the letter B. This is an indication that the letter Y is the last letter of our keyword and the letter B the beginning of the ciphertext alphabet.

We see no such alphabetical sequencing possibilities in our other three crib placement location alternatives so we may now confidently place the crib under ciphertext letters UQBZUY. And just look at what all your good seed has sown. You have now identified 44 of the 93 ciphertext letters in the construction. Take the time to pencil in the recovered plaintext. This will allow you to make educated decisions on more plaintext and further your K2 alphabet recovery process. Chalk up another solution to your solution storekeeping.

When the given crib is not a pattern word, crib dragging can be a stimulating manual exercise. The given crib needs to be placed in each ciphertext letter position to observe those plaintext letters that are generated as a result of each position placement. Patience is surely a virtue and becomes its own reward in doctor's offices as well as shopping malls.

Patristocrat Quiz

P-5. True or False. Cribs with more than one possible placement location cannot be solved.
P-6. True or False. The position of letter Y in crib location UYHXUO makes this location unlikely.
P-7. Ciphertext RZWWUY equals what plaintext word with this K2 alphabet recovery?

P-8. Ciphertext E equals what plaintext letter in this cipher?

Let's take a look at another tool we have at our disposal in the Patristocrat solving process. Pay close attention to the ciphertext frequency counts on the second line of the construction. High frequencies are often indicators of popular plaintext vowels and consonants (senorita). This is particularly true when the constructor's main interest is to disguise words with high frequency letters rather than to avoid their usage entirely. When letter frequencies are not given with the construction, make the process of determining the ciphertext letter frequencies one of your first efforts in attempting to discern potential vowels in the cipher.

As we continue to develop the skill of placing the pattern crib in the cipher we quite naturally begin to question the placement of the non-pattern crib. Let's take a look at this process in a Patristocrat cipher from the JF 2002 Cm.

JF 2002 P-7. 100% fiction. K2 (97/20) (UVION) L. TWIN
9GP 8Z 7FRU 6O 5DKLNQY 4W 3X 2MV 1HIJ

WGXGZ ZZZYQ PKDNL DMQPR KWGVK ZJRUO RKGUF

ORLNY OFXGF OWNZY LZVNY PRFWP DNPQX ZULFD

GUUUU GDGFP QGHPR OQPKO MIPRY LF

The Caesar crib UVION translates into plaintext "about." Notice the fairly uniform distribution of the high frequency ciphertext letters above. This will make the placement of high frequency plaintext letters into the construction a very difficult task. A successful method of crib placement analysis is to match low frequency plaintext letters to like low frequency ciphertext letters. This cipher's crib contains the letter "b" which occurs in the English language approximately 1 percent of the time. We will attempt to match it to H, I and J, ciphertext letters appearing 1 percent of the time in this cipher.

Hypothesis Test
Let's see how ciphertext letter groups with H, I and J as the second letter (GHPRO, MIPRY and ZJRUO) withstand the test of:

1) Letter pattern match
2) No letter self-encrypted
3) Letter frequency match
4) K2 keyword alphabet sequence

Place the ciphertext letters, GHPRO, MIPRY and ZJRUO under the plaintext letters, "about" in the K2 alphabet:

```
   ab cdefghijklmnopqrstuvwxyz
1) G H            P    OR            (GHPRO)
2) M I            P    YR            (MIPRY)
3) Z J            R    OU            (ZJRUO)
```

Test Results

Ciphertext ZJRUO can be ruled out because ciphertext "U" cannot stand for plaintext "u." (Self-encryption).

Ciphertext groups GHPRO and MIPRY meet the non-pattern letter match of the crib word, “about,” have no letters self-encrypted and have letter frequency percentages closely related to those in the English language.

This leaves us with the K2 keyword alphabet flow as the final choice determinant between the remaining cipher groups. GHPRO on line one reflects a desirable alphabet sequence on the left and right hand side of the alphabet line. MIPRY on line two gives no indication of a desirable alphabet sequence. Though it may be possible for an alphabet sequence to appear between plaintext alphabet letters "c" and "n" the lack of this probability rules this place out.

The ciphertext group of GHPRO accounts for 34 percent of the cipher. It is time to pencil in the known plaintext.

Patristocrat Quiz

True or false:
P- 9. Patristocrat frequency counts are useless.
P-10. Non pattern cribs cannot be placed.
P-11. There are four tests in the placement of non-pattern cribs.
P-12. "Senorita" is an acronym for high frequency letter occurrences.

We will close our discussion of the Patristocrat cipher with a few brief notes. Remember that the constructor's main interest on the first page of the Patristocrat column is to disguise letters with high frequency usage. The absence of word divisions in this cipher enables the constructor to accomplish this. Be sure to use the frequency counts that are provided with the construction to uncover the high frequency plaintext letters (senorita). If the frequency counts are not provided, make them your first order of business.

Page two of the ACA Cm Patristocrat column is another story. Here, the diabolical constructor is disguising plaintext that most often never aligns itself with general properties of the English language. Searching for repetitive ciphertext letters that may represent high frequency digraphs or trigraphs (er, re, the, ing) will be helpful here. Also, be aware of the value of titles for possible plaintext words and Google searches that may relate potential wording value.

Always use the keyword alphabet as a simultaneous solving tool (Chapter Nine) to the plaintext recovery process. This will allow the decipherment of many ciphertext letters alphabetically sequenced around the keyword.

Here are two Patristocrats to solve from scratch. Beware of the letter “Q” in P-13 and alliteration in P-14.

P-13. Q Power. K2. (97/18) (KOCM) LIONEL

BGMCC TAERN TBGMZ DFBGZ DFBGM ZABGM CCKBG ZPUTD EBGTE

FBGZF TBGZH TCZDW BGZJR FZPBG RCGNB GZFBG ZCUKB GTEFZ

RDDMZ CT.

P-14. Alliteration. K2 (98/19) (UFQUSM) LIONEL

QCCQC CRFXB QFRKO WXDRZ ODQBX QCLQN DQUCX QVFDK YQVFR

KOQUC XQBFQ CDKQI ROFKQ VGFXQ WQZXD QOWQF FXOFR JXQEE

CRVQF RKO.

Chapter Eleven

Baconian Cipher

Lord Francis Bacon, sixteenth century English philosopher believed that the only true secret system of encipherment was one that concealed the very existence of a secret; one where no one ever knew a cipher existed. Lord Bacon developed a cipher, easily imitated with many subtle variations. Ciphertext (CT) is made to appear as plaintext (pt). Two distinct features hold the key to plaintext conversion.

Sixteenth Century, elite, active English political statesman, he used slightly different font types in the printing of written correspondence to conceal communication he wrote to his peers for exclusive interpretation by a selected few. Readable text use to conceal the fact that there was a concealment process present was a tandem step code device, with one step a text so obvious, no one would be ever looking for the second step.

The system's fundamental principle to compose an alphabet thru combinations that two unique symbols provide was in use long ahead of Bacon's time by the ancient Greeks, whose armies' use of fire torches swung to the opposite directions signified signs into two varying "fonts". The Indians smoke signal communications from mountain tops across the North American Plains also is an example of communication transmission thru symbolic variations.

Lord Bacon developed a Biliteral Alphabet which assigned "a's" and" b's" to represent letters of the alphabet. Each group of five "a's and b's" was assigned to a letter of the alphabet. The Baconian Biliteral Alphabet follows.

Baconian Biliteral Alphabet

A=aaaaa	**E**=aabaa	**IJ**=abaaa	**N**=abbaa	**R**=baaaa	**W**=babaa
B=aaaab	**F**=aabab	**K**=abaab	**O**=abbab	**S**=baaab	**X**=babab
C=aaaba	**G**=aabba	**L**=ababa	**P**=abbba	**T**=baaba	**Y**=babba
D=aaabb	**H**=aabbb	**M**=ababb	**Q**=abbbb	**UV**=baabb	**Z**=babbb

NOTE: THERE IS NO "bb" START IN THE BI-LITERAL ALPHABET

"Bacon" in Baconian Alphabet becomes:

```
aaaab aaaaa aaaba abbab abbaa
  B     A     C     O     N
```

The “a” and “b” units are concealed by assigning ciphertext letters to each equivalent. Once a ciphertext letter has been assigned an “a” or “b” it must always be assigned to that same equivalent.

Let’s work our way through a Baconian Cipher by dragging a crib through its ciphertext. The crib in the following construction has three letters (but). five Baconian biliteral letters are assigned to each plaintext letter. We drag the crib through the ciphertext by comparing each ciphertext letter’s Baconian biliteral letter to the crib’s biliteral letters. A crib cannot fit the construction ciphertext unless all of its biliteral letters are in agreement with the ciphertext’s biliteral letters. See the crib placement conflict process below.

JA 2002 Cm. E-7. Baconian. Enduring benefit. (but) APEX DX

QUOTA SLANT GAVEL ICING GROAT TWINS KNOLL KNAVE

COMET GNOME EIDER CREAM YEAST JOKER ZONED VOCAL

ANKLE DOUBT CLOCK POWER TOTAL ERROR NIZAM NIGHT

YAWNS SPICE OGIVE NOISY XENON FEWER.

ZONED VOCAL ANKLE – These are the only ciphertext letters not generating a conflict with the Baconian letters for the crib “but.” This signals the correct ciphertext placement for the crib. See the worksheet on the following page..

The ciphertext is examined in three word segments to see what letters will permit the placement of the Baconian letters for the crib word “but.”

QUOTA SLANT GAVEL will not permit the placement of ciphertext “but” because the “T” in QUOTA would be a Baconian letter “b” while the “T” in SLANT would be a Baconian letter “a.”

The crib is dragged through the ciphertext until no conflict appears.

*Ciphertext TWINS KNOLL KNAVE seems to present no conflict between its letters but such a placement would result in ciphertext SLANT being represented by Baconian letters bbaab – Recall our note above that there are no “bb” beginnings in the Baconian alphabet.

Ciphertext ZONED VOCAL ANKLE reflects no ciphertext letters in conflict with Baconian equivalents representation – Both “O’s” = a, “N’s” = a, “E’s” = a, “A’s” = b and “L’s” =b. This is an indication of the possible placement of the crib.

CRIB PLACEMENT CONFLICT PROCESS

a a a a b	b a a b b	b a a b a	Conflict
b	u	t	
Q U O T A	S L A N T	G A V E L	T
S L A N T	G A V E L	I C I N G	L
G A V E L	I C I N G	G R O A T	G
I C I N G	G R O A T	T W I N S	N
G R O A T	T W I N S	K N O L L	N
T W I N S	K N O L L	K N A V E	SLANT*
K N O L L	K N A V E	C O M E T	K
K N A V E	C O M E T	G N O M E	E
C O M E T	G N O M E	E I D E R	M
G N O M E	E I D E R	C R E A M	E
E I D E R	C R E A M	Y E A S T	R
C R E A M	Y E A S T	J O K E R	E
Y E A S T	J O K E R	Z O N E D	E
J O K E R	Z O N E D	V O C A L	E
Z O N E D	V O C A L	A N K L E	NONE
a a a a b	b a a b b	b a a b a	

BI-LITERAL ALPHABET KEY

Post the Baconian equivalents above to a ciphertext alphabet.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b		a	b	a		a			a	b		a	a				a		b			a	a		

Post the identified Baconian equivalents (BE) to the ciphertext letters. Indicate plaintext letters where sufficient BE letters appear (5).

QUOTA	SLANT	GAVEL	ICING	GROAT	TWINS	KNOLL	KNAVE
ab	abba	abbab	a aa	a ab	aa	aaabb	aabba
		O				D	G

COMET	GNOME	EIDER	CREAM	YEAST	JOKER	ZONED	VOCAL
aa a	aaa a	a ba	a ab	aaba	aaa	aaaab	baabb
						B	U

ANKLE	DOUBT	CLOCK	POWER	TOTAL	ERROR	NIZAM	NIGHT
baaba	ba	abaaa	a a	a bb a	a	a ab	a a
T		I					

YAWNS	SPICE	OGIVE	NOISY	XENON	FEWER.
ab aa	a aa	aa ba	aa aa	aaaa	a a

EDUCATED SUPPOSITIONS

I = b since SLANT must = N or O
T=a, anticipate N for “now”
Q=a, U=b, anticipate K for “know”
R=b, anticipate “L” for “Knowledge”
W=a, anticipate “E” for “knowledge”
M=b, to complete “E” for “knowledge”
J=b, to complete “S” for “comes”

BI-LITERAL ALPHABET KEY

(Numbered suppositions in black.)

```
                    1 7       6           3 4    2 3     5
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
b   a b a   a   bb a b b a a   a b a a b b a   aa

33 2       2         1 1      4  2  251
QUOTA  SLANT  GAVEL  ICING  GROAT  TWINS KNOLL KNAVE
ababb  abbaa  abbab  babaa  ababa  aabaa aaabb aabba
  K      N      O      W      L      E     D     G
  6 2      6     1  4  4  6      2 7   4
COMET  GNOME  EIDER CREAM YEAST JOKER ZONED VOCAL
aabaa  aaaba  abbab ababb aabaa baaab aaaab baaab
  E      C      O     M     E     S     B     U
         3 2          5 4 2 2    44 4  1  6  1  2
ANKLE  DOUBT  CLOCK POWER TOTAL ERROR NIZAM NIGHT
baaba  bab a  abaaa  aaab aaabb abbab ababb aba a
  T             I           D     O     M
  5       1     1       1             5 4
YAWNS  SPICE  OGIVE  NOISY  XENON  FEWER.
abaaa  a baa  aabba  aabaa   aaaa   aaab
  I             G      E
```

Although not present in the above construction, examination of many Baconian constructions have revealed often used approaches of patterning the Baconian equivalents to the ciphertext, no doubt caused by the constructor’s desire to easily track all of the used a's and b's in an effort to properly apply values to the ciphertext. Awareness of the existence of such a pattern would greatly enhance plaintext recovery. Simultaneous posting of the

Baconian equivalent letters (a & b) to the ciphertext alphabet by the solver will create an awareness of possible pattern arrangements.

Some Observed Pattern Uses.

```
Cm MJ '96 E-10

ABCDEFGHIJKLMNOPQRSTUVWXYZ
aaaaaaaaaaaabbbbbbbbbbbbbb

Cm JF '95 E-4

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abababababababababababab

Cm SO '94 E-9

ABCDEFGHIJKLMNOPQRSTUVWXYZ
bbbbbbbbbbbbaaaaaaaaaaaaa
```

Cm MJ '88 E-5

ABCDEFGHIJKLMNOPQRSTUVWXYZ
aabbaabbaabbaabbaabbaabbaa

Baconian Concealment Cipher Example

The Baconian Cipher construction above would hardly accomplish Lord Bacon's interest in concealing the very existence of a cipher's presence but consider the following text's merit in using two distinct features to generate a concealment device:

BC-1

The "father" of the Baconian biliteral alphabet type message code as we know it, was one, Lord Francis Bacon, a noted scribe, philosopher, one time avid cryptologist, who strongly believed the only secret codes were those that effectively concealed the fact that any secret existed. *Sixteenth Century, elite, active, English political statesman, he used slightly…….*

It seems an innocent and harmless enough looking piece of text but look at what happens to it when the author instructs the recipient of it to assign "a" to words ending in a consonant and "b" to words ending in a vowel. Convert five letter Baconian Biliteral Alphabet "a's" and "b's" to plaintext for the concealed message.

See Appendix III for full message.

Baconian Crib Placement

Let's take the time to recap the Baconian crib placement procedure where no construction attempt has been made to conceal a cipher's existence.

BC-2. Baconian. Look for a conflict. (for) LIONEL

ENCRO SVFKP ERPER KREIF IWPEP EPRGB

TCMQU EGCQG CMETE YVZEL ETJCO YELAV

CREHS GXCEM SOCPE XMCFE.

The task before us is the assignment of letters from the Baconian Biliteral Alphabet to the ciphertext to convert to a meaningful plaintext. Our first step is to find the proper placement of our crib in the ciphertext. Find the values from the Baconian Alphabet for the crib and check all ciphertext letters against these values, looking for a proper fit.
(See below.)

Baconian Biliteral Alphabet

A=aaaaa	**E**=aabaa	**IJ**=abaaa	**N**=abbaa	**R**=baaaa	**W**=babaa
B=aaaab	**F**=aabab	**K**=abaab	**O**=abbab	**S**=baaab	**X**=babab
C=aaaba	**G**=aabba	**L**=ababa	**P**=abbba	**T**=baaba	**Y**=babba
D=aaabb	**H**=aabbb	**M**=ababb	**Q**=abbbb	**UV**=baabb	**Z**=babbb

Ciphertext groups having letters with "a" and "b" conflicts will be excluded as a possible crib placement location. We assign Baconian biliteral letters to the crib letters "for" and then assign biliteral letters to the ciphertext construction in three "word" groupings, looking for those letters with conflicting letter representations under the Baconian alphabet crib letters.

```
  f     o     r
aabab abbab baaaa  CONFLICTS

ENCRO SVFKP ERPER    E
SVFKP ERPER KREIF    FR
ERPER KREIF IWPEP    EPI
KREIF IWPEP EPRGB    E
IWPEP EPRGB TCMQU    none
```

The fifth ciphertext grouping gives us hope of proper crib placement. Posted Baconian values with generated plaintext will shed more light. Baconian letters are posted under the ciphertext letters:

```
CT letters  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Baconian     ba a a a   a  bab ba a
```

BC-2. Baconian. Look for a conflict. (for) LIONEL

```
ENCRO SVFKP ERPER KREIF IWPEP EPRGB
a ab      b abbab  baa  aabab abbab
  L?          O     K?    F     O
TCMQU EGCQG CMETE YVZEL ETJCO YELAV
baaaa aaaaa aaaba    a   ab a   a
  R     A     C
CREHS GXCEM SOCPE XMCFE.
aba   a aaa   aba  aa a
```

No concealment factor is present in the above cipher and the appetite of solvers of any experience length lends its interest in continuing to explore the concealment principle. Let's take a look at a Baconian Cipher which appeared in one of our Cm year end issues to see if we can make such a reality. It was submitted with all due apologies to the author of *"'Twas the Night Before Christmas,"* Clement Clarke Moore or Major Henry Livingston. It conceals a hidden message.

Determine the feature that is common to each of the ciphertext words in the following two Baconian ciphers which qualify them for a Baconian biliteral "a" or "b" assignment and allows the translation into plaintext.(Hint – check out the last letters of each word.)

BC-3. 'TWAS THE NIGHT BEFORE CADENUS! LIONEL

It was the eve before Crypts,
When all through my flat,
No creature be stirring,
Not one to force chat.
The crypts were so carefully hung,
In hope the solve,
Would be so soon
To our tongue.

Constructors were all nestled,
Secure in their bed,
Certain their crypts
Were no manner read.

Out on our Side lawn

Arose a loud noise and clatter,
All rose to view
What's the matter.

Away to the window we flew,
Quick as Olympian's racin',
Hopeful to behold,
Kasiski Determination.

Downstairs a cryptanalyst wore
His Brain most apart,
In trust that a solve
Would soon rear its start.

The fireplace mantle began
Emitting a reverberation,
Down came Santa
With no hesitation.

Toys flung on his back,
He toweled the perspiration,
Attending the backpack's
Exhaustive accumulation.

Held tight in his teeth,
Stem of a pipe glistened,
As a whine across the room
Gave cause for Santa good listen.

Across the space
He sped in good haste,
Toward the area of the dismay,
Quite quickly he raced.

(Massive heap cipher message store.)

Cipher messages lie all around
A confused cryptic's confounded daze.
Santa recognized at once
A baffling crypt, an unending maze.

An eye with a twinkle
Of a merry dimpled child,
Were all that gave hint
Of Santa's crypto cunning guile.

Quick to recognize cipher type,
Santa identified plaintext in French,
While “caracteres” lined up
To reveal a missive of railfence.

Sadness to joyfulness transference
In a moment, As ciphertext became
Plaintext, when under guidance of
The jolly eyes of Saint Nick.

Now Amsco, now Beaufort,
Now Gromark, now you Myszkowski,
Now Foursquare, now dash away,
Solve away, solutions to all.

BC-4. Baconian. Crypto Christmas Wish. LIONEL

I’m dreaming of a tough Quagmire,
Just as ones that made us perceive woe.
When our idea made sense
And we tensed,
For those thoughts of psyche
Now very slow.
I’m dreaming of a tough Quagmire,
With the constructions I thus write.
May you solve in sunny day light
And have all solutions just rite.

Baconian Construction

Let’s review the application of Baconian Equivalent letters (a and b) to each letter of a plaintext message. Notice the suggestion of a plaintext message with the construction ciphertext concealment ploy. The word, bacon, in Baconian equivalent letters is written as:

plaintext	b	a	c	o	n
Baconian Equivalent	aaaab	aaaaa	aaaba	abbab	abbaa
CIPHERTEXT	EARLY	LIGHT	SENDS	ADDED	HOURS

The “a” and “b” units are disguised by the assigning of ciphertext letters to each, logically looking plaintext or cleartext words in their own. The more sensible a message that these ciphertext letters and words can generate, the better the concealment of the actual plaintext message. Notice the suggestion of a plaintext message with the construction ciphertext EARLY LIGHT SENDS ADDED HOURS.

Ciphertext/Baconian Equivalents

Once a ciphertext (CT) letter has been assigned an “a” or “b” it must always be assigned to the same equivalent. (a or b).

```
CIPHERTEXT LETTERS  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Baconian Equivalent a  ba aaa  a ab  aaab   b
```

Become comfortable with the encipherment and decipherment process of the word “bacon,” its assignment of Baconian Equivalent letters to the ciphertext and complete the BC-5 cipher below. Begin by applying all Baconian Equivalent letters identified to the remainder of the ciphertext.

Solving Process Steps

1) Post Baconian equivalents to the ciphertext.
2) Recover plaintext for all five letter entities.
3) Sight read plaintext for uncompleted five letter entities.
4) Continue posting of Ciphertext/Baconian Equivalent alphabet.
5) Complete the plaintext.


```
CIPHERTEXT LETTERS  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Baconian Equivalent a  ba aaa  a ab  aaab   b
```


BC-5. Baconians are fun. (Bacon---) LIONEL

```
EARLY LIGHT SENDS ADDED HOURS
aaaab aaaaa aaaba abbab abbaa
  B     a     c     o     n
TWIXT LANES ABOVE BLACK CAVES
a a a aaaaa a b a  aa    a aa
        a
WHERE FROGS CROAK WACKY MODAL
 aaaa  abaa  aba   a  b  bbaa

GEEKS AWARE LOOKS CLOUD EQUAL
aaa a a aaa  bb a  abbb a baa

PARTS JAZZY.
 aaaa  a  b
```

BC-6. Navigator. (with) LIONEL

STORM NASTY RAILS WRECK BEACH

LINED EARTH PAILS EXTRA BOOZE

PACTS DROWN WHIMS DRIES STOOP

WIELD SPRAY GRIME TOPIC PACTS

MEETS MEDIC FIRST JAUNT CRAMP.

Chapter Twelve

Xenocrypts

If you have never attempted solving a Xenocrypt for fear of not knowing the language, you are performing a huge disservice to yourself. Many of the Xenos on the first page of the column are a lot easier than the Aristos and Pats that cause us so much pain.

Necessary tools are at a minimum. Bi-lingual proficiency is not among them. Although a foreign pocket dictionary is helpful, it is not required. Notice that all of the Xenocrypts on the first page of the column are constructed with a K1 or K2 keyword alphabets. Keyword Alphabet analysis is a most helpful asset to use when solving Aristocrat and Patristocrat ciphers. (See Chapter Five.) Other helpful tools are the *ACA Xenocrypt Handbook* available through our ACA Sales Person and foreign language sites on Internet Web sites.

Let's take a look at the Spanish Xenocrypt in the MA 2003 Cm.

MA 2003 Cm, X-3. Spanish K2. (84) (todas las) Snow white. JOE-O

```
E K   P F   J Q H P Y   S A K   K X   R Y J F E   V F E   O I F X J K E
s     a d     o           t o d a s   l a s       a d s

X Y B K V F E   E K   Z A K J K   K X H Y X R I F I   F V O A X
  o     l a s   s       d           o t a     a l

I F E O Y   F A R Y G Q Y O I F M Q H Y   J K V   F A R Y I.
  a s   o   a   t o     o     a       o   d   l   a   t o
```

Look at the plaintext that is shown by simply fitting the crib (todas las) in the only place it will fit. Xeno cribs present excellent cipher entry points. Post impacted plaintext in red.

Now post the known plaintext letters to your K2 Keyword Alphabet to help you find additional plaintext. Red lettering will remind you of the correct crib letter placement.

```
abcdefghijklmnopqrstuvwxyz (pt)
F  J       V  Y   ER       (CT)
```

Educated Supposition #1 G =b, H =c, K =e, W =m, X =n, Z =p

```
abcdefghijklmnopqrstuvwxyz (pt)
FGHJK      VWXYZ  ER       (CT)(Crib letters)
```

Educated Supposition #1 Plaintext Fill

```
EK PF JQHPY SAK KX RYJFE VFE OIFXJKE XYBKVFE EK ZAKJK
se  a d c o   e en todas las   andes no elas se p ede

KXHYXRIFI FVOAX IFEOY FARYGQYOIFMQHY JKV FARYI.
encont a  al  n  as o a tob o  a  co del a to .
```

Spanish bilinguals or those with a Spanish pocket dictionary will most likely recognize plaintext words, eight, nine, eleven, twelve and fifteen. But such luxuries were not assumed in our original list of necessary tools.

Educated Supposition #2

We can safely assume that a vowel is needed for ciphertext letter “Q” in the third word. Ciphertext“Q” fits nicely for plaintext “i” in the K2 Keyword Alphabet. Ciphertext letters, O and P fit in nicely ahead of Q.

```
abcdefghijklmnopqrstuvwxyz (pt)
FGHJK OPQ  VWXYZ  ER       (CT)
```

Yielding the following plaintext:

```
EK PF JQHPY SAK KX RYJFE VFE OIFXJKE XYBKVFE EK ZAKJK
se ha dicho   e en todas las g andes no elas se p ede

KXHYXRIFI FVOAX IFEOY FARYGQYOIFMQHY JKV FARYI.
encont a  alg n  asgo a tobiog a ico del a to .
```

This should be enough plaintext for even those of us who may have the least acquaintance with the Spanish language. As we go on to make the educated suppositions that CT letters, A, I and S = pt letters, u, g and q, our keyword falls into place. Although we discontinued the crib red lettering above, it is helpful to be aware of letters known to be correctly placed.

A Note on Educational Reading

Speed-reading of educational material is appropriate for overview purposes only. Line by line understanding is a necessary requirement for that which we wish to permanently digest.

The Xenocrypt fundamental principles of which we speak are applicable to many other cipher types. The keyword alphabet recovery process is most useful in Aristocrats, Patristocrats and many of the Cipher Exchange crypts.

We have referenced, above, the special tools which can be used for the solving of Xenocrypts. The *Xenocrypt Handbook* is an immeasurable aid as you begin to tackle the slightly more difficult Xenocrypt constructions, Edited and published by PHOENIX in 1996. it is available in the For Sale list of publications on page 14 of the *ACA Cryptogram* journal.

The handbook is full of instructional material, foreign language word lists, frequency tables and statistical data. We will use it to solve the X-1 French Xenocrypt by OMEGA entitled "Consolation" that appeared in MA 2003 issue of the Cm.

MA, 2003 Cm, X-1. French K2. (97) (triste) Consolation. OMEGA

M Q Q ' T D Y I X H I I S Y M Q I S F I I Z H T M Z Q I Y

Q B X R I Y G B S Y Y I Y E I C P. M Q Q C M V X I S G Q B

R B M S, Q B Y I X X I I Z G M Z G T C F I R I S Z: " S I

Y T M Y V B Y Z X M Y Z I."

We place the crib "triste" under ciphertext letters ZXMYZI. This is the only place the crib will fit and generates the following plaintext:

```
MQ Q'TDYIXHI IS YMQISFI IZ HTMZ QIY
i      ser e e  si e  e et   it  es

QBXRIY GBSY YIY EICP. MQ QCM VXISG
  r es    s ses  e    i    i  re

QB RBMS, QB YIXXI IZ GMZ GTCFIRISZ:
     i      serre et  it     e e t:

" SI YTMY VBY ZXMYZI."
   e s is   s triste.
```

Highlight these placements in red lettering.

K2 Keyword Alphabet:

```
abcdefghijklmnopqrstuvwxyz (pt)
    IJKLM        XYZ       (CT)
```

Let's see what additional plaintext we can gather with our Xenocrypt Handbook French word list:

MQ = i_ becomes MQ = il
IS = e_ becomes IS = en
QCM = l_i becomes QCM = lui
QB = l_ becomes QB = la
GMZ = _it becomes GMZ = dit
VBY = _as becomes VBY = pas
YTMY = s_is becomes YTMY = sois

Check what the additions of plaintext letters, l, n, u, a, d, p, and o do to the Keyword Alphabet.

K2 Keyword Alphabet Update:

```
abcdefghijklmnopqrstuvwxyz (pt)
B  GIJKLM  Q STV XYZC      (CT)
```

Educated Suppositions

R = m, W = q and DF =bc (Ciphertext C has already been used and ciphertext E is more likely to be part of the keyword than ciphertext D or F.

K2 Keyword Alphabet/Plaintext Update:

```
abcdefghijklmnopqrstuvwxyz (pt)
BDFGIJKLM  QRSTVWXYZC      (CT)

MQ Q'TDYIXHI IS YMQISFI IZ HTMZ QIY
il l'obser e en silence et  oit les

QBXRIY GBSY YIY EICP. MQ QCM VXISG
larmes dans ses  eu   il lui prend

QB RBMS QB YIXXI IZ GMZ GTCFIRISZ:
la main la serre et dit doucement

" SI YTMY VBY ZXMYZI."
  ne sois pas triste.
```

Complete the missing letters and you will generate the keyword.

Here's another:

X-2.. Italian. K2. Poetico. (placidi) LIONEL

LPUK L PZGHK JL' MGZUBAB OZB, GK PMGLJALJRL SJBTLOPK Z TLALO, Z QOSUBZO JL G"ZIKO UEL QOZIZB, UEL JKJ TKGGB NSB BIMSOK HKALO.

Internet users can call up, Freelang, a collection of two way dictionaries in 42 languages at http://www.freelang.net/dictionary/index.html

Chapter Thirteen

Polybius Square

As we begin to set our sights upon *Cm* Cipher Exchange (CE) constructions, it will aid us to become familiar with the makeup and working of a keying device known as the Polybius Square that is used to key many of the CE ciphers. Ciphers using the Polybius Square are substitution type ciphers in which each letter of the plaintext is represented by a pair of digits.

Polybius was a Greek historian (203-120 B.C.) who first proposed a method of using a unique two digit number for each letter of the alphabet. A five by five square with numbered columns and rows is used to "store" the alphabet.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Note that the letters "I" and "J" are written in the same cell to divide the letters evenly. To encode, we simply substitute the numbers in the rows and columns for the letter we wish to use. Always put the row number before the column number. For example, the number for the letter "S" will be 43. The numbers for the word "encode" will be:

15 33 13 34 14 15

Are you thinking that this is far too simple and easily decipherable? It is until we complicate the scenario with the introduction of a keyword. Look what happens to our ciphertext numbers for “encode” when the keyword “SQUARE” is introduced to our Polybius Square.

```
   1   2   3   4   5
1  S   Q   U   A   R
2  E   B   C   D   F
3  G   H  I/J  K   L
4  M   N   O   P   T
5  V   W   X   Y   Z
```

Ciphertext for “encode” becomes:

21 42 23 43 24 21

The diabolical constructor can magnify the complexity of the keyword square by changing the order of the letter pattern. The letters can be written in vertically, in reverse order, in a

spiral or in diagonal formation. They need not even begin in the upper left hand corner of the square. What is a poor innocent solver to do? As with Aristocrats, Patristocrats and Xenocrypt ciphers, cribs, frequency counts and knowledge of the general properties of letters, *ACA and You Handbook*, page 14, become very valuable in observing just which direction the keyword square letters are aligned. We will start the solving process with a straight forward example, accompanied by a crib.

PS-1 Polybius Hybrid. Gram cracker.(solver)

```
15    12 14 51 42 31    11 12 13 14    45 14 35 52 24 13

53 32 14   23 24 22 13 12 43 11 45   11 12 13 14

31 13 15 41 45   33 45    15    31 13 15 41

22 13 15 22 34 24 13.
```

Placement of the crib in the only place it will fit (the sixth word is hyphenated) leads to this plaintext and Polybius Square start.

```
15    12 14 51 42 31    11 12 13 14
         O                   r  o

45 14 35 52 24 13    53 32 14
 s  o  l  v  e  r          o

23 24 22 13 12 43 11 45
    e     r          s
```

```
11 12 13 14    31 13 15 41 45
       r  o        r        s

33 45    15    31 13 15 41
    s             r

22 13 15 22 34 24 13.
    r           e  r.
```

PS-1 Use the title, short words and high frequency letters (senorita) to help you complete the plaintext and Polybius Square with its key word.

```
   1  2  3  4  5
1  .  .  R  O  .
2  .  .  .  E  .
3  .  .  .  .  L
4  .  .  .  .  S
5  .  V  .  .  .
```

We began our discussion of a Polybius Square with a construction we called a Polybius hybrid. We referred to it as a hybrid because we put the construction together in a manner to demonstrate its principles. As you use the Polybius Square for future Cipher Exchange constructions, each cipher type will have its own way of using the square as a key to its encryption. We will discuss the subtle variations in the uses of the Polybius Square as we study each cipher type. At present, we will continue to refer to the usage of horizontal and vertical numerals to identify each block of the square.

We presented a simplistic horizontal arrangement of letters in our square to allow us to more easily digest the instruction principles. We will increase the degree of difficulty just a bit in to illustrate how the diabolical constructor may alter a key square to increase the security of the message. Always keep in mind that the purpose of the Polybius Square is for it to be the keying device between the writer and the reader. Let's look for the clues that indicate to us that a key square is something different than a simple horizontal letter flow.

Location of Low Frequency Letters

When crib placement letters result in the locating of low frequency letters in a place other than the last row of the 5 x 5 square, we have a clue that something may be amiss. Perhaps, VWXYZ is part of the keyword and appears in the first or second row of the square, but low letter frequency locations as below tell us even more about the order of the square.

```
  1 2 3 4 5        1 2 3 4 5
1 . . . . V      1 V . . . .
2 . . . . W      2 W . . . .
3 . . . . X      3 X . . . .
4 . . . . Y      4 Y . . . .
5 . . . . Z      5 Z . . . .
```

```
VERTICAL ORDER   REVERSE VERTICAL

  1 2 3 4 5        1 2 3 4 5
1 . . . . .      1 Z X W . .
2 . . . . .      2 Y V . . .
3 . . . . W      3 . . . . .
4 . . . V Y      4 . . . . .
5 . . . X Z      5 . . . . .

DIAGONAL ORDER   REVERSE DIAGONAL

  1 2 3 4 5
1 Z Y X W V
2 . . . . .
3 . . . . .
4 . . . . .
5 . . . . .    REVERSE HORIZONTAL
```

Keep in mind that the letters "I" and "J" are always written in the same cell to allow the complete alphabet to fit in the 25 cell square.

Keyword Recovery

With so many possible alphabet order variations, you may wonder how a key word can ever be recovered, but proper crib placement leads to both plaintext and five by five key square recovery. See how the crib placement below leads to both plaintext and keyword square recovery.

PS-2 Polybius Square. Old timer's lament. (youth)

```
51 35 32 51 41 41    51 14 51 31 13 45
                                    y
23 41    25 12 41 44 51 42    21 14
                     t
44 11 51    45 21 54 44 11.
 t h        y  o   u  t  h
```

PS-2 Determine the square key and alphabet order.

```
  1 2 3 4 5
1 H . . . .
2 O . . . .
3 . . . . .
4 . . . T Y
5 . . . U .
```

PS-3. Poly High. South Sea Adventure. (going)

24 42 34 12 24 43 34 14 12 52 22 11 15

14 15 22 14 42 22 43 45 24 34 15 14 12 13 14

12 25 42 54 15 22 14 45 12 43 32 11 33 43 32

15 24 42 12 43 15 24 11 52 22 54.

.

PS-4. Holly Poly Xmas. (Christmas)

53 42 25 23 42 53 21 31 31 41 12 21 31 31 41 52 53 34 12 32 15 24 42 32 12 15 32

15 53 23 51 23 32 15 15 12 24 23 21 33 15 53 23 41 23 42 54 12 13 21 34 15

14 34 21 35 12 33 15 53 23 54 23 31 31 51 23 32 34 21 35 51 22 15 53 42 25 23 42

52 22 11 21 33 52 53 23 23 54 51 22 54 31 12 25 23 32

Chapter Fourteen

Checkerboard Cipher

We have had some fun in our chapter reviewing the Polybius Square. We will now devote attention to ciphers, appearing regularly in the **Cm** Cipher Exchange column, which make use of the Polybius Square as its keying device. Let's start, here, with a discussion of the Checkerboard Cipher. It is a fun type cipher that uses pairs of letters as ciphertext. The pairs of letters represent the horizontal rows and the vertical columns of the five by five square.

Checkerboard Square Keywords

The ciphertext letters are generated by two five-letter keywords, one to represent the rows of the square and one to represent the columns. A third keyword inside the square allows us to set up the square key and alphabet order. Let's work our way through an example of how the square is set up, along with the use of three keywords.

	W	**R**	**O**	**N**	**G**
R	**M**	**I**	**S**	**T**	**A**
I	**K**	**E**	B	C	D
G	F	G	H	L	N
H	O	P	Q	R	U
T	V	W	X	Y	Z

Checkerboard Construction

A plaintext letter is represented by two ciphertext letters. The coordinate to the left of the square (**RIGHT**) is always the first of the two ciphertext letters and the coordinate at the top of the square (**WRONG**) the last. **MISTAKE** has been chosen as the keyword within the square. See if you can follow the encipherment of the plaintext (pt) below:

```
pt   c  r  y  p  t  o  g  r  a  m
CT  IN HN TN HR RN HW GR HN RG RW
```

This construction lesson points out a very important principle which aids in the recovery of our row and column keyword coordinates. The first letter of the ciphertext pair generates the left hand row coordinate and the last letter of the ciphertext pair, the column coordinate above the square. We need to anagram each of the first and last letters of the ciphertext pairs to arrive at these coordinates .Only five different letters will appear in each of the first and last letters of the ciphertext pairs.

Checkerboard Decipherment

Keeping these principles in mind, we will place the crib and generate the resulting plaintext and square key in the following Checkerboard Cipher. You need only to complete it.

CB -1. Checkerboard. Colorful scene. (yellow)

```
KT BT BH BH AE KH   AW CT   AE AT BT
 y  e  l  l  o  w           o     e

AE LI   CE LE BT   BW CI AW LT LE CE
 o            e

LW AE BH AE CI CT.  AW CE   AW CT
   o    l     o

AE LI CE BT AT BI CT BT LH CE AE
 o       e          e       o

LW AE AI AI BI AT AW LW BE CE BT
    O                       e

LW BE BI CE AW AE AT    BE AT LH
                 o
BE KH BE CI BT AT BT
```

```
   W H I T E
B . L . E .
L . . . . .
A . . . . O
C . . . . .
K . W . Y .
```

First letters of ciphertext pairs yielded KBACL, second letters of pairs THEWI, anagramming nicely into keywords, BLACK and WHITE.

Let's take a look at the Checkerboard construction found in the JA2003 Cm:

JA 2003 Cm, E-4. An Irish blessing. (before) DYETI

UR EA AU AU EE AE **PA EZ ER PR TU EZ** EA
b **e** f o r **e**

PZ EZ PR TU EA AR TA EA PR TU EE AE UE

PA EZ TA EE UE EZ TE TU EZ AA EZ PZ ER
b **e** f o r **e**

AR TR **PR EE UZ EU AU EE** AE UE EZ AA EZ EA AA.
b **e** f o r **e**

There are three possible crib location placements based upon the ciphertext letter intervals shown in bold print. We must evaluate the crib placement effect on the Polybius Square makeup.

Anagramming the five repeated first letters of the construction digraphs generates the word **taupe** for the row keyword of our square. Repeating this process with the second letter of the construction digraphs gives us **azure** as the column keyword of the square.

We now post our three possible crib placements in the Polybius Square:

1

	A	**Z**	**U**	**R**	**E**
T	.	.	R	.	.
A	.	.	.	.	.
U	.	.	.	.	.
P	B	.	.	O	.
E	.	E	.	F	.

2

	A	**Z**	**U**	**R**	**E**
T	F	.	.	.	.
A	.	.	.	.	.
U	.	.	.	.	R
P	B	.	.	.	.
E	.	E	.	.	O

3

	A	**Z**	**U**	**R**	**E**
T	.	.	.	.	.
A	.	.	R	.	.
U	.	F	.	.	.
P	.	.	.	B	.
E	.	.	O	.	E

Now we must enter the mindset of the diabolical constructor to attempt to get a read on his intended Polybius Square path. The first path that jumps out as a distinct possibility is a reverse vertical column path in the second square since the exact number of squares exist to fit the letters "A" thru "F" in reverse order in the first column. The letter "E" already located in the second column is quite likely to be part of the keyword.

	A	**Z**	**U**	**R**	**E**
T	F	.	.	.	.
A	D	.	.	.	.
U	C	.	.	.	R
P	B	.	.	.	.
E	A	.	E	.	O

Let's see what effect these square placements have on the plaintext:

```
UR EA AU AU EE AE PA EZ ER PR TU EZ EA
   a        o     b  e           e  a

PZ EZ PR TU EA AR TA EA PR TU EE AE UE
   e        a        a        o     r

PA EZ TA EE UE EZ TE TU EZ AA EZ PZ ER
b  e  f  o  r  e        e     e

AR TR PR EE UZ EU AU EE AE UE EZ AA EZ EA AA.
         o           o     r  e  d  e  a  d.
```

It looks like we're on the right track. Ciphertext AU and AE which surrounds plaintext "o" is ripe for plaintext "y" and "u." This leads to an opening of UR equaling "m." Ciphertext TE and TU look much like plaintext "he." Let's see what that does to the Polybius square.

CB-2 Complete the Polybius Square.

	A	**Z**	**U**	**R**	**E**
T	F	.	H	.	T
A	D	.	Y	.	U
U	C	.	.	M	R
P	B	.	.	.	.
E	A	E	.	.	O

It looks like a breakthrough. Our "reverse columnar" key is taking the shape of a reverse spiral beginning in the upper right hand corner of the square and looking much like another color to complement **taupe** and **azure**. All that is left to do is to complete the reverse spiral key square and fill in the remaining plaintext.

CB-3. Checkerboard. Detour. (between)

EK UN EA TK UN UB OB EK EA TK EK

EB TN TK EK TB RN UA EA

RB EA EK US EA EA RN EK US UB

OK UB TN RN EK TK TN TK RK RN EB EA OB

UA UB RN TK EK OB RK UA EK TN UB RN.

Chapter Fifteen

Foursquare Cipher

In our last chapter we examined the usage of the Checkerboard Cipher to replace plaintext pair of letters (digraphs) with an equivalent cipher-text pair keyed by a single Polybius Square. The Foursquare Cipher, as its name implies, uses four such squares, **numbered in clockwise order**, to replace plaintext with ciphertext.

Squares one and four contain unkeyed plaintext letters always in horizontal alphabetical order. Squares two and three contain keyed ciphertext letters in any patterned order (vertical (horizontal, straight, reversed, spiral, diagonal, etc.). Ciphertext location is aided with a provided crib. Square numbering order is 1, 2, 4, 3. A picture and an example are worth a thousand words.

1-pt 2-CT

Normal PT Alphabet Order	Mixed CT Alphabet Sequence
Mixed CT Alphabet Sequence	Normal PT Alphabet Order

4-CT 3-pt

FS-1. Foursquare. Commonality. (th ey bo th pr od uc eg-) (fa=NN) (bc=LA)

```
XO TP TL FB TO QB FI KB QE TZ MT GD RY
                        th ey

RQ QD SV TF HB GL KH GX CX QE TP BT SS
                           th

RX QE TZ TH QE GU KI QS AF OA HA OA ID AU QX.
   th ey bo th pr od uc eg
```

The bold ciphertext letters indicate a good fit for our crib with repeat “th” digraphs and we fill in the identified ciphertext letters. Let’s examine the effect of this crib placement on the ciphertext squares.

```
    1              2
a b c d e      . A L T .
f g h i k      N . . . .
l m n o p      . G . K .
q r s t u      . . Q . .
v w x y z      . . . . .

N A . I S      a b c d e
. . . E F      f g h i k
. H . . .      l m n o p
. . . . U      q r s t u
. . . . Z      v w x y z
    4              3
```

The first letter of each plaintext pair in the crib is found in square one, the second in square three. Those two cells are considered the opposite corners of a rectangle. Cipher letters are found at the other corners of that rectangle, the first in square two and the second in square four. Post the ciphertext letters of our crib plaintext results in the sequence below for squares two and four. Complete the two squares for the keywords.

FS-2 Keyword Squares.

```
    2              4
. A L T .      N A . I S
N . . . .      . . . E F
G K M . .      G H K L M
O P Q . .      P Q R T U
. . . . .      V W X Y Z
```

We have filled in the bold type letters where alphabetical sequencing permits us to do so. (You can probably make a good guess at square two, row five.)

The decipherment process of converting ciphertext to plaintext is the reverse of the procedure that we used to post our crib letters to squares two and four. The first ciphertext letter is located in square two and the second in square four. Those two cells form the corners of a rectangle. Plaintext letters are found at opposite corners of that rectangle, the first in square one and the second in square three.

Our ciphertext Square blocks two and four now allow us to find the plaintext letters in the partly solved cipher below. The ciphertext digraphs XO, HB and ID are easily identifiable and the solution is close at hand.

FS-1. Foursquare. Commonality.

```
XO TP TL FB TO QB FI KB QE TZ MT GD RY
   at do                th ey ou
```

```
RQ QD SV TF HB GL KH GX CX QE TP BT SS
         ei    om mo nw    th at

RX QE TZ TH QE GU KI QS AF OA HA OA ID AU QX
   th ey bo th pr od uc eg ra mc ra    er sx.
```

We will continue our discussion of the Foursquare Cipher by working our way through one with a bit more challenge to it than our introductory example. This was published in the Cipher Exchange as E-22 in the JA2001 Cm**,** so you can be assured that there is some trickery involved.

Remember the enciphering and deciphering principles for solving a Foursquare Cipher.

Encipherment: The first letter of each plaintext pair is found in square one, the second in square three. Those two cells are considered the opposite corners of a rectangle. Ciphertext letters are found at the other corners of that rectangle, the first in square two and the second in square four.

Decipherment: The process of changing ciphertext to plaintext is the reverse of that of encipherment. The first ciphertext letter is located in square two and the second in square four. Those two cells form the corners of a rectangle. Plaintext letters are found at the opposite corners of that rectangle, the first in square one and the second in square three.

JA2001. E-22. Unwarranted Admiration. (su/pe/rs/ti/ti/ou/s ;il=OR) BITWISE

```
QT LC PK XH XG AE PD CV PW EE HL CL CY

IP HL QL SH XC WQ MQ CY HY RX KM DP OR
                   th

QT VP SE YP RM PO KD IT QO IS SQ EE CO
                               ti

PO KM LP YM XV MA SQ SQ XT LN BL LV SQ
         su pe rs ti ti ou s         ti

KR WQ UY SH XV VC EM TQ CL HY.
            pe
```

The repetitive ciphertext digraph **"SQ"** allows for easy placement of the crib. We complete all of the plaintext that our crib placement permits and post our identified ciphertext digraphs to our foursquare matrix using our principles of encipherment from above.

```
    1               2
a b c d e       . . . . .
f g h i k       O . . . .
l m n o p       . . . . X
q r s t u       . . M S Y
v w x y z       . . . . .

. . . . V       a b c d e
. . . Q .       f g h i k
. . . R .       l m n o p
. A M T .       q r s t u
. . . . .       v w x y z
    4               3
```

Ciphertext letters, X and Y in square 2 and Q, R and T in square 4 suggest vertical columnar alphabetical sequencing. We are able to add ciphertext letters to squares two and four. (**Bold type**.)

FS-3 – Find the Keywords.

```
    1               2
a b c d e       . . . P U
f g h i k       O . . Q V
l m n o p       . . . R X
q r s t u       . . M S Y
v w x y z       . . N T Z

. . . P V       a b c d e
. . . Q W       f g h i k
. . . R X       l m n o p
. A M T Y       q r s t u
. . N U Z       v w x y z
    4               3
```

Our Foursquare deciphering rules now allow us to recover additional plaintext on route to a solving completion.

FS-4. Complete the Plaintext.

```
QT LC PK XH XG AE PD CV PW EE HL CL CY
it                      ei
```

```
IP HL QL SH XC WQ MQ CY HY RX KM DP OR
                   th       po       il

QT VP SE YP RM PO KD IT QO IS SQ EE CO
it ie    te nt                ti

PO KM LP YM XV MA SQ SQ XT LN BL LV SQ
         su pe rs ti ti ou s        ti

KR WQ UY SH XV VC EM TQ CL HY.
      eu    pe       yj
```

Hint: Look for Europe and responsibilities.

FS-5. Tooting one's horn. (al lr ai lr oa dm en fr om th)

SA DI RO DI EO BQ HX CI DQ LP HV KQ VS OL DS RL QS WG HX PC XG BY YH

QK UE TG RS WG RL SV QE TG FO QA NE LP BZ PH RL XT SG QL VB LY OV RQ

YS LD LP BZ WG SX LM.

Chapter Sixteen

Railfence and Redefence Cipher

Cryptologists have long contended that encipherment construction is one of the best ways to learn many idiosyncrasies of the various cipher types that will aid in the solving process.

This is well illustrated with the Railfence Cipher**, a** transposition cipher that came into being during the American Civil War. This cipher looks like an aerial view of a railfence. A simple illustration of the technique should help.

```
T   A   E   I   R   P   T   C   E
 H R I F N E S T A S O I I N I H R
  E   L   C   A   N   S   O   P
```

In this example the plaintext is written in a zigzag pattern between the three rails (lines). We refer to this pattern as a three rail fence with no offsets. An offset refers to the number of rails excluded from the beginning of the cipher's plaintext. (See rail examples four through seven on the next page.) The text begins at the top left in a cipher with no offsets. The ciphertext is taken off in groups of five horizontally across the "fence" top to bottom and written in groups of five letters: TAEIR PTCEH RIFNE STASO IINIH RELCA NSOP.

ACA practice limits the number of rails used to three through seven rails.

It is the variation of rails and offsets that creates the complexity and challenge of this cipher type. A crib aids the process of evaluating the variations of rails and offsets but trial, error, and a good eraser are invaluable tools towards the solution.

However, this trial and error process makes us intimately familiar with the construction routine and is the very process that has aided computer-oriented members to work at the development of programs that produce solutions in the blink of an eye. It behooves us to work to learn the intricacies of the Railfence system to attain such a level of understanding.

The development of Railfence cons for the *Cm* is a good place to begin. As you increase the difficulty through rail and offset variations you will gain an expertise in the recognition of these variables when solving.

A good tool that helps with the trial and error determination of the correct number of rails and offsets is a Railfence template. (Appendix IV.)

Three through Seven Rail Types. Ciphertext read horizontally, plaintext is zigzag.

Three Rails, No Offsets

```
P   n     t     h     f     t
 l i t x w t n o f e s
  a   e     I     o     s
```

Four

```
___       k       s       e       n       f       f
   A    n f   t p     r p   e t     o f     o   o
     b a   i s   a e     r s     s n   s t     n
       l     r     c       e       a       e       e
```

Five

```
___           n           i           e
  ___       a k       s   s       s   t
     T    l     s     e     a     f     o     o
       w b       p c       n f       f   w
         o         a         o         t
```

Six

___ a q e
___ l n e u s t
___ b k s a f t
T e s e l f h
h e p c a o r e
r a n e

Seven (No offsets)

A I h a
C t o t r r i
A c n m e n l
C u s o e e s
o r a r t v
n t r f o e
s e s

RFC-1. Railfence. Paper & Pencil. (error)

(4 rails, you determine the offsets.)

RNLSL CSROL RSSEA ECOUN OIFEI RRIET FAARO RUSPP NPIST

OFAEC PEEUA OTINE ROCEA DLIRN HQLRD FC.

Post the ciphertext along the horizontal template rows (See Appendix IV) until the crib "error" is observed in a zigzag diagonal position. Offsets are involved in this cipher so you will have to experiment with a varying number of offset blank spaces in the first diagonal line.

RFC-2. Railfence. Use a template. (cipher)

FIEAT WESOA LHRSG NATOS TTIUR CPMSE OISOF SHRIE CNF.

See Appendix IV For the Railfence Solving Template.

Redefence Cipher

The same solving principles used to decipher the Railfence Cipher can be put to use for the solving of the Redefence Cipher with one slight twist. The Redefence Cipher construction mixes the fence rows to increase the complexity of the solving procedure. (There go those devious encipherers again attempting to stay one step ahead of the innocent cryptanalysts.)

We will follow the procedure to solve the Redefence Cipher in the MA 2012 *Cryptogram* issue with four rails, no offsets used in the construction, in a rail order of 3, 2, 4, 1.

MA2012 E-12 Redefence. Tranquility. MARSHEN

LIEOH TMTOA EFRSL ANASH UTIEI DLSIA

TUROM SAPFL EHYCT LSELN FM.

There are fifty-two letters in the cipher construction. Count off fifty-two spaces in a zig zag path for a four rail cipher in the Railfence Template located in Appendix IV. Post the ciphertext letters horizontally in these four rails, beginning with the spaces in rail three and continuing with rails 2, 4 and 1, in this order. The cipher construction will reveal a plaintext solution in the following zig zag arrangement.

C t l s e l n f m
a s h u t i e i d l s i a t u r o
l i e o h t m t o a e f r s l a n
m s a p f l e h y.

Just a bit more complex than the Railfence Cipher, the Redefence Cipher requires much trial and error to test the posting of the ciphertext letters in all possible rail sequence combinations. Become familiar with the process and those with computer programming aptitude can join the ranks of other ACA computer solvers in the development of a program which will generate a solution in the "blink of an eye." (RISHU)

We will provide the number of rails and offsets in the following Redefence Ciphers to allow you to become familiar with the solving process as you "cut your teeth" on this cipher type.

SO 2012, E-11. Redefence. Oral Output. Four rails, one offset. (more) APEX DX

FEALS ADNDN MRISI TADNA RIIDE EAHOT LSAOO SDNE.

MA 2011, E-8. Redefence. Divine right. Five rails, two offsets. (were) RIG R MORTIS

UAYAC TWRDS NCVNO GIHDO SGWRH POSTH VRTES EAOAD ERTON FROSE SEGAA AEFON TSAEI DSET.

Chapter Seventeen

Polyalphabetic Cipher (Quagmire)

Our cipher type discussions, heretofore, have centered on mono-alphabetic cipher type constructions (single alphabet). It is now time to extend our cipher solving skills to those constructions that use more than one alphabet to key the ciphertext encipherment.

We refer to this cipher construction type as polyalphabetic and this type of keying process takes place in what is known as a periodic cipher.

A periodic cipher is one in which the substitution process takes place in a repetitive manner that coincides with the length of the keyword. If the key word of the cipher is seven letters in length, the cipher will be represented by seven columns and seven different alphabetic substitutions will be used, one for each column in the cipher.

For the encipherment of a period seven cipher, text is written horizontally into seven column lengths. Each column is encoded with its own cipher alphabet, generating what is referred to as a polyalphabetic cipher. Plaintext for "The Tyro Gram column is written for the young at heart" would read:

```
1 2 3 4 5 6 7
t h e t y r o
g r a m c o l
u m n i s w r
i t t e n f o
r t h e y o u
g a t h e a r
t.
```

Each column is enciphered with an alphabet that begins with the keyword letter representing its column. Unlike the simple substitution type mono-alphabetic cipher, a polyalphabetic cipher permits a letter to stand for itself. Self-encryption permitted.)

Let's use the keyword **CRYPTIC** to encode our tyro gram plaintext. Our ciphertext alphabets for the seven columns become:

```
  abcdefghijklmnopqrstuvwxyz
1 CDEFGHIJKLMNOPQRSTUVWXYZAB
2 RSTUVWXYZABCDEFGHIJKLMNOPQ
3 YZABCDEFGHIJKLMNOPQRSTUVWX
4 PQRSTUVWXYZABCDEFGHIJKLMNO
5 TUVWXYZABCDEFGHIJKLMNOPQRS
```

6 **I**JKLMNOPQRSTUVWXYZABCDEFGH
7 **C**DEFGHIJKLMNOPQRSTUVWXYZAB

The ciphertext letters for each column number are now used to encipher the plaintext message. Substituting the ciphertext letters in each column for the plaintext letters at the top of the above table we arrive at the following enciphered message:

Ciphertext:

C R Y P T I C
1 2 3 4 5 6 7
V Y C I R Z Q
I I Y B V W N
W D L X L E T
K K R T G N Q
T K F T R W W
I R R W X I T
V.

Written out in five letter groups, the cipher would appear:

VYCIR ZQIIY BVWNW DLXLE TKKRT

GNQTK FTRWW IRRWX ITV.

The solving process puts all of the principles that we have discussed here into reverse. Conventional ciphers are much longer in length than the one we have reviewed here and allow us to use frequency analysis by column to make inroads into the plaintext.

Previously our cipher type analysis has discussed only those ciphers free from the need of period determination. If we are to extend our solving prowess to all cipher types it is necessary for us to learn how to determine the period length, or number of columns, in a periodic cipher.

A periodic cipher is one in which the substitution process takes place in a repetitive manner that coincides with the length of the keyword. If the key-word of the cipher is seven letters in length, the cipher will be represented by seven columns with seven different alphabet substitutions, one for each column in the cipher.

Polyalphabetic substitution ciphers use multiple lines of keyed ciphertext to cover a message’s plaintext instead of the mono-alphabetic process of one keyed line of ciphertext letters.

Period Determination

Let's begin the discussion of how to detect the period length or number of columns in a cipher with those ciphers that reveal period determination by a simple repetition of letters. Quagmire ciphers fall in this category. A crib always accompanies these ciphers.

Q-1, JF 1997 Cm E-21. Quagmire II. Cloudburst. (shortestrecordedperiod.) LIONEL

```
TEFCB JUTHA QAWHJ UBHBJ FIDJH WETRV
   sh ortes treco rdedp eriod

WDGCK UTGAK JIEAO DQPWR GWJHU RWDXP


TWWXU MCNFE UKVSE NATTF KZAAN DGTBM


HAWVX REMJD XYWHU EBMZL LFSDL FQRRW.
```

We have placed the crib correctly. Let's see how this determination was made. We begin by looking for repetitive intervals in the given crib, **shortestrecordedperiod**. We have the letters, s, o, r, t, e and d as our repeated letters in the crib with intervals of 2, 3, 4, 5, 6, 8, 9 and 10 spaces appearing at different points between these repeated letters.

One of these intervals will be the cipher's Period, keeping in mind the term Period refers to a reoccurring definite interval, cyclical in nature. Now we determine which of the intervals proves to be the cipher's foundation. **The interval that properly reflects like ciphertext letters for like plaintext letters will generate the proper periodic repetition.** We try different periodic column formats until we find like ciphertext letters representing like plaintext letters.

Interval/Period Nine Table

```
123456789 123456789 123456789
TEFCBJUTH DQPWRGWJH HAWVXREMJ
   shorte
AQAWHJUBH URWDXPTWW DXYWHUEBM
strecorde
BJFIDJHWE XUMCNFEUK ZLLFSDLFQ
dperiod

TRVWDGCKU VSENATTFK RRW.

TGAKJIEAO ZAANDGTBM
```

Note ciphertext letters "**J**, **U** and **H**" represent plaintext letters "**o**, **r** and **e**" on the first three lines of the **Period Nine** ciphertext format. A look at all other possible repeated crib letter space intervals will not yield matches of all repetitive letters. Once a ciphertext letter is identified in each Period column (1-9) it retains the same identity within the column. This allows us to place the lower case plaintext letters as shown below. Read down each nine column matrix for the plaintext.

Period Nine Columnar Format

```
123456789      123456789      123456789
TEFCB**JU**T**H**      DQPWRGWJH      HAWVXREMJ
   sh**or**t**e**       t e    e

AQAWH**JU**B**H**      URWDXPTWW      DXYWHUEBM
strec**or**d**e**                        ec  d

BJFID**J**HWE      XUMCNFEUK      ZLLFSDLFQ
dperi**o**d           s

TRVWDGCKU      VSENATTFK      RRW.

TGAKJIEAO      ZAANDGTBM
                 r    d
```

You are familiar with the K2 Keyword Alphabet in usage with an Aristocrat simple substitution cipher. The plaintext normal alphabet is on the top and the keyed ciphertext alphabet beneath. The Quagmire II Cipher uses the same K2 Keyword alphabet approach but since it is a polyalphabetic cipher type, it will have multiple keyword lines under the normal plaintext alphabet. Each of these lines represents a Period in the cipher. This Period Nine, Quagmire II cipher will have nine keyword lines.

Each keyword line contains the same keyword but begins its ciphertext line with a letter that will generate a vertical keyword under the plaintext "a" column of the **Keyword** matrix.

Let's plug in the ciphertext letters that have been identified into our **Keyword matrix**. The Period column number is shown on the left side.

```
  a b c d e f g h i j k l m n o p q r s t u v w x y z
1       B                             A
2                                J       Q
3         F                          A
4         W                          I C
5       H       B D
6                                J
7         H                          U
8         B                              T
9           H
```

Since each keyword line contains the same keyword, the ciphertext (CT) letter sequence will be the same in each line. Since CT letters B and D are 5 and 6 spaces from CT letter H on line 5, they may be placed the same distance away on any other line that H appears. **Be sure that the same space is kept between the letters.** Our keyword matrix is now:

Q-2, Keyword Matrix

```
  a b c d e f g h i j k l m n o p q r s t u v w x y z
1       B D F             U           A T         H
2                                   J     Q
3     B D F             U           A T         H
4         W                         I C
5     H         B D F             U           A T
6                                   J     Q
7         H       B D F             U           A T
8         B D F             U         A T         H
9           H         B D F           U           A T
```

Q-1, Period Nine Plaintext Updated

```
123456789     123456789     123456789
TEFCBJUTH     DQPWRGWJH     HAWVXREMJ
T eshorte     et e    e     y
AQAWHJUBH     URWDXPTWW     DXYWHUEBM
strecorde     m     y       e  ec  d
BJFIDJHWE     XUMCNFEUK     ZLLFSDLFQ
dperiod       s   m               f
TRVWDGCKU     VSENATTFK     RRW
t  e    s         w yf
TGAKJIEAO     ZAANDGTBM
t r    s        r i yd
```

Additional keyword ciphertext and plaintext generate one another. Complete each. The additional plaintext generated by adding ciphertext letters to the keyword matrix based on the same letter sequencing of each keyword line allows us to make educated assumptions of yet additional plaintext.

The second plaintext letter of the message is obviously an “h.” It is also obvious that the cipher is referencing “The shortest recorded period of time . . .” “rainy day” is prompted by the cipher’s title, Cloudburst, in ciphertext group ten and “expected” jumps out at us in group twelve. Continue to complete the plaintext and Keyword matrix until you are finished.

Quagmire Cipher Review

1. Period length is determined by finding the proper interval between repeated crib letters that will allow repeated ciphertext letters to stand for the repeated letters in the crib.

2. Each keyword matrix line contains the same keyword which generates the identical alphabetical letter sequencing in each line, causing letters sequencing to appear at like intervals.

3. When any two lines of ciphertext alphabets appear with a letter in common, the information may be combined. The alphabets are identical, simply shifted against each other.

4. An indicator key letter in the first column of the keyword matrix may form a vertical keyword.

5. The Quagmire polyalphabetic cipher allows a letter to be substituted for itself.

6. Quagmires I, II, III and IV follow the same keyword principles as simple substitution with the exception of the fourth review point above.

Period Determination

We stated that a Quagmire's period length is determined by finding the proper interval between repeated crib letters which will allow like ciphertext letters to represent the repeated letters in the crib. This is a trial and error procedure that is best concentrated in the area of five to ten Period columns for an average length cipher. Sort the text into five columns as a start, looking for a match of repeated ciphertext (CT) and plaintext (pt) letters. If no match exists for each of the repeated CT/pt letters, continue searching for the columnar Period break that produces the proper match.

The ACA and You Handbook can provide Period length assistance based on the number of ciphertext letters in a construction with guidelines that spell out ACA minimum and maximum limitations.

Each keyword matrix line contains the same keyword. This means that each of the period lines generates the same alphabetical sequencing and letters will appear at like intervals. For a Quagmire II, plaintext letters appear at the top of the matrix with the ciphertext letters below containing the keyword. An indicator key letter in the first column of the keyword matrix forms a vertical keyword.

A note on educational reading - Speed-reading of educational material is appropriate for overview purposes only. Line by line understanding is a necessary requirement of all material that we wish to permanently digest and store to memory.

Chapter Eighteen

Period Determination

There is a tendency for us to shy away from polyalphabetic cipher types which require a determination of its Period length, believing that complex mathematical formulas or a difficult factoring approach is necessary to arrive at the proper number of columns to satisfy Period determination. I hope this chapter will persuade you that the pencil and paper solvers have no need to exclude these Period determination cipher types from their solving prowess.

There are two common methods applied in the determination of the periodicity of a periodic cipher type.

Index of Coincidence

William Friedman and his wife, Elizebeth (not a typographical error, the unusual spelling chosen by her mother to avoid the nickname of Eliza) , were American cryptanalysts who made substantial contributions to cryptology and played a significant role in the decryption of enemy ciphers during World War I and II.

The Index of Coincidence developed, by William, in 1920 is based on the likelihood that any pair of letters in a message are equal to each other. The Index of Coincidence for the twenty-six letters of the English alphabet as used in typical conversation or messaging is 0.0667. This can be arrived at by visualizing the assimilation of some hundreds of letters placed in a common container in the ratio of their frequency appearance in normal text or conversation. (See *ACA and You* Handbook, General Properties of Letters, Page 14). The calculation of drawing meaningful text dialogue from a random collection of these letters is 0.0667.

Computer analysis of polyalphabetic ciphertext can expeditiously determine the probability of proper Period determination by comparing the Index of Coincidence between possible Period lengths, discerning which length most closely corresponds to the 0.0667 average Index of Coincidence of common text. Needless to point out, this approach does not lend itself to pencil and paper computation. Let's examine a more friendly paper and pencil approach to Period determination.

Kasiski Factoring System

Friedrich Kasiski was a Prussian Army Officer who rose from the ranks of an enlisted Private to that of Major in the 1860's, serving as a cryptanalyst.

In 1863, Kasiski published the book, *Die Geheimschriften und die Dechiffrirkunst* (*Secret Writing and the Art of Deciphering*), that devoted most of its pages to the solution of periodic ciphers. It was in this book that he introduced the recognition of letter patterns as a way to break periodic ciphers. He cited the length of the interval between letter repetitions as the clue to the length of a cipher's keyword or period length.

The Kasiski Factoring System is very user friendly to the pencil and paper solver and worthy of our study and attention. Those interested in the recreation of mathematics and/or the dynamics of letter frequencies upon the flow of the printed or linguistic word will take great delight in the examination of reoccurring digraph and trigraph patterns.

Factoring Process

1. Identify Repetitions
2. Indicate Positions
3. Find Differences
4. Factor the Differences
5. Tabulate Factors

Kasiski Period Determination – Short Method – Identify Digraph & Trigraph Repetitions

Digraph and trigraph (two and three letter groupings) repetitions are identified, located, assessed and computed in the same manner. Locate the position in the cipher text of each repetition, subtract the first position location from the second, factor the difference and tabulate the factors. Factoring simply refers to the process of determining what whole numbers could have been multiplied to produce a specific product – in this case that the differences of repeated digraph/trigraph position numbers.

Let's go through the process with the following cipher construction, a 2002 Period Five Gronsfeld. We will indicate the cipher's letter positions above the ciphertext to facilitate computing the number of spaces which generate (**factor) the differences.**

SO Cm, 2002 E-1 Gronsfeld. Impaired Decision Making LIFER

```
 2       8      13
FKIOK TYMSM XQIUY WHAXE DRNSI
    30        37&38        47         5 5
RLVEM SJGPY YKIUM YVBJQ JIWSE  SRBII WGZJR P.
```

Cipher Construction Positions

```
KI  2 37    MS 8 30
IU 13 38    IW 47 55
```

Find Differences

KI 37 - 2 = 35 **MS** 30 - 8 = 22
IU 38 - 13 = 25 **IW** 55 - 47 = 8

Factors

Difference	**2**	**4**	**5**	**7**	**8**	**11**
KI 35			5	7		
MS 22	2					11
IU 25			5(2)*			
IW 8	2	4			8	
Total	4	4	15	7	8	11

* Squared numbers carry a weight of two.

The factor columns represent the potential Period of the cipher. Each factor column entry is a whole divisor number for the difference entry. (KI-35 is divisible by 5 and 7.) **The factor column with the highest total will indicate the proper (factor) Period for the cipher (5).**

More Digraph Repetitions

JF Cm, 2002 E-4 Variant. Face Cards, RIG R. MORTIS

```
1  4   6               17                        33       40
ISHLU  VJFCW  FPPNW  UISYL  ERSRK  DVFKU  KOVJY  ZCYIP
VNDKC
                   59   61 (6   5)68           76 80      84
SIJVF  YLTJE   QNSMH   PKGTV   JGLUX   YQZFN  HTLRM   HWYHT
NMZZW
        97       104
NAJLV  VPVDA  JHRPK  SGSCZ.
```

Cipher Construction Positions:

```
IS  1 17   LU   4 68   VJ 6 33
VJ  6 65   VJ  33 65   PV 40 97
MH 59 80   PK  61 104  HT 76 84
```

Factors

Difference	**2**	**3**	**4**	**7**	**8**	**9**
IS 16	2		4(2)8*		8	
LU 64	2		4		8(2)*	
VJ 27		3				9

VJ 59 Prime Number – No factors in range.

VJ	32	2		4		8	
PV	57	Prime Number – No factors in range.					
MH	21		3		7		
PK	43	Prime Number – No factors in range.					
HT	8	2		4		8	
Total		8	6	20	7	40	9

*Squared numbers carry a weight of two.

The factor column with the highest total (8 = 40) will indicate the proper Period.

Chapter Nineteen

Vigenere Cipher Type

Does Chapter Eighteen constitute appropriate Young Tyro fodder? Our Tyro nomenclature and the column's dedication, "to the young at heart" should not exclude a visionary concept, one of entertaining a goal of translating cipher solving rudimentary study into a skill which can yield lifelong satisfaction and contentment, a temporary escape from real life tasks and commitments which surround us. We will continue to attempt to reduce many advanced cipher types to their simplest terms to allow us to take on a myriad of ACA cipher types.

We will now analyze a polyalphabetic cipher type that will allow us to use the Kasiski Factoring System of Period Determination discussed in the previous chapter. The Vigenère cipher was named after Blaise De Vigenère, a French diplomat and cryptographer, who surprisingly thought cryptanalysis as "a worthless cracking of the brain."

Nonetheless, the highly competitive battle of wits between cryptographers and cryptanalysts led to his design of the Vigenère Square, a 26 x 26 matrix for use in the construction of polyalphabetic (Periodic) ciphers. David Kahn refers to this square as "probably the most famous cipher system of all time." Let's examine its design and purpose as we study its features. Plaintext letters (lower case) are on the top row of the matrix with ciphertext letters (UPPER CASE) posted down the remaining twenty-six rows.

Vigenère Square

```
  abcdefghijklmnopqrstuvwxyz pt
A ABCDEFGHIJKLMNOPQRSTUVWXYZ
B BCDEFGHIJKLMNOPQRSTUVWXYZA
C CDEFGHIJKLMNOPQRSTUVWXYZAB
D DEFGHIJKLMNOPQRSTUVWXYZABC
E EFGHIJKLMNOPQRSTUVWXYSABCD
F FGHIJKLMNOPQRSTUVWXYZABCDE
G GHIJKLMNOPQRSTUVWXYZABCDEF
H HIJKLMNOPQRSTUVWXYZABCDEFG
I IJKLMNOPQRSTUVWXYZABCDEFGH
J JKLMNOPQRSTUVWXYZABCDEFGHI
K KLMNOPQRSTUVWXYZABCDEFGHIJ
L LMNOPQRSTUVWXYZABCDEFGHIJK
M MNOPQRSTUVWXYZABCDEFGHIJKL CT
N NOPQRSTUVWXYZABCDEFGHIJKLM
O OPQRSTUVWXYZABCDEFGHIJKLMN
P PQRSTUVWXYZABCDEFGHIJKLMNO
Q QRSTUVWXYZABCDEFGHIJKLMNOP
R RSTUVWXYZABCDEFGHIJKLMNOPQ
S STUVWXYZABCDEFGHIJKLMNOPQR
T TUVWXYZABCDEFGHIJKLMNOPQRS
U UVWXYZABCDEFGHIJKLMNOPQRST
V VWXYZABCDEFGHIJKLMNOPQRSTU
W WXYZABCDEFGHIJKLMNOPQRSTUV
X XYZABCDEFGHIJKLMNOPQRSTUVW
Y YZABCDEFGHIJKLMNOPQRSTUVWX
Z ZABCDEFGHIJKLMNOPQRSTUVWXY
```

A keyword whose number of letters is equal to the cipher period is used. It may consist of more than one word and unlike single substitution cipher keywords, duplicate letters are permitted to be repeated. We will use TYROGRAMS as our keyword(s) to encipher our plaintext message with the Key Square.

```
    TYR OG RAMSTYRO G RAMSTYRO
Pt: how to encipher a Vigenere
CT: AMN HU VNOAIFVF G MISWGCIS
```

To obtain the ciphertext, read down the first column on the left until you reach the key letter "T." Read across the row until you reach the column of the first plaintext letter "h." The ciphertext letter "A" is located at the intersection of this row and column. Repeat this procedure for each letter of the plaintext to determine the ciphertext. Become familiar with this process. Did you notice that the Vigenère allows a plaintext letter to stand for itself? (Self-encryption)

Let's review the Vigenère Cipher usage with a Cm cipher. Notice the construction five letter groupings which is standard format for the Vigenere cipher construction.

SO2004 Cm. Vigenère. Good advice. ERNO

```
GLSTO EBYUZ YZZTU TUDJS OZWSF KSUUN FEHUT OTNCZ
Buyno twhat youca nuseb utwha tyouc annot dowit

HZZKQ NAEDF OJOYT KHKEO NJXKA CFKUT YAWZW KCLYF.
houtw hatyo udono tneed isdea ratan ypric ecato.
```

Cryptanalysis development begins with an understanding of a cipher's origin or construction process. Let's see how the Vigenère Square is used to develop the ciphertext for the plaintext that appears beneath it by referring to the construction process appearing below.

The constructor chose the keyword, **FRUGAL**, as a basis for a period six cipher. The Period six matrix that appears further down the text will allow you to refer to the Vigenère Square to follow the relationship of the ciphertext to the plaintext. The encipherment process is begun by writing the plaintext horizontally beneath the chosen keyword. All letters in the first column are then enciphered using **F** as a key, the second column using **R** as a key, the third using **U** and so on. The ciphertext generated by the key letters of each column is beneath the plaintext.

A look at the Vigenère Square key will reveal how each column key letter in a keyword is used to generate ciphertext for the plaintext. Run your finger across the ciphertext of row **F** for the first column key letter **F** until you arrive at plaintext letter **b** (top row). You will find ciphertext **G**. It becomes the first letter of the ciphertext. Second column key letter **R** in row **R** will yield ciphertext **L** for plaintext "**u**." Third column key **U** reveals ciphertext **S** for plaintext **y**. Continue searching for the remainder of the ciphertext letters to see if you can duplicate the ciphertext in the original Vigenère construction shown above.

Construction Process

```
F R U G A L F R U G A L F R U G A L F R U G A L F R U G A L
B u y n o t w h a t y o u c a n u s e b u t w h a t y o u c

F R U G A L F R U G A L F R U G A L F R U G A L F R U G A L
a n n o t d o w i t h o u t w h a t y o u d o n o t n e e d

F R U G A L F R U G A L F R U G A L F R U G A L F R U G A L
i s d e a r a t a n y p r i c e c a t o.
```

Cryptanalysis

Of course, armed with the constructor's key, we are not yet practicing the art of cryptanalysis. Read on for some insight in how to attack this cipher type without the key.

The Vigenère Cipher, reduced to its simplest terms, is a series of simple substitution ciphers. Each period or column is a single substitution cipher in itself. Its complexity is two-fold in

that its period must be determined (see Chapter Eighteen) and its single substitution columns are all short reads with no intelligible message within the column.

A shortcut to period determination but not always purely definable can be found with a check into *The ACA & You* Handbook to determine the required length of the Vigenère Cipher type. It is stated as having rows ten to fifteen lines deep. This standard would limit the cipher that follows (75 letters) to a Period of five through seven. We will save you the Period determination work on this cipher and define it as Period 5.

V-1. Vigenère. Common word. LIONEL

```
MOINS   KKXYI   BZSEI  HMXYI   FVWKY

LLHNS   KKWZR   MOIVR  ZSMJL   EHRXY

TNIRR   WIIXM   GZQRR   RZIEX  XUGVW.
```

The five letter ciphertext grouping is always used in a Vigenère cipher construction regardless of period length.

You will remember that a Vigenère Cipher is written in horizontally across its Period length, so we will insert the ciphertext horizontally over five column lengths.

Treat each matrix column as a single substitution cipher. You need to find the key letter for each column that will produce the most high frequency letters (**senorita**) in that column. The five column keys will spell a keyword.

All of our learned simple substitution strategies can be applied to each column's solutions. Look for repeated ciphertext letters within each column to represent high frequency letters. We have highlighted highly repeated ciphertext letters as likely "**senoritas."**

Might there be a letter "e" among them?

Vigenère Matrix

```
1 2 3 4 5
_ _ _ _ _  (Keyword)
M O I N S
K K X Y I
B Z S E I
H M X Y I
F V W K Y
L L H N S
K K W Z R
M O I V R
Z S M J L
```

E H R X Y
T N **I** R **R**
W I **I** X M
G **Z** Q R **R**
R **Z** **I** E X
X U G V W

Check the Vigenère Square to determine how the assignment of **senorita** letters to high frequency ciphertext letters impact each column letter decipherment. Those letters generating the most high frequency letters and the least low frequency letters in a column will best create word formations when grouped together with the adjacent columns.

Each column must be treated as a separate single substitution cipher and is independent of the other columns. Ciphertext letter I in column three may or may not be the same plaintext letter as ciphertext letter I in column five, depending upon the key letter of each column. Keep in mind the most frequently use trigraph (three letters) in the English language and the most frequent opening trigraph found in much text.

Become highly aware and adept with this Vigenère Square and cipher system that David Kahn exclaims as "the most famous cipher system of all time." Future study will reveal how cryptographers worked at modifying this cipher to stay one step ahead of the cryptanalysts.

It would be unfair to leave our talk on the Vigenère Cipher without a word or two on a means to limit the labor intensity of peering through the rows and columns of the 26 x 26 Vigenère Square. A slide device neatly fits the Square's intent and is a useful aid.

Vigenère Slide

The slide is a simply crafted device that allows the alignment of the total 26 ciphertext and plaintext letters of the Vigenère Square with a very simple apparatus that looks like this:

(pt)
abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz
DEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABC
(CT)

It is very reminiscent in likeness to the Caesar Shift, and in fact, allows us to make mono-alphabetic Caesar Shift recovery. The chief distinction of the Vigenère Cipher is that it is polyalphabetic in nature and requires the need to use more than one alphabet per cipher. The Vigenère Slide allows us to easily meet this requirement while allowing a shift in either direction. Construct your slide so the plaintext **top line is stationary and the cipher- text bottom line is movable.**

Let's use the slide in a review of the solving process of the Vigenère Cipher that appeared in the **SO200404 Cm** by **ERNO** which appears earlier in this chapter. This cipher has been identified as a period six type and requires us to recover a six-letter keyword.

SO2004 Cm. Vigenère Cipher. Good advice. ERNO

GLSTO EBYUZ YZZTU TUDJS OZWSF KSUUN

FEHUT OTNCZ HZZKQ NAEDF OJOYT KHKED

NJXKA CFKUT YAWZW KCLYF.

We post it horizontally to six columns.

Key ? ? ? ? ? ? (Keyword)

```
G L S T O E
B Y U Z Y Z
Z T U T U D
J S O Z W S
F K S U U N
F E H U T O
T N C Z H Z
Z K Q N A E
D F O J O Y
T K H K E D
N J X K A C
F K U T Y A
W Z W K C L
Y F
```

Use your slide to perform a column by column search for the high frequency letters "**senorita"** and to recover the keyword. Each column has its unique key letter that identifies its plaintext. The Vigenère slide will allow you to analyze each column of text with a different key letters. Each key letter will generate a different set of plaintext letters. Find the key letter for each column by determining which key letter generates the highest frequency plaintext letters and the least fewest frequency plaintext letters.

Align a ciphertext letter on the bottom of the slide under plaintext "a." The letter appearing directly above the ciphertext letter is its corresponding plaintext letter. The ciphertext letter aligned below the plaintext letter "a" becomes the key letter for the column.

V-2. Vigenere. High Frequency.

OIPOE ZXMWQ OSIBA EESFH LAXDD

IGHVZ LIFXU SVVZL AWUZR VZUSK

RKZBA TZIJC ILLEF SEWKI MHSXH

GVATL DSSHY MVOEQ BBFVX S.

The Universal PhoeBee Cipher Slide

The PhoeBee circular cipher slide was developed in 1998 by Honeybee and Phoenix. It can be used as a cipher solving slide for all of the Vigenère type ciphers along with the Porta and Portax cipher types. This slide can be ordered from Honeybee. See the *For Sale* section on page fourteen of the *Cm*.

Beaufort, Gronsfeld, Variant Ciphers

As cryptanalysts became able to solve the Vigenère Cipher, spinoff ciphers appeared to challenge their skill. The Beaufort, Gronsfeld and Variant Cipher are variations of the polyalphabetic Vigenère Cipher that we should identify and become familiar with their solving process.

The history of the battle of wits between the cryptographer and the cryptanalyst is an interesting study in the creativity of mankind. Each time a cipher type's security is breeched, another type arises to take its place. This is true of the Vigenère cipher.

When the Vigenère Square was first developed as the basis of the polyalphabetic cipher, it appeared to be the cipher to end the need of future cipher types. But, alas, it became recognizable and decipherable after repeated use. The need to add to its complexity became a necessity.

Enter, the Beaufort, Gronsfeld and Variant Ciphers that generated slight variations upon the Vigenère in order to make decipherment more complex. The four cipher slides are shown below. We have noted their differences. Remember that these slides are used only to convert ciphertext letters to plaintext letters. Each column's key letter dictates the positioning of the slide. Let's compare the Vigenère slide to its three spin-off replicas.

Vigenère Slide - pt = plaintext, CT = CIPHERTEXT

```
(Pt)    abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz
(CT)    DEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABC
```

The ciphertext letter on the bottom of the slide aligned under plaintext "a" represents the column key letter. The letter that appears directly above each ciphertext letter is the plaintext.

Variant Slide

The only difference from the Vigenère is that the column key letter appears in the plaintext alphabet below the A of the ciphertext alphabet that we place at the top of the slide. Remember that each column key letter appears directly over the plaintext slide letter "a." Use the plaintext start beneath the slide to find the keyword and complete the cipher.

(CT) XYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVW
(Pt) abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

MJ2008 E-2. Variant. Man vs. machine. (QILECHA) DANEEL

```
YMQFV XRHTX PQGLM UARYD UVQQB ATHST TGKBF GMAGL CTXVR EBATH
Parto fthei nhuma nityo fthe

CTTCV UKODV YPABB GMMMP DGPKX CIBYN AAZJY XIKBO NYWDC TTAAQ

AMQZL GSPPE JEHYV N.
```

Beaufort Slide

The Beaufort cipher simply reverses the ciphertext alphabet beneath the plaintext alphabet to create a reciprocal encipherment. W = a or a = W, so it does not really matter which alphabet is labeled plaintext or ciphertext. We will label the top of the slide as plaintext. Find the keyword of the cipher below with its plaintext beginning and complete the cipher.

(Pt) abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz
(CT) ZYXWVUTSRQPONMLKJIHGFEDCBAZYXWVUTSRQPONMLKJIHGFEDCBA

JF 2008 E-2. Beaufort. Shooting off your mouth. (MJYYWB) DANEEL

```
NFNIE YLBHT UUUBB UECXW SSRTU UYKUJ FIEQZ YQQEW BAQQN GHWEL
Speak wheny arean gryan
YJXDQ XBDAE IDOMT TICTB RCNHG QBDQ.
```

Gronsfeld Slide

The Gronsfeld Cipher uses key numbers from 0 to 9 instead of letters. The key number sequence does not generally come from a keyword. Numbers may be repeated since any number of columns requiring a key number may be used. Each ciphertext letter is displaced to the left of the plaintext by the number of letters equal to the key number.

Four displacements are shown.

```
(Pt)  abcdefghijklmnopqrstuvwxyz
(CT1) BCDEFGHIJKLMNOPQRSTUVWXYZABCD..
(CT2) CDEFGHIJKLMNOPQRSTUVWXYZABCDE..
(CT3) DEFGHIJKLMNOPQRSTUVWXYZABCDEF..
(CT4) EFGHIJKLMNOPQRSTUVWXYZABCDEFG..
```

These four slide placements each reflect a period displacement. CT1 = a displacement of one. CT2 = a displacement of two. CT3 = a displacement of three. CT 4 = a displacement of four. Displacements up to nine can be used. Each column will contain its own number of displacements. Key # displacements are tried for each column to determine the key # that will create the most high frequency letters. Determine the key numbers used in the cipher below to complete the plaintext.

MA 2008 E-3. Gronsfeld. Thinker rethought common wisdom. RIG R MORTIS

```
XUHUW LRLWV URWPL RLUWZ CITLN IQWBN UBVKN UNKJK ICQXU TQVOI
Plato didno jogdi etort ake

LAIMA JQMHU BMWBR VOBWQ MJSUP QBBQL HZMJB NZUPQ WLAHO KMCWU

PGM.
```

Chapter Twenty

Cryptarithms

Cryptarithms are mathematical ciphers or puzzles where letters are used in place of numbers. One letter is used to represent one and only one number. Their use is more for a mathematical solving exercise of enjoyment rather than secret message communication.

Our *Cm* constructions often use a keyword or phrase to key the problem. It has the same number of letters as the base of the numbering system. Ten letters are used to represent our normal decimal system of ten numbers. The keyword letter order is indicated by 0-9, 9-0, 0-1 or 1-0. This will become clearer as we work through a construction. Let's begin with an addition problem in a cryptarithm construction format. Problems are published in line form to save space in the *Cm* column.

Addition. (Two words, 0-9 Key Order.)

SONFTS + FUYPTC = RTTYCUS

Conventional addition format.

```
  SONFTS
+ FUYPTC
 RTTYCUS
```

```
Key Order _ _ _ _ _ _ _ _ _ _
          0 1 2 3 4 5 6 7 8 9
```

Give Aways

Let's look for the letters that are given away in the problem. R = 1 as a left hand digit carry in the sum. C = 0 since S + C = S. Because zero and nine are the only two numbers possible to produce like numbers in a same column and N + Y = Y, N must equal 9.

```
Our key is now: C R _ _ _ _ _ _ _ N
                0 1 2 3 4 5 6 7 8 9
```

Keep in mind that two words form this key. At this point anagramming can help in the key recovery and mathematical solution to the cipher.

We can rule out the letters FSPTY being the number eight in the key as each are unlikely to precede the letter N, our number nine value. The letters O or U must be equal to eight. Since T + T = eight in column four of the addition, it appears that U will equal 8 and T will equal 4. Our updated key:

```
C R _ _ T _ _ _ U N
0 1 2 3 4 5 6 7 8 9
```

We know that the sum of column three in our problem ends in zero. The only two numbers remaining with a sum of zero are 7 (F) and 3 (P). Our key is now:

```
C R _ P T _ _ F U N
0 1 2 3 4 5 6 7 8 9
```

It is now fairly simple to locate the three remaining letters: `C R Y P T O S F U N`
`0 1 2 3 4 5 6 7 8 9`

A check of the mathematical values will confirm that we have the correct key.

```
  SONFTS
  659746
  FUYPTC
+ 782340
 RTTYCUS
 1442086
```

Apply these same principles to the following subtraction problem:

C-1. Subtraction. (Two words, 1-0)

NUBSRMU – JOEOSY = MENRRU

Let's continue our cryptarithm discourse with a discussion of the process of solving multiplication and division construction types. Remember, each letter that appears in the cryptarithm is used to represent one number and one number only. Let's begin with a multiplication problem.

C-1. Multiplication. (Two words, 9-0)

FSNI * TNIS = NGPPIS; + GNORS; + FSHI; = TGTOYPIS

We write this in multiplication order. The first point we notice is a four-digit multiplicand with only three product line in the problem. This alerts us that a zero is somewhere in the multiplicand.

```
  FSNI
x TNIS
 NGPPIS
 GNORS
 FSNI
TGTOYPIS
```

The zero (S) becomes obvious as we see its placement in the problem. Since the third product line has the same letters as the multiplicand, T must equal 1. In our addition, P + S = P, confirms that S must equal zero. G + F = TG on the bottom line, F must equal 9. Let's put each of these letters into our 9-0 key.

```
Key order: F _ _ _ _ _ _ T S
           9 8 7 6 5 4 3 2 1 0
```

Let's look at I x I = I in our first multiplying activity. There are only three numbers that are multiplied by its same number that will generate the identical last digit, 1, 5 and 6. The digit, 1, has been already used. Let's focus on the 5 and 6 digits.

We need a number that will generate two identical digits when multiplied by the next number(s) in our multiplicand. Work through the multiplication of the number, 5, through all of the yet to be used digits in our key for the value of N. (We already know that the letter after N in the multiplicand is zero (S). You will find no possible combination of 5 x N and S that will generate identical digits in the first product line. But, 6 x 5 (N) and zero (S) will yield 33. We have added three more letters to our key.

```
Key order: F _ _ I N _ P _ T S
           9 8 7 6 5 4 3 2 1 0
```

Anagramming will complete the key as we only have four remaining letters to be placed, R, Y, G and O. Check the arithmetic of your solution.

C-2. . Division. (Two words, 1-0)

SOUTHERN / STRIFE = FRS; - STRIFE = IUETRRN; - IORFRHR = FEEUNN.

We write this in a natural division order and notice a three-digit divisor with only two lines of subtraction. This alerts us that a zero is somewhere in the divisor.

```
         _____FRS
STRIFE|SOUTHERN
       STRIFE
        IUETRRN
        IORFRHR
         FEEUNN
```

The zero jumps out at us in the first line of subtraction. E - E = R can only equal zero. An identical divisor and multiplicand on the first line avows the first dividend digit as 1. The fifth column of the second subtraction, R - R = U must be a nine, for zero is spoken for. We have two of the values for the second column of the second subtraction, leaving letter 0 as 8. Continue the logic to complete the solution.

```
F _ _ _ _ _ _ O U R
1 2 3 4 5 6 7 8 9 0
```

We remember from our grammar school mathematics' primer that a number's square results when we multiply it by itself. Conversely, we can define a number's square root as the number multiplied by itself, with its difference added to the product, is equal to the original number. We'll reach into the ACA *Cm* archives to explain the principles of square root procedures. Our *Cryptogram* Ye-Ed at the time, PHOENIX, presented a nine-step presentation of the process in the SO '94 *Cm* that we will use as the foundation for our discourse on the square root cryptarithm.

First of all, keep in mind all of the tips that we have reviewed to identify the numbers, one, nine and zero. Also, be on the alert for digits squared that generate the same last digit in the squares. (C-1) In order for one to be alert to all of the tip aids in a square root problem, an understanding of the square root mathematical process is necessary

Square Root Procedures by PHOENIX, *The Cryptogram,* SO 1994

To find the square root of a number:

1) Mark off the number in groups of two figures in both directions from the decimal point. Add a zero to the last decimal group if necessary.

2) Determine the greatest perfect square of the leftmost group and write it below. Write its square root above the group.

3) Subtract the perfect square from the leftmost group and bring down the next group adjacent to the remainder to form a partial dividend.

4) Multiply the root already found by 20 for a trial divisor. Divide it in to the dividend. The whole number quotient is the next digit of the root being determined.

5) Add the last digit to the trial divisor to form a complete divisor. Multiply it by the last root digit and write the product under the dividend.

6) Subtract this product from the dividend; bring down the next group to form a new dividend.

7) Reiterate steps 4 through 6 until the remainder is zero, or until as many places as needed have been determined.

8) Add zeroes to the decimal part as needed. The decimal of the root goes directly above the decimal in the number.

9) If at any time the partial divisor is greater than the first part of the dividend, write a zero as the corresponding figure of the root. Draw down the next group of figures and proceed as before.

We will use these square root procedures to find the square root of 526930.81.

```
      7  2  5 .9
    v52'69'30.81'
     49
      369
142   284
       8530
1445   7225
       130581
14509  130581
```

Back to the square root definition – 7 squared, plus its remainder, 3, represents the square root of 52. Follow this problem's mathematics to its conclusion.

Let's try a square root without the given numbers.

SR-1. Square root cryptarithm. (Two words, 0-1)

```
   U V
 V RU'ER
   DU
   SFER
    VGA
    DFI
```

0 9 8 7 6 5 4 3 2 1

Do you recognize that the letters S and F are giveaways? Other known quantities: U squared generates a final U digit; R is one greater than D and E is one greater than G. (Why?)
We'll continue our cryptarithm cipher discussion with a look at the approach of solving a cube root problem. Before we can apply any of the cryptic solution principles we have learned to a cube root, we must be fully aware of the mathematical procedure of solving one. Once again we reach back to PHOENIX's discussion of the methodology of root solutions in the SO 1994 *Cm*, this time as it pertains to a cube root

.

To Find the Cube Root of a Number:

1) Mark off the number in groups of 3 figures in both directions from the decimal point. Add zeroes to the last decimal group if necessary.
2) Determine the greatest perfect cube of the leftmost group and write it below; write the cube root above the group.
3) Subtract the greatest perfect cube from the leftmost group and bring down the next group adjacent to the remainder to form a partial dividend.
4) Multiply the root (squared) already found by 300. Use this number to divide the new dividend. The whole number part of the quotient is a good guess for the next root number. If this trial root generates a number larger than the existing dividend, use the possible root minus 1. Note: the trial root in one part of the example was too large.
5) Add 30 times the product of the root already found and the trial figure, and the square of the trial figure, to the partial divisor. Multiply it by the last root digit and write the product under the dividend.
6) Subtract this product from the dividend. Bring down the next group to form a new dividend.
7) Reiterate steps 4 through 6 until the remainder is zero, or until as many places as needed have been determined.
8) Add zeroes to the decimal part as needed. The decimal of the root goes directly above the decimal of the #.
9) If the partial divisor is greater than the first part of the dividend, write a zero as the corresponding figure of the root. Draw down the next group and proceed as before.

Cube Root Example.

```
                          4   2   7    .9
                    3V78'347'809' .639
                      64
                      14 347

  300x42= 4800
   30x4x2= 240
         2
        2 =  4
_______________
          5044
             x2=     10 088
                      4 259 809
300x422=  529200
```

```
   30x42x7=  8820
          2
         7=    49
           538069
               x7=   3 766 483
                       493 326 639
300x4272=54698700
 30x427x9= 115290
         2
        9=      81
          54814071
               x9=     493 326 639
```

CR-1. Cube root Cryptarithm. (Three words, 1-0)

```
    Y   L
  _____
V RY'OSD
  AY
  OP OSD
  OP PSS
     UE
```

__	__	__	__	__	__	__	__	__	__
1	2	3	4	5	6	7	8	9	0

Go through steps one through nine. Only the numbers 3 and 4 can generate a two-digit cube for the first quotient and only one of those numbers will yield the same last digit as the quotient. Y minus Y tells us the value of P. Steps four and five will provide the value for L and we are well on our way to solving another cipher type that we might have ignored in the past.

We will continue our discussions on the cryptarithm arithmetic cipher problems with a look at a couple of types that we might tend to avoid if we were not aware of their potential simplicity.

Factorial Equation cons usually enjoy a C-Special ranking in the cryptarithm column but may not be as hard as their placement in the column suggests. Here is an opportunity for cipher solving success rather than cipher retreat.

Factorial Equations.

Factorial Equation constructions usually enjoy a C-Special ranking in the cryptarithm column but may not be as hard as their placement in the column suggests. Here is an opportunity for cipher solving success rather than cipher solving retreat.

Webster defines “factorial” as “the product of a series of consecutive positive integers from 1 to a given number.” Thus, factorial four (written 4!) = 1 x 2 x 3 x 4 = 24. Let’s apply this relatively simple math formula to a SO2004 *Cm* Cryptarithm construction.

SO 2004 Factorial. (Three words, 0-1) **APEX DX**

A! + D! = EDD A! – N! = AFF
N! + W! = OWW (I! / A!) – TV = DAA

Our usually devious constructor, APEX DX, has been kind by providing us with four equation results that end with identical cipher letters, DD, FF, WW and AA. This leads to four equations ending with identical numbers. Searching for a factorial that will lead us to a three digit solution ending in identical numbers produces 6! = 1 x 2 x 3 x 4 x 5 x 6 = 720 or 5! = 1 x 2 x 3 x 4 x 5 = 120. We now search for a D! to add to 720 or 120 that will produce a three digit total ending in identical numbers. Both 2! (1 x 2 = 2) and 4! (1 x 2 x 3 x 4 = 24) fill this bill. This provides us with sums of 722, 744, 120 or 144 as our first possibilities.

Moving on to the second equation, we will find that 5! = 1 x 2 x 3 x 4 x 5 = 120 is the only factorial that will keep the three digit solution and two identical ending digits in equation two when subtracting N1 factorial. Thus A! (720) – N! (120) = 600 is the solution for equation two and A! (720) + D! (1 x 2 x 3 x 4 = 24) = 744 is our solution for equation one.

Partial solution left for you to complete.

```
F     E A N D
0 9 8 7 6 5 4 3 2 1
```

Logarithms.

Webster defines a logarithm as the exponent (power) to the base that a specific number must be raised to produce a given number.

ND2004 *Cm* Logarithm. (Three words, 0-9) **MARSHEN**

INASO = I DSTAF = S
Log O Log YET

This logarithm is stating that the Log of digit “O” = “I” and will produce the number INASO. We need only to run through all single digit numbers (representing “O”) to determine what power will produce the number INASO. Keep in mind that INASO’s first digit (I) and the power (I) must be the same number. We will try a couple of digits below, leaving the correct digit for you to find. Four, to the seventh power = 4 x 4 x 4 x 4 x 4 x 4 x 4 = 16384. The first digit (1) does not match the power (7). Six, to the sixth power = 6 x 6 x 6 x 6 x 6 x 6 = 46656. This digit has a pattern not present in the digit lettered INASO

Will the digit, 5, provide the charm? The answer to this first logarithm will allow you to place five of the ten key letter positions and put you well on route to the final solution.

__	__	__	__	__	0 ?	__	__	__	__
0	1	2	3	4	5	6	7	8	9

C-3. Addition. (Two words, 0-9)

GOEATG + AMYPTC = RTTYCMG

C-4. Subtraction. (One word, 1-0)

LUBJRMU - ACECJK = MELRRU

C-5. Division. (Two words, 0-1)

REOTH / RUO = GF; - IGF = YUH; - FIU = OY

C-6. Multiplication. (Two words, 9-0)

MPE * SRT = ITPE; + OUOE + MPE = SOLUPE

C-7. Addition. (One word, 0-9)

GOLINGER + BYLONGER = YOOLNOGH

Chapter Twenty-One

Affine & Hill Cipher Types

The Affine (Linear Substitution Encryption) and Hill (Lester Hill, U.S. mathematician) Cipher techniques manipulate numbers in ciphertext with complicated formulae base to disguise message plaintext over and above the simple substitution process. Numbers have been commonly used to encipher plaintext but the Affine and Hill Ciphers use mathematical formulae and logic to disguise the plaintext further through a series of mathematical equations.

The Affine Linear Substitution Encryption in its most basic application form may first apply addition and then multiplication to its plaintext message. To convert the plaintext letter “C” by this method, 5 might be added to the numerical value of the letter (C = 3; 3 + 5 = 8) and that sum multiplied by some other constant, such as 5 (5 x 8 = 40). The resulting cipher

letter is N (40 modulo* 26 = 14 – N). (Encyclopedia of Cryptology, David E. Newton, Instructional Horizons Incorporated, 1997.)

In mathematics, modular arithmetic (sometimes called clock arithmetic) is a system of arithmetic for integers, where numbers "wrap around" after they reach a certain value—the modulus. A familiar use of modular arithmetic is in the 12-hour clock, in which the day is divided into two 12-hour periods. If the time is 7:00 now, then 8 hours later it will be 3:00. Usual addition would suggest that the later time should be 7 + 8 = 15, but this is not the answer because clock time "wraps around" every 12 hours; in 12-hour time, there is no "15 o'clock". Mathematics would refer to 15 o'clock as mod (12) 3.

Likewise, when working with enciphering the English 26 letter alphabet there is no 27th digit bur mod (26) 1.

The Hill Cipher suggests that a series of plaintext letters can be converted into ciphertext with the use of four simultaneous linear equations where variables are raised to no power higher than the first and all variables have the same values.

Needless to relate, such complex base formulae do not allow for the ease of plaintext encryption and certainly will not relate to the desire of making elementary classroom mathematics fun and games. But they do provide a path to a simplistic approach of making secret messaging through elementary mathematics fun while achieving the primary objective of simultaneously educating the student. Supported by the Affine and Hill Cipher premises and willed with the desire to make mathematics fun, we set out on a journey to make math fun for our younger solvers as they work at uncovering secret messages and learn to embrace those dreaded multiplication tables.

We will begin this chapter with two numerical ciphers, dissimilar to the usual ACA cipher types that we are used to seeing in *The Cryptogram.* They are cipher types from our *Young Tyros Junior Newsletter* which we use to make mathematics fun for our younger solvers. Determine what mathematical process must be used with the following ciphertext numbers so that each represents a letter of the alphabet with a value from 1 to 26. Keep in mind that the mathematics base has been constructed for younger elementary students, so keep the thought stream simple.

A&H-1. Turkey Day. LIONEL

```
 87  77 749  53  10  68  38 577  25 63 859
 72 563  61  22  01 889  10  66  75 96 778
 41 378  10  67  50  99  36  21  01 33  10
 94  81  84  36  05 757 775  18 884 40  96
788  95 785  78  04  36  86  68 113 99  10
569 668  53  32 775  10 382  41  85 96  58
 41  77 839  71  10  66  24 758  81 94  14.
```

A&H-2. Bewhiskered Santa. LIONEL

```
838 01  77 749 10 883 995 53 45 775
 83 32  99 676 68  14  41 22 95  96 668
 99 63  85  58 72  59  62 23 65  45 991
199 50 919  83 72  31 883 86 87 992
299 71  05 887 27  67  76 63 59  11 777
774 58  10 775 53  01 877 23.
```

Use the key below to decipher the mathematical computations which follow it.

```
Key     a b c d e f g h i j k l m n o p q r s t u v w x y z
        4 8 1 1 2 2 2 3 3 4 4 4 5 5 6 6 6 7 7 8 8 9 9 9 9 9
            2  6 0 4 8 2 6 0 4 8 2 6 0 4 8 0 2 1 4 0 4 6 8 9
```

A&H-3. (12x3-24)(8x9-2)(12x8+2)(8x8)(9x8+9)(12x5)(7x4)(8x7+14)(36-32)(26x2)

A&H-4. (X=2+2)(X=52-4)(X=7x4)(X-5=15)(X-2=6)(X=10x7)(X+15=19)

Let's use our Affine & Hill Cipher discussion as an opportunity to introduce fractions into our ciphering activity.

Cracking the Fraction Code

Fractions, like the multiplication tables, tend to scare the "bejeebies" (spell check will have its own wits "bejeebied" with this word) out of elementary student's first time exposure to this part of their mathematics lessons but I have found the following explanation of fractions, one with which the first time fraction student is able to relate:

$$\frac{1}{4}$$

The bottom number of a fraction tells you how many equal pieces there are in the whole object. The top number tells you how many pieces of the whole object that you are thinking about. Let us suppose that you receive ¼ of a pie. The bottom number tells you that there were four equal pieces in the pie. The top number tells you that you received one of those four equal pieces.

Exercises

FR1. A pizza has eight slices. You eat three of the pieces. What fraction did you eat?
FR2. An apple is cut in two parts. You eat one part of the apple. What apple fraction did you eat?
FR3. Since it is your birthday, your mother has promised you two pieces of your birthday cake. The cake has eleven pieces. What fraction of the cake will you receive?

Let’s have some fractioning ciphering fun.

Key:

a	b	c	d	e	f	g	h	i	k	l	n	o	r	s	t	u	w
1/4	2/4	3/4	1/5	2/5	3/5	4/5	1/6	2/6	3/6	4/6	5/6	1/6	2/8	3/8	4/8	5/8	6/8

FR4. Pizza Pieces Cipher

Determine the fraction, the letter and solve the message.

PIZZA PIECES

Your Share	**Whole**	**Fraction**	**Letter**
6	8		
1	6		
1	4		
4	8		
1	6		
1	4		
2	8		
3	5		
1	8		
5	8		
2	8		
6	8		
1	6		
2	5		
2	5		
4	6		
3	8		
1	4		
5	6		
1	5		
3	5		
4	6		
2	6		
2	5		

3	8
1	4
4	5
1	4
2	8
2	4
1	4
4	5
2	5
4	8
2	8
5	8
3	4
3	6

You're thinking that this is an over simplification and huge distance from the Affine & Hill Ciphers concept and objectives for someone outside of the realm of elementary school mathematics. You wish for a better example of an actual Affine Cipher Linear Encryption Process. Be careful what you wish for. Far be it from us to leave the reader wanting more and receiving less. We will leave you with the task of constructing an Affine Cipher key based on the Affine Linear Substitution Encryption process described in paragraph two of this chapter. Using **5** as your addition and multiplication constant determine the ciphertext for the 26 letters of the alphabet to provide an enciphering key for the Affine Linear Encryption Process.

A&H 5. Affine Linear Substitution Encryption

We will start you out with plaintext letters "a" thru "d" – You complete the key.

```
Pt    a b c d e f g h i j k l m n o p q r s t u v w x y z
CT    D I N S
```

Use this key to decipher the following cipher.

A&H-6. Incarceration.

UMX JVKPU AKRPVQ RP D NGVPXS LRQS.

Chapter Twenty-Two

Fractionated Ciphers

Fractionated Morse Cipher

A fractionated cipher is one where a plaintext letter is enciphered over two or more ciphertext letters. The process will become clearer as we discuss the encipherment process. As we have stated many times in the past, the best learning technique and starting point in developing a comfort level with the solving of any cipher type is to become aware of its encipherment process. We will begin our study of the fractionated cipher with a look at one of our favorite ciphers, the Fractionated Morse Cipher.

The Fractionated Morse Cipher contains most all of the fascinating elements of the solving process, including crib placement and keyword recovery, while providing us with the opportunity to become familiar with the use of the Morse Code system and its interaction with enciphered message plaintext.

Morse Code

The Morse Code was developed in the early 1840's by Samuel F. B. Morse for use with his electromagnetic telegraph system. Although it was not designed as a secret messaging system, cryptographers quickly developed means to incorporate its design and contents into a system of secret messaging. The Fractionated Morse cipher is one example of such efforts. The Morse Code letters, numbers and punctuation can all be found in the Appendix of *The ACA and You* Handbook. Although this ACA periodical makes the claim of "not intending to be a solve book" its pages reflect volumes upon the enciphering process. Understanding this process remains a fundamentally sound approach into the unraveling of ciphertext construction into that of clear or plaintext.

Fractionated Morse Encipherment

Each plaintext letter is converted to Morse Code using "X" between letters and "XX" between words. "XXX" does not exist. Punctuation is optional but is not normally used for Cm construction purposes. "Solving is fun" becomes: •••x---x•-••x•••–x••x-•x --.xx••x•••xx••-•x••–x-•xx. Before proceeding with the encipherment we need to create a key alphabet which will give us the ciphertext substitutions for the Morse Code plaintext.

The Fractionated Morse key alphabet is set up in three tiers with a series of dots, dashes and x's. The first row is composed of nine dots, nine dashes and eight x's to fill the 26 letter alphabet. The second row is composed of three dots, thee dashes and three x's until the final two x's. The third row is a series of dot, dash and x's until the final dot and dash.

A picture is worth a thousand words. We will use "CIPHER" to set up our key alphabet which now appears over a fixed series of dots, dashes, and x's.

```
C I P H E R A B D F G J K L M N O Q S T U V W X Y Z
• • • • • • • • • – – – – – – – – – x x x x x x x x
• • • – – – x x x • • • – – – x x x • • • – – – x x
• – x • – x • – x • – x • – x • – x • – x • – x • –
```

The keyword or key phrase can start at any point in the series of Morse Code symbols. The series of dots, dashes and x's beneath the keyed alphabet remain constant from encipherment to encipherment. The plaintext (Solving is fun) coded series of dots, dashes and x's, now in vertical groups of three, transformed into ciphertext based on the above key looks like this:

```
pt • x – – x • • – – x • • x – • x x
   • – x • • – • • – x x • • • • – x
   • – • • • x x x • • • x • x – •
CT C W N F S R P J K Y A P S J I V
```

CIPHERTEXT CONSTRUCTION: CWNFS RPJKY APSJI V

The fractionation process is now evident. Twelve plaintext letters (Solving is fun) have been enciphered into sixteen ciphertext letters. Becoming familiar with this encipherment process is the first step in its solving process. Our next column will address the decipherment of the Fractionated Morse Cipher.

We have defined the Fractionated Morse Cipher as the process of spreading a plaintext letter across two or more ciphertext letters through the use of a series of Morse Code dots and dashes complemented with x's used as letter and word separators. (A single x is used as a letter separator while two x's, 'xx' indicate a word separation.) The above encipherment process defines the three-tier cipher construction process. Let's begin the solving process of a typical *Cm* Fractionated Morse Cipher type.

MJ2000. E-13. Terse codes. (frequency) PHOENIX

LMUTR DNRXG LIUQL RARVR GPEDH RHLTD RQRDF THARW WLHMU
80 92
XJZRD RRIVY MQQBG AKFUQ RBOQD VBLMU QHSUI LCAAS **U**KWLS

YFUNU SQBRH XMDZT DNEYL RIZHO QVDTL RMQWA DAAHX MDYRM

AKSXD PRMQW ADLFQ BNKXM DZNKM XVHJW WWNBB DXLTD R.

Crib Placement:

We assign the appropriate Morse Code symbols to the crib word "frequency" with a single x to indicate a separation between letters and a double xx to indicate word dividers. Thus, a

double xx must appear before the f and after the y of the crib “frequency.” Since the fractionated process can spread a plaintext letter across more than one ciphertext letter, we must examine three possible locations of the xx word separator before the crib word “frequency.” Apply the Morse Code symbols to the plaintext letters, being sure to place a single x letter separator between the interior letters of the crib.

```
f   r e q   u e n c   y
x . x . x . . x - - . . x
x - . x - - . . . . x - x
. . - . - x - x x - - -
1 2 3 4 5 6 7 8 9 10 11 12
```

No pattern

```
f   r e q u   e n c y
x - . x - - . . . . x - x
. . - . - x - x x - - -
. x . x . . x - - . . x
1 2 3 4 5 6 7 8 8 3 9 10
Q H S U I L C A A S U K
```

```
f   r e q u e n c   y
. . - . - x - x x - - -
. x . x . . x - - . . x
- . x - - . . . . x - x
1 2 3 4 5 6 7 8 8 3 5 9
```

Pattern match Positions 80 thru 92 No Construction Pattern Match

The pattern line beneath the three coded cri placement analyses represent the pattern of the Morse Code symbols applied to the crib word “frequency.” Examine the ciphertext to look for repeated ciphertext letters matching the Morse Code symbol patterns. You will find an identical pattern match between the second crib placement analysis and positions 80 thru 91 of the ciphertext. Verify the validity of this crib placement by placing the crib cipher text letters to the Morse Code keyword alphabet process referenced above.

```
* * * S * C * A * * * H I * K L * * Q * U V * * * *
. . . . . . . . . . - - - - - - - - - x x x x x x x x
. . . - - - x x x . . . - - - x x x . . . - - - x x
. - x . - x  .- x . - x . - x . - x . - x . - x . -
```

Keyword Alphabet (Educated Judgments):

This alphabet sequence allows us to SWEG (Scientifically Wild Educated Guess) additional letters in the ciphertext alphabet. HI*KL clearly is not part of the keyword; so this part of the alphabet will be in order and J can be inserted. Low frequency letters (F, G, P, W, X, Y and Z) can also be placed in the above alphabet. Beware of improper SWEG leading to plaintext garbage.

```
* * * S * C * A * F G H I J K L * P Q * U V W X Y Z
. . . . . . . . . . - - - - - - - - - x x x x x x x x
. . . - - - x x x . . . - - - x x x . . . - -  -x x
. - x . - x . - x . - x . - x . - x . - x . - x . -
```

The keyword appears at the beginning of this alphabet sequence. The cipher title gives a good clue to the key. **Plaintext Recovery**: Apply the symbols to the ciphertext letters. The additional "educated judgment" letters will allow much plaintext recovery and keyword completion.

FM-1. Fractionated Morse. Morton Salt? (rains)

```
ESPBD PQHTS VSDPN KWNRH SDRJG AAVXT JHWNI UHFD.
```

Morbit Cipher

We have defined the Fractionated Morse Cipher as the process of spreading a plaintext letter across two or more ciphertext letters with the use of a series of Morse Code symbols. We will continue the discussion of a fractionated cipher with a look at the Morbit Cipher. The Morbit Cipher also complements the Morse Code dot and dash symbols with the use of X as a letter separator and XX as a word separation. It differs from a Fractionated Morse Cipher, with a two-tier encipherment rather than three. We will begin with the encipherment process to understand the cipher's foundation.

A nine-letter keyword is selected to assist in randomly assigning numerals 1 to 9 to the Morse symbols array. Numerals are assigned based on the alphabetic order of the letters in the key word. Since more than one nine letter word fitting the numerical pattern may be found, this keyword cannot be recovered with confidence. Again, a picture is worth a thousand words.

```
Morbit Keyword:     A M U S I N G L Y
                    1 5 8 7 3 6 2 4 9

1 5 8 7 3 6 2 4 9
• • • - - - X X X
• – X • – X • – X
```

The plaintext, "good day" is enciphered:

```
g   o   o   d   d   a   y
- • - - - - - • X • X - - -
- X - X - X • X - • • X • -
3 8 3 6 3 6 7 8 4 1 2 6 7 3
```

The Morse Code symbols are entered for the plaintext letters and a ciphertext number is assigned to the Morse Code symbols in units of two based on the numbers under the keyword (**AMUSINGLY**). If the plaintext "good day" appears in the middle of a sentence, we would add XX before "g" and after "y." Let's try solving one.

M-1. Morbit. Munsters Ball. (threat) LIONEL

```
                                          31          40
91543 15693 82679 15513 71912 47638 79442 62299 34515 42432

65565 24321 34564 26553 15121 24234 78382 63254 54429 45242

82299 34549 15829 24245 12495.
```

Solution Process

1) Assign Morse Code symbols to the crib.
2) Determine Morse Code symbols pattern.
3) Seek Morse Code pattern in ciphertext.
4) Post recovered plaintext for all ciphertext.

Crib Pattern Determination

(Two possibilities) Pattern 1 Pattern 2

```
  T H   R   E A   T                 T   H   R   E A T
X - • • X - X X - - X               X X • • • • • • X X
X X • • • • • • X X               X - • • X - X X - - X
1 2 3 3 4 5 4 4 2 2                 1 2 3 4 5 4 4 5 1 6
7 9 4 4 2 6 2 2 9 9
Ciphertext Positions 31 thru 40
```

The three pairs in the first pattern provide a good start for examining the ciphertext for a similar letter pattern. You will find the same letter pattern beginning in position 31 of the ciphertext highlighted below. This is an excellent indication that you have found the correct crib placement and are ready to begin the plaintext recovery process.

```
91543 15693 82679 15513 71912 47638 79442 62299 34515 42432
65565 24321 34564 26553 15121 24234 78382 63254 54429 45242
82299 34549 15829 24245 12495.
```

Plaintext Recovery

Insert the recovered plaintext Morse Code symbols above the crib pattern for the ciphertext numbers they represent.

```
7 9 4 4 2 6 2 2 9 9
X - • • X - x x - -
X X • • • • • • X X
  t h   r   e a   t
```

Apply the known ciphertext Morse code symbols (**79426**) to the ciphertext, and find the plaintext equivalents. Partial word recovery will lead to symbol recovery for remaining ciphertext. No more than four Morse Code symbols may appear in a row without a separator

immediately following. (See the *ACA and You* Handbook, Appendix 1 for numeral and punctuation exceptions.)

Here is a reference to a Holiday personage to challenge your learning retention. Recall that we stated a nine-letter keyword is used to assign numbers 1 through 9 to our Morse Code symbols array. The keyword(s) for this Morbit Cipher is either CHRISTMAS or BOXINGDAY. Find the correct key, and readable plaintext will follow.

M-2. Morbit. Kris Kringle. LIONEL

92258 75948 39221 78766 92652 62528 32594 64752 83576 34546 35352 58753

52183 13691 67995 46797 94954 62135 82631 69384 45463 53528 42535 41938

26225 92358.

Keyword Analysis (Pick a winner)

```
C H R I S T M A S
B O X I N G D A Y
. . . - - - X X X
. - X . - X . - X
```

Our next Morbit Cipher does not provide the keyword. Refer to the crib pattern determination process above and the proper placement of the crib in the ciphertext. This will lead you to the recovery of the plaintext.

TG-2. Morbit. A Lot to be Thankful For. (your) LIONEL

62751 78386 81757 15413 19742 84394 31327 24946 25762 45651 65512 65715

48642 72451 26571 94313 27972 42941 31938 42938 64943 13272 49442 42162

58387 565.

Chapter Twenty-Three

Ragbaby Cipher

In presentations to groups with crypto interests, I begin my talks with a bit of cryptology history and lore, citing the age-old battle of wits between the cryptographer and the cryptanalyst. As one cipher system was developed to mask the high frequency letters, a

cryptanalyst would go to work at removing the mask.

The Ragbaby, a poly-alphabetic substitution cipher with a systematic progressive key, was developed in the early 1950's by ACA member, SHERLAC, as a means to disguise high frequency letters and further the security of secret messages.

Before we stretch our mental capacity in wonderment at the Ragbaby deciphering principles, let's look first at its construction routine that serves as its foundation.

Discussion of the Ragbaby Cipher provides us with an excellent opportunity to re-state one of our most basic solving axioms. **The unarguably most beneficial aid to the success of mastering a cipher solving process is the understanding of its construction process.**

24 Letter Keyed Alphabet – Keyword, CIPHER

Encipherment is performed with word divisions intact and a 1 to 24 numbering system is assigned to the plaintext letters. A 24-letter keyed alphabet, traditionally paring the letters I/J and W/X, is used to convert plaintext to ciphertext.

CIPHERABDFGKLMNOQSTUVWYZ
J X

The numbers are interrupted with each word division as the next number in sequence begins each new word. Ciphertext is then assigned by selecting the letter representing the sequential number of spaces to the right of the plaintext letter in the keyword alphabet. A "picture" is worth a thousand words:

pt:	Now	is	the	time	for	all	good	men..
#:	123	23	345	4567	567	678	7890	890
CT:	OSC	HV	WBF	YAUK	NWL	LUV	SZCT	WMC

Number each remaining letter in a word by counting up from the number of the first letter in a word. Ciphertext is written, as above, with word divisions intact. A hyphenated word or one with an apostrophe is considered a single word and the numbering system continues across the hyphen or apostrophe.

The counting to encipher plaintext "Now" to ciphertext OSC" is shown below.

CIPHERABDFGKLMNOQSTUVWYZ
>1
>12
3 >12

Keep in mind that I/J and W/X share the same position in the 24-letter Ragbaby ciphertext alphabet. These couplets are counted as one in the shift of letter spaces between plaintext

and ciphertext letters.

A 1 to 24 numbering system is continued throughout the encipherment of the plaintext. Each new word continues the numbering sequence with the next highest number. When the number 24 has been reached, the numbering sequence restarts with 1. Since 24 will result in identical plaintext and ciphertext letters, this is often a good entry point into the cipher's placement. The preserving of word divisions in the ciphertext also allows cipher crib placement by the counting of word letters. Crib placement is also aided with the retention of punctuation in the ciphertext.

Let's reverse the enciphering process to decipher a Ragbaby Cipher.

R-1. JF2007. Unbalanced arguments. (because) ANGO-KA

YBWHC OD QDAM GT**:** GMTQT YEG LKHY RRSL KP DPLB UQMQT KP

PUC EPBU RVDT ZURV YPBVNIU PCY TAT**'**A DYRD Y HDG UO SITEH ND.

Word divisions and punctuation are all in place, including an apostrophe, a colon and some very short words that will all help us in the encipherment process. Using our construction principles as a guide, we know that our first step in the decipherment process will be to number the ciphertext letters. These numbers indicate the ciphertext letter location relative to the plaintext letter it represents in the Keyword Alphabet. 1Y indicates that CT letter Y sits one letter to the right of its plaintext letter representative.

Numerical Sequencing

```
                                          11
12345 23 3456 45  56789 678 7890 8901
YBWHC OD QDAM GT: GMTQT YEG LKHY RRSL

 1 1111 11111 11 111 1111 1111 1111222
90 0123 12345 23 345 4567 5678 6789012
KP DPLB UQMQT KP PUC EPBU RVDT ZURVYPB
                                 because
1112 112 122 2 2222 2 222 22 2
7890 890 901 2 0123 1 234 34 41234 12
VNIU PCY TAT'A DYRD Y HDG UO SITEH ND.
                          g  o s
```

Encipherment uses a keyword alphabet to select cipher- text letters 1-24 spaces to the right of the plaintext letters they represent. Decipherment will reverse this procedure and select letters to the left of the ciphertext letters to determine the plaintext message.

Whenever a twenty-four appears above a ciphertext (CT) letter, the plaintext (pt) letter will be the same letter as the ciphertext letter. **In a Ragbaby cipher, a letter may represent itself. (Self-encryption)**

Crib Placement

Our benevolent constructor has used only one word in the message that is seven letters long. Crib placement is simply a matter of matching the crib to the seven- letter ciphertext word. We have inserted the crib "**because**" along with the plaintext letters, **g, o** and **s**, which are 24 letters away from the ciphertext letters in the key alphabet.

Keyword Alphabet Letter Placement

We will use our crib placement and numerical sequencing to aid us in our recovery of the keyword. We begin with the identification of the 1 to 24 numerical sequence at the top of our table and compute the number of alphabet spaces separating the crib pt from its CT letters.

```
2 2 2 2 2 1 1 1 1 1 1 1 1 1 9 8 7 6 5 4 3 2 1
4 3 2 1 0 9 8 7 6 5 4 3 2 1 0
              b                               Z
            e                                 U
          c                                   R
        a                                     V
      u                                       Y
    s                                         P
  e                                           B

    U         B   E                       Y Z
2 2 2 2 2 1 1 1 1 1 1 1 1 1 9 8 7 6 5 4 3 2 1
4 3 2 1 0 9 8 7 6 5 4 3 2 1 0
```

We post those letters with the known spaces between the pt and CT letters in the key alphabet. B is 16 to the left of Z; E, 22 left of B; E, 17 left of B; U, 21 left of Y We can now return to the cipher construction and **identify pt letters** in the message by using the key alphabet letters and the number of spaces between the pt and CT letters.

Example: The letter E appears 17 spaces to the left of letter U, thus U17 = e. U appears 20 to the left of letter Y, so Y20 = u. B appears 16 left of letter Z, so Z16 = b.

Plaintext Recovery Process

In our Ragbaby enciphering process, we placed our crib in the plaintext, along with the plaintext letters g, o and s, three letters that are 24 places away from the ciphertext letter, consequently sharing the same plaintext (pt) letter and ciphertext (CT) letter.

Ragbaby solving procedure reverses its construction process, identifying pt letters by their location to the left of the ciphertext letters. CT, 16Z = pt, "b" because of its location, 16 spaces to the left of CT Z in the key- word alphabet. (See keyword alphabet.)

```
                                    11
12345 23 3456 45  56789 678 7890 8901
YBWHC OD QDAM GT: GMTQT YEG LKHY RRSL

 1 1111 11111 11 111 1111 1111 1111222
90 0123 12345 23 345 4567 5678 6789012
KP DPLB UQMQT KP PUC EPBU RVDT ZURVYPB
                          e      because

1112 112 122 2 2222 2 222 22 2
7890 890 901 2 0123 1 234 34 41234 12
VNIU PCY TAT'A DYRD Y HDG UO SITEH ND.
     you     t      a   g  o s
```

Plaintext recovery is aided by short words "a" & "to" (2) as well as a punctuation mark (apostrophe in this one is a "t "or "s"). Plaintext recovery of "**you**, **a** and apostrophe **t"** adds to our **keyword alphabet.**

Keyword Alphabet

```
C A U T   O   B   E                         Y Z
2 2 2 2 2 1 1 1 1 1 1 1 1 1 9 8 7 6 5 4 3 2 1
4 3 2 1 0 9 8 7 6 5 4 3 2 1 0
```

Our keyword alphabet now looks like this.

A good case can be made for the keyword of "caution" which would generate the following completed keyword alphabet.

```
C A U T I O N B D E F G H K L M P Q R S V W Y Z
2 2 2 2 2 1 1 1 1 1 1 1 1 1 1 9 8 7 6 5 4 3 2 1
4 3 2 1 0 9 8 7 6 5 4 3 2 1 0
```

We use this completed keyword alphabet to fill in the remainder of our JF07 Ragbaby plaintext, locating those pt letters the noted spaces to the **left** of the ciphertext letters in the cipher.

JF07. Unbalanced arguments. (because) ANGO-KA

```
                                  1   11
12345 23 3456 45  56789 678 7890 8901
YBWHC OD QDAM GT: GMTQT YEG LKHY RRSL
Words to live by: Never put both feet
```

```
 1 1111 11111 11 111 1111 1111 1111222
90 0123 12345 23 345 4567 5678 6789012
KP DPLB UQMQT KP PUC EPBU RVDT ZURVYPB
in your mouth at the same time because

1112 112 122 2 2222 2 222 22 2
7890 890 901 2 0123 1 234 34 41234 12
VNIU PCY TAT'A DYRD Y HDG UO SITEH ND.
then you don't have a leg to stand on.
```

Follow the ciphertext conversion to plaintext, beginning with the plaintext beginning, "Words." Pt "W" is one to the left of CT "Y," "o" is two to the left of "B," "r" is three to the left of "W," "d" is four to the left of "H" and "s" is five to the left of "C."

As in all decipherment processes, the key is the charm that allows us to read the secret message. Attack the Ragbaby key with proper crib placement, short word analysis; word guesstimates based on the cipher title and the ever-present watch for that common trigraph "the." This cipher makes ample usage of the **"senorita"** letters and common digraphs and trigraphs. Ragbaby constructors feel less of a need to alter the general properties of letters.

R-1. JF 1999 Cm. Marital Bliss. (TBWNWFP = parents) LIONEL

PE TBWNWFP QLK LV YASAQ EGDU USHKQAM DGATRCC. EEG LFLVCB'V GNBLC MSN EAML AM GUF MEHEE VDT AZI QVQIYN'I WONQY EYQ UGEQ GE WTV UPDKZ.

R-2. MA2011 Cm. Change is recommended. (perfect) MARSHEN

YBED CST YOVYTP EFCSKSV SGDK MUKGN OGVMW NL MQAIPC WLL GTV AQ ZS; KP GVIH NF WCV LMZR AIMB PHPTGK SO'C KVVAV LEAG TKB QBI.

R-3. JF 2012 Cm. Premature. (before it) WORD WIZARD

FQCGZOIW PAMI NBECK DROTL PVK WMAH LUN GEBUP ZSNAGMP BL UFPZ NUVCIAQFA FPT CIEE DISIHP LL ZNDIY TFYQZLG. *TBTHKIO *WWHKEV

Chapter Twenty-Four

Route Transposition Cipher

A cipher which retains all of the letters of the plaintext message but simply changes their order is referred to as transposition cipher, unlike a substitution cipher which substitutes one letter for another. There are many ways to rearrange the letters of a word or message. A simple reverse order of the word" transposition" in ciphertext becomes NOITISOPSNART. Cryptology's battle of wits between the cryptographer and the cryptanalyst through the years discarded this encipherment as too easy to decipher, leading to encipherment processes of a more complex nature. The Route Transposition cipher type is one of those systems.

The Route Transposition Cipher (Construction)

One form of a transposition cipher is where plaintext is converted to ciphertext by constructing it in a specific arrangement of rows, columns, spirals or diagonal paths and extracting it by, yet, another predetermined path sequence. **The letters must form a complete square or rectangle.** A picture is worth a thousand words:

W	**A**	**R**	**L**	**F**
H	**S**	**W**	**S**	**L**
A	**F**	**H**	**A**	**I**
T	**O**	**E**	**N**	**E**
H	**U**	**E**	**D**	**S**

Extraction of the letters by rows in the above matrix produces a ciphertext of WARLF HSWSL AFHAI TOENE HUEDS, but a vertical read of its columns reveals a plaintext message of "What has four wheels and flies?" Let's try another:

T	**R**	**U**	**C**	**K**
E	**O**	**V**	**E**	**W**
G	**C**	**X**	**R**	**I**
A	**O**	**N**	**H**	**T**
B	**R**	**A**	**G**	**A**

A vertical read of these columns produces a ciphertext of TEGAB ROCOR UVXNA CERHG KWITA but a counter-clockwise spiral read of the matrix beginning in the lower right hand corner will reveal a plaintext message of "A garbage truck with no cover."

Complexity of the Route Transposition Cipher

The ease of construction of the Route Transposition Cipher, coupled with its infinite number of paths or routes of placing the plaintext in and extracting it out makes this a highly desirable form of encipherment.

Both messages above could have been enciphered in any number of paths, horizontal rows or vertical columns, consecutive or alternating paths, reverse order paths, diagonal routes, spiral routes, while making use of any number of starting points.

Solving the Route Transposition Cipher

Let's begin with an easy ciphertext construction whose title line indicates the number of letters in the construction.

RT-1. Abe Lincoln at Gettysburg (25) LIONEL

FCNER OODNS URSYA REEEG SAVAO

1) Determine the number of columns needed to form a complete square or rectangle.
2) Post the ciphertext by column or row.
3) Look for readable plaintext.

Route Transposition Possible Paths

Our completed square or rectangular matrices may use any of the following routes or combination of routes to insert plaintext and extract ciphertext:

- Horizontal - Alternating Horizontal
- Vertical - Alternating Vertical
- Diagonal - Alternating Diagonal
- Clockwise Inward or Outward Spiral
- Counterclockwise Inward or Outward Spiral
- Starting Positions – Upper, lower left and right

These represent the common routes that you will find in our Cm cipher constructions, but do by no means represent all of the possible routes that may be available for encipherment in the real world of secret messaging. Routing can include geometric designs, pictorial artistry and ad infinitum schemes limited only to the boundaries of the creative mind. The seemingly limitless route choices and ease of cipher construction makes this a highly desirable cipher type for secret messaging.

Construction

We'll use a twenty-five block matrix to review many of the available routes for the encipherment of the plaintext "A Route Transposition Cipher,"

A	**R**	**O**	**U**	**T**
E	**T**	**R**	**A**	**N**
S	**P**	**O**	**S**	**I**
T	**I**	**O**	**N**	**C**
I	**P**	**H**	**E**	**R**

The plaintext is entered in horizontal rows, but it need not be. Check out the variations in the ciphertext when the letters are extracted from various routes:

Rows

Alternating AROUT NARTE SPOSI CNOIT IPHER
Reversed TUORA NARTE ISOPS CNOIT REHPI

Columns

AESTI RTPIPOROOH UASNE TNICR
Alternating AESTI PIPTR OROOH ENSAU TNICR
Reversed ITSEA PIPTR HOORO ENSAU RCINT

Spiral

Clockwise AROUT NICRE HPITS ETRAS NOIPO
Counter Clockwise OPION SARTE STIPH ERCIN TUORA

Diagonal

AERST OTPRU IIOAT POSNH NIECR
Alternating AREST OURPT IIOAT NSOPH NICER
Reversed AREOT SURPT TAOII NSOPI NHCER

When we note that all of these extracted ciphertext variations begin at the upper right or left corners of the grid, you can appreciate the complexity of the Route Transposition with encipherment beginning options still available at other locations of the grid.

Increasing the complexity of this cipher type, is the option of installing the plaintext in these same route variations, which prompts the question," What is an innocent solver to do?" Here are a couple easy ones to get you started.

RT-2. Heredity. (56) (from)

Look for the rest of the crib adjacent to the only "F" in the matrix.

```
L I H C T S O M
C S E D N E R D
O R F D E D N E
I L G N O L A M
M R I E H T E N
I L S R E H T O
O T D E N E T S
```

RT-3. Optical Illusion (70) (two)

```
X E E S R A Y
F L D E E I L
L C A S T C N
E A M S H I O
S T E A G T S
R C H L U P A
E E S G A O W
H P D O D E E
F S N W S H H
O A A T N T S
```

Now it's on to the need for some cryptanalyst procedures for the remaining ciphers.

Route Transposition Solution Procedures

1) Determine the grid size by the number of letters.
2) Assume as near a square as possible (ACA Guidelines call for 8 x 8 square maximum and 8 x 10 rectangle maximum.
3) Look for word portions in normal alphabetical order. (See row and spiral example above.)
4) Where cribs are provided, look for grid adjacent letter sequences which support the crib.
5) Reconstruction relies heavily on trial and error.
6) The letter "X" is often used as a null letter to satisfy the number of positions needed in a Route Transposition and can be a signal to its ending.

RT-4. Just Desserts. (45) (job)

TFLDI HOLHT ERDAS RAOVO EJNEW WOEOE ABIOL RWSNL DETEX..

RT-5. Geometric Detour (56) (between)

TOTAE NOIES THRDN TTISR RTIET ICWWN UCROS ESEEO TNOUN HSTBE PSDNC X.

RT-6. Vision. (84) (usual)

TRSWH UEIDF NSHVO IASTS UOCTE OCLVU IMERI ACYIL EANOT ERNLA ENILG NOSCC ANTOT MTTUE UEITY TSEHH NEMS.

APPENDIX I

ARISTOCRAT SOLVING TOOLS

FEW POCKET TIPS

Here is a comprehensive list of Aristocrat Cipher deciphering tools under the acronym of **Few Pocket Tips**. A creative minded can create a 3 x 5 pocket fitting card to keep handy for their solving expeditions.

F – Frequency counts

A good place to begin to look for the plaintext of frequently reoccurring letters.

E – Endings, popular word

Repetitious CIPHERTEXT word endings may well be these popular word endings – ing, ion, tion, ed, es, ess, ent

W – Word beginnings

Popular word beginnings include, an, at, be, de, dr, en, in, no, pre, pro, re, se, th, un. Keep these in mind as plaintext present itself.

P – Pattern words

These are words that have reoccurring letters. We refer to the pattern word of "there" with the reoccurring letter "e" as having a pattern of 1-2-3-4-3, which means that the third and fifth letters are the same. Pattern letters are helpful in uncovering ciphertext Some of the most popular are: "That, there, good, poor, see, little, people." Pattern word lists can be found on the Internet and in many publications which define them by word length and letter sequence.

O - One letter words

One letter CIPHERTEXT words are plaintext letter "giveaways". Most always it is an "a" or an "I."

C – Cribs/tips

Placing cribs or tips in the correct location in the cipher will lead to the recovery of more plaintext. Lower case cribs are already plaintext and can be placed directly. Tips given in upper case letter Caesar format must have its letters shifted to arrive at the plaintext crib to be placed in the cipher. (See the JF or MA, 2000 Cm's for a review of

this process.)

K – Keyword alphabet

We have talked at some length about the value of the Keyword Alphabet as a deciphering tool and an aid to constructing a disguised message. Refer to the Keyword Alphabet example (JF11 Cm) to refresh your mind on its process.

E – Ending letters

Those letters most often used to end English words are, d, e, g, s, t, n, r, y – consider these letters as the plaintext begins to fill in.

T – Title

Do not overlook the cipher title as a good source for potential plaintext words in the ciphertext.

T – The

Keep on the lookout for repetitive three letter CIPHERTEXT (trigraphs) repeats which could signal the existence of the word "the" in the plaintext.

I – IQ

Sorry, but this is the only way I can slip the letter "Q" into our acronym. "Q" is usually followed by "u" and then by a vowel, "a, e, i, or o."

P – Position of letters – Most popular

"**a**," first or next to last; "**e**," second or next to last or last; "**i**," third from end; "**o**," second; "**u**," first or next to the last; "**y**," last.

S – Short words

Keep an eye out for these short words – in, it, is, of, no, on, and, the

POTPOURRI

A potpourri of cipher solving lore follows with Nom source references. These principles can be applied to most cipher types.

Crypts First Word or Two (ZANAC)

The following words are the first (or first and second) highest frequency opening plaintext of more than 1000 randomly selected ciphers from the ACA **Cm Journal. The** (18%), **A** (5%), **I** (5%), **It is** (2%), **We** (2%), **To** (2%), **If you** (2%), **It's** (2%).

"That" Pattern (ZANAC)

Have you ever wasted time trying "that" for the 1231 / ABCA pattern word, only to find yourself led astray? Here are ten additional frequent words with the same pattern. "Area, dead, ease, edge, else, high, says, tact, tent, test."

The Nudge as a Learning Tool (QUIPOGAM)

I get excited over the cipher nudge as a learning tool. I "cut my teeth" in learning to solve the Amsco cipher with nudges from FIZZY, Cryptarithm mathematical bases, other than ten, with nudges from RISHU and most recently learned a most valuable axiom in the solving of the Tri-digital cipher with a nudge from QUIPOGAM. He pointed out that although a Tri-digital ciphertext number can stand for up to three letters, a plaintext letter must always represent the same ciphertext number.

Some 122 / ABB Pattern Words (ZANAC)

These eight words should always be kept in mind when looking at those with a 122 / ABB pattern:

ALL BEE ERR FEE OFF SEE TOO WEE

THE LETTER 'H' (CRYPTODOOD)

The letter 'H', except when beginning a word, is usually preceded by one (or more) of a small group of letters, C, G, P, S, T and W. If you find that it is a 'G' then the letters following this 'GH' are usually 'I', 'OU', 'AU' or 'EI'. (Examples are fight, might, bough, tough, laugh, naughty, eight and neighbor.)

Finding the letter 'H' in a cryptogram will happen very often. This is because one of the first words we try to find in a cryptogram is the word **'THE'**. When placed, other occurrences of these letters usually appear in the cipher. When found, the small group of letters above can be attempted to precede it.

SENORITA (SIR REBRAL)

We have continually referenced the SENORITA letters as an anagram to recall the most frequently used letters in the English language. It comes from the keyboard of a nine year old original member of the ACA Kiddee Krewe, Ryne Bogart (SIR REBRAL), in a MA

2001 Cm article titled, “Cryptology is fun.” Proud pop, ACA Krewe, PHILLIES, tells us that Ryne has continued to grow up, smart.

Apostrophe Words: Contractions in ascending word-length order. (ZANAC)

‘D ‘M ‘S ‘T ‘LL ‘RE ‘VE

2-Letters -I’d, I’m
3-Letters -He’d, It’s, I’ll, I’ve, It’d, He’s, We’d
4-Letters –She’d, One’s, Ain’t, We’ll, we’re, We’ve, You’d, How’s, Can’t, He’ll
Who’s, Don’t, Why’s, Isn’t, She’s, Let’s
5-Letters –They’d, That’s, Aren’t, She’ll, You’re, You’ve, What’s, Hasn’t
You’ll, When’s, Wasn’t
6-Letters – There’s, Doesn’t, They’ll, They’re, They’ve, Where’s, Mustn’t, Weren’t
7-Letters – Couldn’t, Wouldn’t
8-Letters – Shouldn’t

Former ACA member, **Helen Fouche Gaines’ (PICCOLA)** study of ciphers, *Cryptanalysis*, remains a classical text in the study of cipher analysis. Her account of vowel behavior follows.

Vowel behavior.

1. A, E, I, O, are high frequency, U is moderate.
2. Letters contacting low frequency letters are usually vowels.
3. Letters showing a wide variety of contact letters are usually vowels.
4. In repeated digraphs, one letter is usually a vowel.
5. In reversed digraphs, one letter is usually a vowel.
6. Doubled consonants (c) usually flanked by vowels (v), and vice versa. (cvvc or vccv).
7. It is unusual to find more than 5 consonants in succession.
8. If the CT letter with the highest frequency is assumed to be E. Any other high frequency letter that contacts it often cannot be a vowel.
9. E is the most frequent vowel and rarely contacts O. Both double freely.
10. “A” may follow but rarely precedes E.
11. The vowel that reverses with E is I.
12. Observations 10 and 11 apply to the vowel O, but U precedes E and follows O.
13. The only vowel-vowel digraphs of consequence are OU, EA and IO.
14. Three vowels in sequence may be IOU, EOU, UOU and EAU.

***Codes, Ciphers & Secret Writing,* Gardner**

1. The most common word letter end is E.
2. The most common word letter beginning is T.
3. The most frequent two letter words, OF, TO, IN.
4. The most common three letter words, THE, AND.

5. Q is most always followed by U.
6. The consonant most often following a vowel is N.
7. The most common double letters in regular order are LL, EE, SS, OO, FF, RR, NN, PP & CC.
8. The most frequently used four letter word is THAT.

The Science of Secret Writing, Dwight Smith

Order Frequency of Initial Letters: T, O, A, W, B, C,
D, S, F, M, R, H, I, Y, E, G, L, N, P, U, J, K.

Order Frequency of Final Letters:
E, S, T, D, N, R, Y, F, L, O, G, H, A, K, M, P, U, W

Quote Authors' Names (ZANAC)

http://www.quoteland.com/author.asp

Authors' names are most useful with proper nouns at the beginning or end of Aristocrats, Xenocrypts and many Cipher Exchange constructions indicate an author's name. The above list is not a pattern list but often, names will be found to contain a pattern and can indicate exact names like "Ann, George, William, Richard" and many others. Proper nouns form a frequency table and pattern list of their own. Keep such a list with your own patterns.

Constructor Patterns

Also helpful is a constructor index list with their use of frequent cipher topics, title relevancy, vowel (use or disuse), grammatical style (use of past or present participle verbs ending in “ed” or “ing”), foreign language proficiency for Xenocrypt X-7 identification.

WSJ.Com Making Every Word Count (FLEUR DE LIS)
Check this site for word frequencies and a list of the one hundred most used English words.

Solving Resources

Check the **Resources** section under our ACA Website at www.cryptogram.org for helpful tips on all cipher types and nudges on current *Cm* ciphers.

APPENDIX II

PATRISTOCRAT SOLVING TECHNIQUES

1) Do not ignore the cipher title. It can lead you to educated word guesstimates.
2) Pattern crib – Align crib plaintext (pt) letter pattern with ciphertext (CT) letter pattern.
3) Non-pattern crib – Drag pt crib through the CT, looking for additional logical plaintext.
4) Letter frequency count – Locate high and low crib letter frequencies to CT high and low letter frequencies.
5) Pattern words – Look for potential pattern words at the beginning and ending of the ciphertext. Verify them by dragging potential pattern word letters through the plaintext.
6) Non-pattern words – Look for large non-pattern words from large word usage constructors (PETROUSHKA) at the start and finish of the ciphertext and drag their letters through the plaintext.
7) Alliteration – Look for wordbreaks in cipher alliteration constructions by being alert to reoccurring letters spaced at average word lengths through the cipher (4.3 letters for normal writing).
8) Look for high frequency CT digraphs (2letters) and trigraphs (three letters) that may represent high frequency pt digraphs "th, er, re, on, no, an, he, in, ed, nd, ha" and pt trigraphs "the, and, tha, ent, ion."
9) Google those cipher titles that may suggest quotations from famous statesmen, comics, personalities, etc. Plaintext may be revealed.
10) Keyword construction recovery. Do not overlook the opportunity to use the keyword alphabet as an aid to recover additional plaintext. The K2 alphabet below suggests possible additional plaintext recovery.

```
abcdefghijklmnopqrstuvwxyz
T   XYZC PH RABDFGJ  MN
```

11) "Keyblock discipline" is a term used by ZANAC to keep an eye on low frequency letter placements in K1 and K2 keyword alphabets. Letters occurring once or twice in the cipher construction are candidates for "b, c, j, k" at the beginning of the keyword alphabet sequence following the keyword and "v, w, x, y, z" possible candidates for the end of the alphabet sequence before the keyword. High letter (vowels) frequencies can aid in pinpointing the keyword placement.
12) Look for triplets (that's three identical letters in a row. (Ex. **miSS S**ome). They are easy to spot; after the second letter you can undoubtedly place a word divisor. They narrow the number of possible substitutions to 2(or at most 5). They can confirm or infirm other guesses (by elimination). The most frequent triplets are S and L. You can also find O, E and F. (TWEETY)

Helpful Cm Articles for Patristocrat Solving

JA 91 – The Rookie's Guide to solving Pats, LAMONT CRANSTON
JA 91 – The Science of Cryptanalysis, FAUSTUS
SO 91 – The Solution of Straight-Substitution Crypts, FAUSTUS
ND 91 – Ciphers – Vowel Spotting and Digraphs, PICCOLA
JF 92 – A Method For Finding Repeated Sequences, PICCOLA
MA 92 – Consonant-Line and Vowel-Line Methods, S-TUCK and BAROKO

APPENDIX III

BACONIAN CONCEALMENT CIPHERS

The two texts below appear very real and clear but consider their concealment of an underlying secret message when two distinct features are used to generate a concealment device. In these exercises, the Baconian equivalency letter is determined through the examination of the final letter of each word. Consider its verb or consonant status and assign the "a" and "b" equivalency on this basis. Continue this route until you arrive at five letter equivalencies that establish plaintext letters logical cleartext.

A.

The "father" of the Baconian biliteral alphabet type message code as we know it, was one, Lord Francis Bacon, a noted scribe, philosopher, one time avid cryptologist, who strongly believed the only secret codes were those that effectively concealed the fact that any secret existed.

Sixteenth Century, elite, active English political statesman, he used slightly different font types in the printing of written correspondence to conceal communication he wrote to his peers for exclusive interpretation by a selected few.

This system's fundamental principle to compose an alphabet thru combinations that two unique symbols provide; in use long ahead of Bacon's time by the ancient Greeks, whose armies use of fire torches swung to the opposite directions signified signs into two varying "fonts". The Indians smoke signal communications from mountain tops across the North American Plains also is an example of communication transmission thru symbolic variations.

Simple substitution is the cryptographic art applied. A pure novice without any knowledge of cryptography is able to read the coded message quite easily when keys are provided the receiver.

Readable text use to conceal the fact that there was a concealment process present was a tandem step code device, with one step a text so obvious, no one would be ever looking for the second step.

So, Bacon's noteworthy successes with cryptography lie in these very principles. It is claimed that he actually used the cipher as a preservation technique for historical documents, a media of lineage trace and a vessel for literary pseudo usage identification. Countless are many historians, literary personage, researchers and academics, who, pondering a Shakespeare connection, promote the question, who really penned some of the many works of Shakespeare? But such a pretense promises a story some brave soul can address another day where mind and matter compete with logic and reason.

Possibly, Bacon had his tongue in the proverbial cheek while declaring the true cipher was one not laborious to write, type or read. A strenuous mental exercise is necessary to construct Baconian text, a difficult task, attempting to write this bilateral type cipher in meaningful dialogue to promote plaintext concealment while being grammatically correct. ACA Krewe members who readily struggle thru Baconian constructions remain well aware of such.

Two versions of the Baconian cipher exist. One type, like null ciphers, conceals any plaintext existence, reading much like plaintext in its own. The second Baconian type, a verbal collage, conceals the message with series of words,

The Baconian type cipher concealment may use a variety of alternative methods for ciphertext dialogue. The use of any two distinct characteristic variations, either thru font styles, wordage length, message punctuation style, vowels, syllable number, consonant order, are all variables put to use in order to construct various ciphertext message cover of plaintext repartee.

We expend all such ruminations in the endless quest of the truly perfect cipher, the one which advocate, Francis Bacon, chose as a bastion of trust and security. He logically concluded that the most ingenious type cipher path devised by cryptographers, lie subject to cryptanalysis solution, as all paths can be followed backward to their very ultimate inception.

The Baconian Cipher is a good cipher to truly cover up the existence of any cryptography activity. Its value to the cryptographer is that no truly discernible trace of evidence exists to hint some sinister motive is taking place.

Though many a change has made the present day megabytes communiqué much the opposite of the ancient Greece torch fire communication technique and Indian mountain side clouds of smoke, divergent symbol signals still remain quite alive and with us today.

B.

The Baconian consists of two unique levels. We begin a simple substitute alphabet procedure to replace the message we are concealing with the use of five surrogate “b” & “a” type letters. The alternative use of font choice preference or symbols include a variable style that we can use in disguising the “b” & “a” substitute type. Concealments also are accomplished thru using a substitute message which appearance gives off the apparent resemblance of the real message. Dragging a nudge, or crib, is a technique that we use to find the place the crib fits the ciphertext type in identical like sequence**.** We do this thru comparing the Baconian equivalents that embodies to those the same like representative type ciphertext surrogate letters utilize. Where no variance be there evident, diverse use active thru use of conflicting type equivalents, no dispute due in appropriate place of locale.

APPENDIX IV

RAILFENCE TEMPLATE

It would be foolhardy to label either pencil and paper or computer solving techniques as the "proper approach" for solving any cipher. They are inter-related and have a bond between them. Pencil and paper solving is the learning foundation for cryptography, and cryptographic computer programming and computer programs have much to offer pencil and paper enthusiasts in alternative routes of solving routines and the elimination of much of the grunt work and drudgery of trial and error erasures.

The Rail Fence Cipher was a popular Civil War cipher. For some people, the construction process is the very best route of learning the idiosyncrasies of cipher types as an aid to the decipherment process. This template was developed to allow one to reverse the process of zig zag plaintext generating ciphertext rows. The template will be an aid to all wishing to encipher plaintext messages and also deciphering Rail Fence ciphers. It should be noted that this same template can be used to encipher and solve those dreaded Redefence ciphers as well.

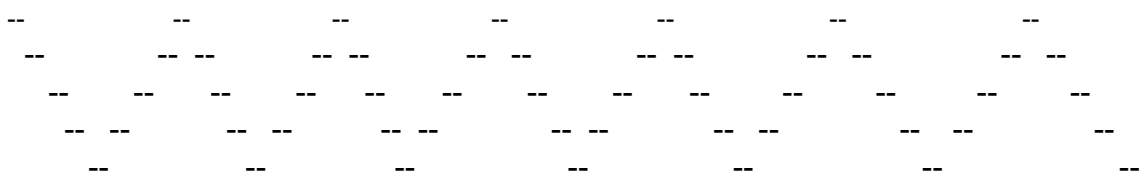
The template can be enlarged on a copy machine to any workable size for the user. There are patterns for Rail Fences ranging from 3 to 7 rows (rails) and space for over 60 letters. If more letters are required, tape two templates together at an appropriate place. Be sure to make copies of your enlarged copy which can be used for future Rail Fence ciphers.

Simply post the ciphertext letters to the horizontal spaces for desired number of rails and look for readable plaintext in the zig zag pattern spaces. Use only the number of spaces, counting from left to right in a zig zag path, which equals the number of letters in the cipher construction. Offsets are observed by leaving blank the number of spaces on the left hand side of the template to equal the number of offsets required. As spaces are skipped on the left hand side of the template they should be added to the right until the spaces used equal the number of ciphertext letters in the construction.

<u>Rails</u> **<u>Ciphertext Letters</u>**

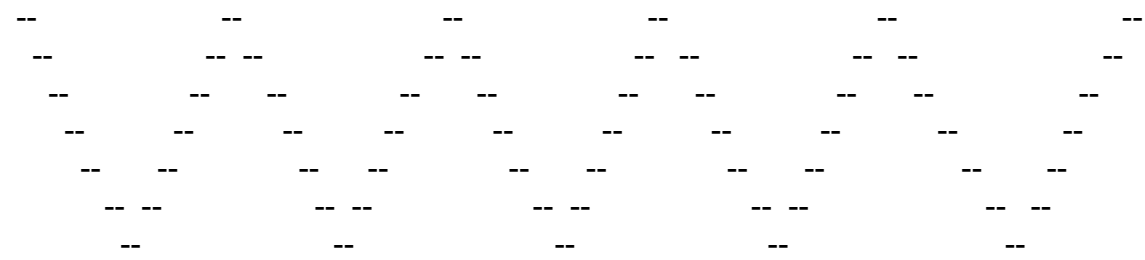
```
3  --     --      --     --     --     --     --     --     --    --     --    --     --    --     --    --
     -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
       --     --      --     --     --     --     --     --     --    --     --     --     --    --     --    --

4  --       --       --       --       --       --        --       --       --        --         --         --
    --    -- --    -- --    -- --    -- --    -- --    -- --    -- --    -- --    -- --     -- --     -- --
      -- --    -- --    -- --    -- --    -- --    -- --    -- --    -- --    -- --    -- --     -- --
        --       --       --       --       --       --       --       --       --        --         --
```

5



6

7



Special Note: Construction of the Railfence cipher will demonstrate that offset blank spaces at the start of the cipher are added to its end.

Use only the number of spaces that equal the ciphertext letters in the construction. Count off 52 spaces for a 52 letter construction, zig zag path, from left to right on the template.

APPENDIX V

NULL VARIABLES

1. Distinguish principles for determining the position of a plaintext letter within a ciphertext word. First through infinite number of all words or nouns, verbs, adjectives, adverbs.
2. Part of speech – noun, verb, adjective, adverb. Counting pattern from the beginning or ending of each word.
3. Letter following a part of speech – consonant, noun, verb, syllable, adjective, adverb.
4. Some counting pattern from the beginning or ending of each word.
5. Middle letters of ciphertext words.
6. Word syllables.
7. Letters within selected word syllables.
8. Counting patterns relative to vowels or consonants within a ciphertext word.
9. Counting patterns relative to all ciphertext – Example every fifth letter or word.
10. Punctuation mark patterns – letter or word following.
11. Letter shape distinctions – Enclosed space or not, symmetrical or not.
12. Letter placement based on initial letter of each word – A = first letter, B = 2nd letter,
13. Digraph/Trigraph counting within a ciphertext word or through multiple words.
14. Do not exclude the possibility of two or more plaintext letters per ciphertext word.
15. Be aware of the possibility of plaintext being reversed in ciphertext.

AAHJU
Larry Mayhew

Nulls Ciphers from the Cryptogram, Grouped by Rule

BION Presentation to ACA 2006 Seattle Convention

One letter per word, numeric pattern (52 ciphers)

am48e10 jf93e2
ja60e2 mj94e5
so60e2 nd94e3
so60e8 jf98e7
jd66e4 mj98e6
nd68e1 so98e3
mj70e1 nd98e4
so71e2 jf99cc06
nd74e3 mj99e7
so75e5 ja00e9
jf78e2 ma00e1
so78e5 nd00e2
nd79e3 ma01e2

nd80e3 ja01e3
ac816 nd01e2
nd81e10 ma02e5
ma83e8 nd02e6
ma84e11 jf03cc8
so84e8 so03e7
ma85e6 jf04x12
ma86e3 ja04e2
so86e5 ja04x9
ma88e6 ja05ja1
jf89e5 ja05xsp1
nd89e1 so05x12
ma92e3 mj06x10

One letter per word, key letter (5 ciphers)
mj76e2
ja95e2
jf01cc8
ja03e12
jf06e11

One letter per word, unique shape or feature (2 ciphers)
ja02e18
ac763

One letter per word, according to formula (3 ciphers)
ma87e8
jf97e5
ma03e11

One letter per word, numeric pattern, restarted at random (1 cipher)
ma89e4

Two letters per word, numeric pattern (12 ciphers)
am48e13
ja64e10
nd69e3
ma73e4
mj79e5
ac821
ja88e9
ja90e3
ma91e2
mj93e3
ja94e1
mj05e6

One or two letters per word, numeric pattern (4 ciphers)
so75e11
mj82e2
so87e2
mj06e7

One or two letters per word, according to formula (2 ciphers)
ma90e6
ac725

Group of letters, key group (1 cipher)
ja68e3

Ignore word divisions, numeric pattern (14 ciphers)
fm49e15
nd76e9
mj80e4
so85e4
ma90con4
nd90e9
ja91e4
ja92e2
nd92e2
jf94e4
ma95e6
nd95e3
nd99e5
so05e18

Ignore word divisions, key letter (2 ciphers)
mj72e12
so93e3

Count blanks as letters, numeric pattern (1 cipher)
so83e16

One letter per word, numeric pattern, reversed text (2 ciphers)
jj52e7
mj96e14

Two letters per word, numeric pattern, reversed text (1 cipher)
ac791

Divide by syllables, numeric pattern (1cipher)
so96e7

Morse code (1 cipher)
ac363

Two messages, one letter per word, both numeric (1 cipher)
so97e7

Two messages, one letter per word, numeric & key letter (2 ciphers)
mj97e7 jf04e11

Null Rule Examples

One letter per word, numeric pattern - nd81e10
Lack tremendous motion? Ask Miss Grace Henderson. Managing leads abuse whenever stomach hurts. Henderson's doctors chase out small or tremendous plain! Attend!
(Alternate second letter from end and second letter from start)

One letter per word, key letter-ja95e2
FAITH POWERFUL OVERGROWN SEPTAGENARIAN SCREAM MNEMONIC FREEDOMS LAMENTATION VIRTUOSO MOURN FOREIGNERS AREA SWORD THIRST UNDERGROUND TWITCH APPLAUD HARDWARE NIGHTS HYPOTENUSE LAWYER AGROUND FUEL (letter before last vowel)

One letter per word, unique shape or feature - ja02e18
RUFUS NYLON FAIRY SPOTS HAUNT POUND ERROR FROGS DAUBS VUGGS TOKEN THERE MELTS POUTS SHODS OBOES BAIZE THREE BROAD UVROU BUSES.
(Unique straight or curved letter)

One letter per word, according to formula - ma87e8
LUCKY ZOO: CAMEL, PUMAS, LIONS, GNU, PUFFINS, SEALS. WATCHED OTTER, CROCODILE, OSTRICH. VISIT AMUSING MARMOSETS, HOWLERS. LOVED PIGEONS, SPOONBILL. FOUND WALKS, DWELLINGS, GRASSES.
(Middle letter, = first plus last divided by 2)

One letter per word, numeric pattern, restarted at random - ma89e4
DWARFISH PROFESSOR TRIES TO SOLVE CIPHERS. EARLY ADVANCES ARISE, BUT ARE RESTRICTED TO UNPROVEN CLEVER GUESSES. CRITICISM GROWS, STATEMENTS OF WHIZ ARE ANNOYING. SHREWDLY HE MENTIONS NEW CONDITIONS. CIPHERBREAKING FOLLOWS GENEROUS TIPS ONLY!
(1, 2, 3, 4, 5, 6, 7 restart at random)

Two letters per word, numeric pattern - nd69e3
BRIGHTLY GLIMPSED SCHOLARS STRANDED OCTAGONS SECTIONS CONTESTS BATTERED NAUTICAL ACTIVATE HANDPUMP BALECLIP GOLDRING BAKEBEAN LATESHOW ADIPOSED (letters 3 and 6)

One or two letters per word, numeric pattern - mj82e2
Bully boys sing sexy doggerel, Crazy enjoyment! Imitative dame
Edits their attempts, Waxes lyrical. (first pair, then second to last letter)

One or two letters per word, according to formula - ma90e6
PYLON OVERSIZE AGO HALO TORPID DRACO SEQUIN NEMESIS STEW TRAITOR DEPTH DOGMA SPAN PLOYS PARASOL ANALYSIS
(Last pair from odd length words, last letter from even)

Group of letters, key group - ja68e3
MJU RG S SAN GL HIP SUG WIL NFUF A LZG LARR NUG IV GAK ETUE
JDO ING SDA G YOFF MWA MTG BEL ENG LBU GA OY

Ignore word divisions, numeric pattern - ja92e2
FOR THE ORDERS AND BOYS MAKE CODES OF SIX TYPES. ALWAYS OBTUSE, LANGUAGE REPEATS A WORD TO DEFEND NATURALS. (2,3,4,5 Pattern)

Ignore word divisions, key letter - so93e3
KILN OATH SWORN LEARNS DODGE IOTA SEAL AFIELD SIP OINKS WEALTH CHRISM (letters before vowels)

Count blanks as letters, numeric pattern - so83e16
MUCH FAVORS NOW REMAIN A MOMENTARY GLIMPSE SEES NO ORDERS FOR MY REPORT COULD NOT SENSE METHOD. (4, 5, 6 Pattern)

One letter per word, numeric pattern, reversed text - jj52e7
You should always be energetic, brave, tireless in opposing wretched evil men of Soviet internationales's high tyranny
(First, last, first, first in reverse)

Two letters per word, numeric pattern, reversed text - ac791
SWISS UNTESTED SCORES DANDER EVENING ERUPTS PLEASES HISTORIES INTENSE SUTURES ABACUS EDIBLE EXPLOITS ITEMIZES SWIRLS ELEVATION OUTSWIMS THRIFTS EVASION UNFASTEN CARELESS BICYCLE REDCOAT TONNAGE OUTDRAW (1 and 4 from each word, reverse)

Divide by syllables, numeric pattern - so96e7
IMPETUOUS MARINATE PARISHIONER ZYMURGY TORTUOUS GALIOT DROUGHT SYNECDOCHE VACUOLE VERTIGINOUS PANEGYRIC NARCOSIS WROUGHT UXORIOUS LOGARITHMS PTERODACTYL MAYHEM PUSILLANIMOUS MINISTERIAL EQUINOX INTERPLANETARY XENOPHOBIA SPHINX EUPHONIOUS OXYACETYLENE.
(First letter of last syllable)

Morse code - ac363
COUNTERESPIONAGE TATOO ILLICIT PARADIGM UNSCIENTIFIC PHOSPORESCENCE PROCRASTINATION AUDIOPHILE PENITENTIARY INSIGNIFICANCE PERISCOPE ECLIPTIC DIVISION QUADRANGLE UTTERANCE HIRSUTE TITTER HORNBLENDE OBLITERATION SANITARIUM SETTLEMENT FORMIDABILITY KOHLRABI PHALANX OMNISCIENT BIBLOMANIA AISLES SUNLIGHT UTILIZING DIETICIAN HARPSICHORD WAREHOUSEMAN TRICHINOSIS BISCUTS EFFERVESCENT PARALYZED RATTLETRAP MYSTIC SUPERSTITION MALICE (T = dash, I = dot. Word with no T or I = space.)

Two messages, one letter per word, both numeric - so97e7
*L*ABRINTHINE *I*NCLEMENCY *K*AOLIN *E*STROGEN *A*NGIOSPERM *R*UTHERFORDIUM *O*UTDOORSMAN *L*UMINOSITY *L*ONGITUDINAL *I*NUNDATE *N*ASTURTIUM *G*RAPHICS *S*PRINGELIKE *T*RIBALISM *O*BITURARY *N*IHILIST *E*ERIENESS *X*EROGRAPHY *Y*EASTY *Z*ONINGS *W*ORKROOM *O*SSIFY *R*HYOLITE *D*UODECIMALIZE *S*TAPHYLOCOCCUS
(1, 2, 3, 4, 5, 4, 3, 2 pattern and first letter)
(Group following group with G)

Two messages, one letter per word, numeric & key letter - mj97e7
*S*ATYR TEACHER *A*LIENATION *N*EST *I*NKED *S*YMBOL *L*EAN *A*MPLIFY *W*ORKOUT *L*ORE *E*THEREAL *K*EYING *A*DVENTUROUS *D*UO *V*OTER *I*NCHES *S*ERIAL *E*XAMINE *D*ARKEST (first letter, and letter before last vowel, counting Y as vowel)

Keyed null - Worst country song titles 1
LIAISON BECKON BEEN ABNEGATE AIRDROPS MANIFOLD MELON MERGE SNAGS PEOPLE SOFTNESS OUTGO MOTORIST PANOPLY ABDOMINAL AFGHAN MOSCOW ACROBAT AGNOSTIC ALTOGETHER INDENTS KAOLIN DRABNESS OGLE OMINOUS ONTO POLYNOMIAL PROGENY TENUOUS
(Repeated key word: song. Plaintext is letter before the first key letter in each word)

Keyed null - Worst country song titles 2
EPISCOPAL KEYSTONE CONSTRUCT RECREATION FRAGILITY YODELER HOMEY IDIOCY ILLUSION SHUCK DRYING FALLOUT ACQUIRE SHABBY HATCHED ABBOT PLAYFUL PLUMBING FRUITFUL UNILATERAL UNSEEMLY LYNCH ACOLYTE MINIBUS MINIBUS OFFSET TEENAGER CUTELY DEMOCRATIC DURATION PEDICURE NONSKID EYESIGHT GABARDINE LARCENY ROMANTIC STRIATION WIREPULLER WIRING
(Key: country. Second letter before key letter in each word)

Nulls -- Easy as 1, 2, 3?
Mini Con -- Lake George, NY
May 5, 2012
BECASSE

Binary Number Key, MJ12, E-11 Null. An apple is...(tooth) DABASAP

```
PHIL SAID "BIKE EAST LINDA.SETUP MURAL.TEAM APOLLO ITCHY. SUBARU WASHED."
0001 0010  0011 0100  0101  0110  0111 1000   1001  1010    1011   1100
```

For each word, align its binary number (first word gets 0001, second gets 0010, etc.) with the right hand edge of the word, and the significant letters are above the "1" digits.
In binary, numbers from 1-15 are represented like this:

1- 0001	4-0100	7-0111	10-1010	13-1101
2- 0010	5-0101	8-1000	11-1011	14-1110
3- 0011	6-0110	9-1001	12-1100	15-1111

APPENDIX VI

The Cryptogram, ND 2007

Affine & Hill Ciphers

By LIONEL

How Urban Elementary School Youth Struggling With Multiplication Tables Find Comfort In The Affine and Hill Cipher Types.

Principal Miss Rosemary cautioned, "Let me be honest up front. These children are not only academically challenged but have a myriad of interests and places they would rather be than in an after school tutoring program." These were sobering words to one volunteering to lend a helping hand to inner city second, third and fourth graders, who wanted no part of taking on addition, subtraction, division and multiplication tables

What can a teacher to do to enter the mindset of a seven, eight, nine or ten year old, whose attention is attracted to video and computer games, arcades, text messaging and all of the modern technical ingenuity coming down the pike? How do we motivate a mind-tired child after a full day of classrooms in a place that he or she does not want to be? How do we convince a child that learning can be more exciting than frolicking with siblings and friends in fun and games distant from the classroom?

Enter, Terrell, a second grader, steeped in an exuberant personality exhibited in all directions but classroom learning. When his second grade teacher, Miss Mullen, related that all Terrell wanted to do was to have fun, it sent me way back, too many years to count, with thoughts of my third grade teacher, Mrs. Lane, who expressively exhibited the persona of an educator having fun. "Learning should be an exciting fun-filled experience," voiced a bubbling Mrs. Lane, "How can one not get excited in pursuit of all the knowledge that the universe has to offer?" Now, I had only to fathom how to get this message across to Terrell.

We began with reading, writing, spelling, and basic addition and subtraction, all a turn-off for Terrell, who just wanted to have fun and witnessed no interest in "universal knowledge impact" upon his persona. Conversations about his areas of interests led to super heroes' adventures. I inquired as to whether he was aware of how super heroes were able to communicate with allies in discreet and private messaging. Enter the world of secret messaging and the Cipher Wheel.

"Wouldn't it be cool to be able to communicate to your friends in a way that your big brother and sister could not understand what you were saying?" I asked Terrell. "What do you mean, Mr. Lee?" was Terrell's reply. I scribbled the cipher, "OYDKKH EO BQJ." (Caesar Shift of four letters will reveal the plaintext message, "School is fun.") I suggested that Terrell bring this message home to his brother and sister and challenge them to read it. "But I can't read it myself, Mr. Lee," was Terrell's retort. A short introduction to the Cipher

Wheel and Terrell could not wait to get home that afternoon with his new found learning tool. I cautioned him to keep the Cipher Wheel out of sight.

At our next session, Terrell was eager to relate the stumping of his siblings and eager for more practice with the Cipher Wheel. Our one hour session zipped by as I entwined the Cipher Wheel with reading, writing, arithmetic and another secret message for Terrell to take home to his siblings.

Future tutoring sessions introduced Terrell to the Caesar Cipher and Cipher Slides as a prelude and introduction to the most rudimentary Affine and Hill Cipher application to secret messaging. My game plan was to tie in addition, subtraction, division and multiplication practice to ciphers and secret messaging. Oh yes, we would face the dreaded multiplication tables that Terrell's friends in the upper classes had promised him were coming down the pike. Oh, how challenged students do dread the intrusion of the multiplication tables into their uncomplicated world. I promised Terrell that they would be fun and prepped him to look forward to them as an important part of his secret messaging.

And look forward to them Terrell did. His second grade teacher, Miss Mullen, inquired into what mysterious feeding process in our tutoring sessions was prompting Terrell to lobby for the introduction of the multiplication tables in the second grade curriculum. I cautioned Terrell that he might not be the most popular young man in his classroom when the multiplication tables arrived but he responded, "Don't worry Mr. Lee, I'll show them how to use them for secret messages."

Wow! A volunteer tutoring program that I had approached with apprehension had now taken a positive turn for the better. Requests began pouring in from students for my services and fellow tutors began asking if learning was accompanying the "game playing" that was being reported as taken place in our sessions. I had to discontinue substituting for absent tutors as their students wished to stay with me.

But the best was yet to come, with the appearance of the "dreaded multiplication tables," as we introduced the Affine and Hill ciphering construction approach to our second, third and fourth grade students.

The Affine (Linear Substitution Encryption) and Hill (Lester Hill, U.S. mathematician) Cipher techniques manipulate numbers in ciphertext with complicated formulae base to disguise message plaintext over and above the simple substitution process. Numbers have been commonly used to encipher plaintext but the Affine and Hill Ciphers use mathematical formulae and logic to disguise the plaintext further through a series of mathematical equations.

The Affine Linear Substitution Encryption in its most basic application form may first apply addition and then multiplication to its plaintext message. To convert the plaintext letter "C" by this method, 5 might be added to the numerical value of the letter (C = 3; 3 + 5 = 8) and that sum multiplied by some other constant, such as 5 (5 x 8 = 40). The resulting cipher

letter is N (40 modulo 26 = 14 – N). (*Encyclopedia of Cryptology*, David E. Newton, Instructional Horizons Inc., 1997)

The Hill Cipher suggests that a series of plaintext letters can be converted into ciphertext with the use of four simultaneous linear equations where variables are raised to no power higher than the first and all variables have the same values. Needless to relate, such complex base formulae do not allow for the ease of plaintext encryption and certainly will not relate to the desire of making elementary classroom mathematics fun and games. But they do provide a path to a simplistic approach of making secret messaging through elementary mathematics fun while achieving the primary objective of simultaneously educating the student.

Supported by the Affine and Hill Cipher premises and willed with the desire to make mathematics fun, we began our journey. A simple alphabetical/numerical slide is constructed, relating letters of the alphabet to a numerical sequence:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
```

Let the fun and games begin. Numerical ciphertext is developed, incorporating the mathematical lessons of the day. This simple slide is sufficient to relate to the second grade's most basic math problems and is expanded as higher class math relates to double digit multiplication tables, columnar addition and long division type problems. A second grade numerical ciphertext, related to the numerical slide might look like this:

```
(6 + 3)  (6 + 6)  (5 + 4)  (6 + 5)  (3 + 2)  (10 + 9)
   I        l        I        k        e         s
(2 + 1)  (4 + 4)  (10 + 5)  (5 + 10)  (7 + 5)
   c        h         o        o         l
```

The classroom exercise enjoyment is enhanced as secret messages are related to the students and geometrically compounded as students are challenged to develop their own secret notes to take home and challenge the family. (My first secret message to Terrell related to school being fun. He however related that he could come up with much more interesting plaintext.)

This mathematical recipe for secret messaging to initially challenge siblings, friends and family and in later years to cover up messages from uninvited prying eyes establishes an intensive avenue to motivation.

Ah, yes, the interminable age-old competition between the cryptographer and cryptanalyst reared its ugly head one day when a student lamented that a brother had figured out her ciphering slide system. What is a cryptographer to do? Why it's elementary, my dear Watson (the student's actual name), simply change the slide. Reverse the alphabetical order, use an inside out alphabetical arrangement, arrange the slide with every other letter order, etc. etc. etc. And so, cryptology and mathematics education had been saved to live another day.

“Affine and Hill” brought the classroom alive for both the student and the teacher by demonstrating that learning can be fun. It has transferred the mathematical educational journey from one of “the blahs” to a passion for numbers. This inspirational transference has made both student and teacher eager to return to the classroom in much the same nature of anticipation that is engendered into the looking forward to the newest video game, ball game or latest movie or DVD. It has invigorated this educator into looking forward to the next academic year.

APPENDIX VII

FOURSQUARE CIPHER

C. T. LETTER FREQUENCIES

(PER 100 DIGRAPHS)

a	b	c	d	e	5	6	7	8	4
f	g	h	i	k	3	2	5	4	3
l	m	n	o	p	4	4	4	8	6
q	r	s	t	u	3	3	5	8	6
v	w	x	y	z	1	0	0	1	1

5	6	6	7	5	a	b	c	d	e
3	3	5	4	2	f	g	h	i	k
5	3	3	9	5	l	m	n	o	p
4	3	5	6	8	q	r	s	t	u
1	0	0	1	1	v	w	x	y	z

Based upon 825,000 digraphs from English language word lists.

a	b	c	d	e	5	5	8	8	4
f	g	h	i	k	3	2	4	5	2
l	m	n	o	p	5	4	4	7	5
q	r	s	t	u	3	3	5	9	6
v	w	x	y	z	1	0	1	2	2

4	6	7	6	5	a	b	c	d	e
2	2	4	5	2	f	g	h	i	k
4	3	3	9	5	l	m	n	o	p
4	2	6	7	6	q	r	s	t	u
1	1	0	3	1	v	w	x	y	z

Based upon 5,000 digraphs: "Statistical Methods in Cryptanalysis" by Kullback.

JF78 AC-155 FOURSQUARE "U-boating"

Sq 2:

K	S	G	M	N	X	F	R	Y	B	V	W	L	U	E	O	P	C	T	D	Z	H	Q	I	A	
16	14	13	12	10	10	10	9	9	7	7	7	6	6	5	5	5	4	4	3	3	2	2	1	-	(170)

Sq. 4:

C	P	Q	F	V	L	Y	O	X	D	S	G	N	U	E	A	I	K	R	T	W	H	M	B	Z	
15	14	13	12	11	11	10	9	9	8	8	7	7	6	5	4	4	4	4	3	3	2	1	-	-	(170)

	a	b	c	d	e	D	S	R	K	U	
	f	g	h	i	k	E	O	B	L	V	
1	l	m	n	o	p	P	F	C	M	X	2
	q	r	s	t	u	T	W	G	N	Y	
	v	w	x	y	z	H	A	I	Q	Z	
	C	D	F	N	U	a	b	c	d	e	
	R	I	G	O	W	f	g	h	i	k	
4	A	V	K	P	X	l	m	n	o	p	3
	S	E	L	Q	Y	q	r	s	t	u	
	H	B	M	T	Z	v	w	x	y	z	

RISHU
5/03

INDEX

SOLUTIONS

Chapter One

Caesar Cipher (1)
K1 – Cryptography is fun.
K2 – ACA members are called Krewe.
K3 – Noms are ACA code names.
K4 – Send in your sols.

Caesar Cipher (2)
K1 Caesar ciphers are easy
K2 Alphabet table helps solving.
K3. Look for intelligible word.
K4. Register in the Kiddee Krewe.

Chapter Two

Pig Pen Cipher
K1. Code
K2 Keys
K3. Allow
K4. Read

Telephone Cipher
K1 Family fun
K2 Telephone code
K3 Secret writing
K4 Gary Rasmussen

Chapter Three

Steganography Cipher
S1 Hit ASAP treat (Forward, paragraph one, line one.)
S2 False
S3.True
S4.False

Chapter Four

Keyboard Cipher
KB1 Computer keyboard key device
KB2 Can create many different keys
KB3 How can we find the proper key
KB4 See next chapter for key construction

Chapter Five

Keyword Quiz
KW-1. Correct
KW-2. Incorrect, E cannot = e
KW-3. Correct
KW-4. Incorrect ”r” in keyword “cryptogram” cannot be repeated

Aristocrat Cipher
A-Example: The cryptographer is always checking for small words or single letter words that provide a good entry point into the disguised message.

A-1. Solvers are delighted when they discover the repeated use of the most frequent vowel in a cipher.
A-2. Delighted
A-3. "e"
A-4. Four
A-5. The kiddee korner column is a good way to learn and become familiar with many of the little tools those are helpful in solving aristocrats

.

A-6. a, e, o, t
A-7. B, P and V appear once, JQXZ do not appear at all.
A-8. The same
A-9. The corn farmers in the central and northern parts of the United States look for corn stalks to be knee high by the Fourth of July.
A-10. Over the river and through the wood, And straight through the barnyard gate. We seem to go extremely slow, It is so hard to wait. Over the river and through the wood, Now grandmother's cap I spy! Hurrah for the fun! Is the pudding done? Hurrah for the pumpkin pie. Lydia Child. (Keyword – thanksgiving)
A-11.Christmas, Hanukkah, and Kwanza come but once a year. When they come they bring great cheer. A haven that peace may grace may well be within our own embrace should goodwill occupy our personal space.(Keyword – HOLIDAYS

Chapter Seven

Null Cipher

N-1. Try a null. (3 rd. letter each word)
N-2. Every other letter.
N-3. See how easy it is. (Last letter of each word.)
N-4. Write a friend. (Letter following each vowel.)
N-5. (Third letter of each word.) Come solve this null cipher and send it in for credit.
N-6. (Fourth letter of each word.) Dashing through the snow.

Chapter Eight

Construction Quiz

C-1. False
C-2. False
C-3. False
C-4. True

Keyword Alphabet

KW-1. No
KW-2. Plaintext
KW-3. Four

Chapter Nine

Keyword Alphabet

KW-1. It is easy to write and send disguised messages.

KW-2. K2
KW-3. Four
KW-4. False
KW-5. Keyword begins under pt letter. "b."
KW-6. Keyword PETUNIA is surrounded by the remainder of the alphabet.
KW-7. LUCKY
KW-8. True

Chapter Ten

Patristocrat Quiz

P-1 . Letter frequency count .
P-2 . Six
P-3 . True
P-4 . Steganographic
P-5 False
P-6 True
P-7 bigger
P-8 "t"
P-9 . False
P-10 . False
P-11. True
P-12 . True
P-13. Quarrelsome quaint quint quail quarry quickens quest quite quivering quixotic quorum quit quirky questionnaire.
P-14. All alliteration designs are always able acts of actionable art also akin to acute adages and attentive application.
Keyword - ARTICHOKES

Chapter Eleven

JA 2002 Baconian

E-7 – Knowledge comes but wisdom lingers.

Concealment cipher

BC-1 This message…..
BC-2- Look for a conflict
BC-3 –Happy Holidays to all and to all a good solve. Submit for SOLS credit.
BC-4 – Cryptic Xmas.
BC-5 – Baconians are fun ciphers.

```
CT LETTERS  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Baconian    ababaaaaabbaaabbaaaababababa
```

BC-6 – Each must row with his own oars.

Chapter Twelve

Xenocrypt Keyword X-3 – SIERRABLANCA
Xenocrypt Keyword X-1 – CHAPEAU

X-2 – Keyword QUALCHE**abcdefghikllmnopqrstuvwxyz**

ZQUALCHEBDFGIJKMNOPRSTVWXY

Esco e salgo ne' placidi rai, lo splendente universe a verder, a bruciar ne l' amor che bramai, che non volli qui impuro goder.

Chapter Thirteen

Polybius Square PS-1 – TYRO (Horizontal) A Young Tyro solver who decrypts Tyro Grams is a gram cracker.

PS-2 – HORSE (Vertical) Excess energy is wasted on the youth.

PS-3 – SOUTH PACIFIC (Horizontal) I'm going to wash that man right out of my hair and send him on his way.

PS-4 - POLYBIUS (Vertical) Have a holly jolly Christmas it's the best time of the year. I don't know if there'll be snow but have a cup of cheer. Burl Ives.

Chapter Fourteen

Checkerboard Cipher CB-1 – BLUE (Horizontal)

Polybius Square CB-2 – TURQOISE - Reverse Spiral, Beginning Upper Left Corner

CB-3 – BANKS, OUTER, ROADBLOCK, Vertical, Upper Left Corner beginning – The shortest distance between two is under construction.

Chapter Fifteen

Foursquare Cipher FS-1 – What do Nabisco and the young tyros have in common. Why that is easy. They both produce gram crackers.

Foursquare Keyword FS-2 - SALTINE, NABISCO (Horizontal)

FS-3 – BOWL, GOLDFISH (Vertical)

Foursquare Cipher FS-4 – It's a complex fate being an American for one of the responsibilities it entails is fighting against a superstition valuation of Europe. Henry Jales.

FS-5 – STEAM, TRAIN, Vertical. All railroad men from the conductors to the engineers know that the steam that blows the whistle can't be used to turn the wheels x.

Chapter Sixteen

Railfence Cipher RFC-1 – Paper and pencil solutions of Railfence ciphers require a lot of trial and error for success. (Four rails, two offsets.)

RFC-2 – XX This four rail cipher message contains two offsets.

Redefence Cipher SO E-11 -After all is said and done, more is said than done. 2,1,3

MA E-8 – Thousands of years ago cats were worshipped as Gods and cats have never forgotten it. (2, 4, 1, 3, 5)

Chapter Seventeen

Polyalphabetic Quagmire Q-1 – The shortest recorded period of time in history lies between the minute you put something away for a rainy day and the unexpected arrival of rain.

Q-2 – RAIN STORM, ATMOSPHERIC

Chapter Nineteen

Vigenere Cipher V-1 – THERE – The word "there" is one of the most used words in the English language and begins many sentences

V-2 – SENORITA – We can remember the most used letters

in the English language with the word senorita that uses all of the common ones.

Variant Cipher, MJ 2008 E-2 – ROBOTICALLY – Part of the inhumanity of the computer is that once it is completely programmed and working smoothly it is completely honest. Isaac Asimov.

Beaufort Cipher, JF 2008 E-2 – FURIOUS – Speak when you are angry and you will make the best speech you will ever regret by Ambrose Bierce.

Gronsfeld Cipher, MA 2008 E-3 - 8971889 – Plato did not jog or take maintenance medications. In fact he said attention to Health is the greatest hindrance to life.

Chapter Twenty

Cryptarithms C-1 - NUMBERSJOY
C-2 – FINESTHOUR

Square Root SR-1 – FIVEGUARDS

Cube Root CR-1 – OLDYEARSUP

Factorial F-1 – FIVEANDTWO

Logarithm L-1 - EASYTOFIND
C-3 – CRYPTOGAME
C-4 – LUMBERJACK
C-5 – EIGHTYFOUR
C-6 - MULTIPROSE
C-7 - NEIGHBORLY

Chapter Twenty-one

Affine & Hill Ciphers A&H-1 – On Thanksgiving Day all over America families sit down to dinner at the same moment halftime. (Add digits.)
A&H-2 – Santa's whiskers need no trimming. He kisses kids Not the wimmin. Burma Shave. (Add digits.)
A&H-3 – Cryptogram
A&H-4 – Algebra
FR-1 – 3/8
FR-2 - ½
FR-3 – 2/11
FR-4 - What has four wheels and flies? A garbage truck.
A&H-5 – `abcdefghijklmnopqrstuvwxyz`
`DINSXCHMRWBGLQVAFKPUZEJOTY`
A&H-6 – The worst prison is a closed mind.

Chapter Twenty-two

Fractionated Morse MJ2000. E-13 – MORSE. The lead type used by……
FM-1 – CIPHER – When it rains it pours. Ancient Proverb.

Morbit Cipher M-1 – Trick or treat, was no threat, Bristled

Chapter Twenty-three

Ragbaby Cipher

R-1 – (COMPATIBLY) My parents had an awful time getting married. Mom wouldn't marry him when he was drunk and Dad wouldn't marry her when he was sober.

R-2 – (IMPROVE) Were all things perfect here there would be naught for man to do; if what is old were good enough we'd never need the new.

R-3 – (TIDYUPSOME) Cleaning your house while the kids are still growing up is like shoveling the walk before it stops snowing. Phyllis Diller

Chapter Twenty-four

Route Transposition Cipher

RT-1 – Four score and seven years ago. stubble caused Mortisha's sweat. Burma Shave.

M-2 – The man who gets his lady's applause must Act not look like Santa Claus. Burma Shave.

M-3 – If you cannot pay your bills be thankful that you are not one of your creditors.

RT-2 – Entered – Horizontal, Exit Reversing Horizontal, Start Top Right – Most Children descended from a long line their Mothers listened to.

RT-3 – Entered Horizontal, Exit Reversing Vertical, Start Bottom Right – She was only the opticians daughter, two glasses and she made a spectacle of herself.

RT-4 - Entered Horizontal, Exit Vertical, Start Top Left – The reward for a job well Done is to have done it so well x.

RT-5 - Entered Vertical, Exit Horizontal, Start Top Left – The shortest distance between two points is under construction x.

RT-6 - Entered Vertical, Exit Horizontal, Start Top Left – The clairvoyant society will not have its usual meeting this month due to unforeseen circumstances.

Appendix III – A. This message is used to illustrate the only true secret system of concealment is the one that conceals the existence of a secret. Send Sols to Sol Ed. (Word endings, consonant = a, vowel = b.)

B. Please submit solution for credit. (Word endings = Vowel - a
Consonant = b)