CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI
January 13, 1996
Revision 0

LECTURE 6
XENOCRYPT MORPHOLOGY
Part II

SUMMARY

In Lecture 6, we continue our review of materials related to ciphers created in languages other than English. In order to augment PHOENIX's soon to be published ACA Xenocrypt Handbook, we will focus on six diverse systems: Arabic, Russian, Chinese, Latin, Norwegian, and Hungarian. Each offers a unique perspective in deciphering communications and supports the cultural universal concept presented in Lecture 5.

Lecture 7 will give practical language data for Xenocrypts commonly published in the Cryptogram - French, Italian, Spanish, Portuguese. [I will not cover either Esperanto or Interlinguia. I consider both as useful as advanced Hittite in modern communications.]

SHAREWARE

I have transmitted to the Crypto Drop Box word translation software for Russian, Spanish, German, Danish and Portuguese. Single use license is granted. Also, I have sent a Russian tutorial program to NORTH DECODER to put on the Crypto Drop

ARABIAN CONTRIBUTIONS TO CRYPTOLOGY

A colleague of mine in Sweden sent me an interesting reminder of the historical foundations of cryptology. He suggested that I include in one of my lectures a discussion of Dr. Ibrahim A. Al-Kadi's outstanding 1990 paper to the Swedish Royal Institute of Technology in Stockholm regarding the Arabic contributions to cryptology.

Dr. Al-Kadi reported on the Arabic scientist by the name of Abu Yusuf Yaqub ibn Is-haq ibn as Sabbah ibn 'omran ibn Ismail Al-Kindi, who authored a book on cryptology the "Risalah fi Istikhraj al-Mu'amma" (Manuscript for the Deciphering Cryptographic Messages) circa 750 AD. Al-Kindi introduced cryptanalysis techniques, classification of ciphers, Arabic Phonetics and Syntax and most importantly described the use of several statistical techniques for cryptanalysis. [This book apparently antedates other cryptology references by 300 years.] [It also predates writings on probability and statistics by Pascal and Fermat by nearly 800 years.]

Dr. Al-Kadi also reported on the mathematical writings of Al-Khwarizmi (780-847) who introduced common technical terms such as 'zero', 'cipher', 'algorithm', 'algebra' and 'Arabic numerals.' The decimal number system and the concept of zero were originally developed in India.

The Arabs translated in the early ninth century, Brahmagupta's "Siddharta" from Sanscrit into Arabic. The new numerals were quickly adopted through-out the Islamic empire from China to Spain. Translations of Al-Khwarizmi's book on arithmetic by Robert of Chester, John of Halifax and the Italian Leonardo of Pisa, aka Fibonacci strongly advocated the use of Arabic numerals over the previous Roman Standard Numerals (I,V,X,C,D,M).

The Roman system was very cumbersome because there was no concept of zero or (empty space). The concept of zero which we all think of as natural was just the opposite in medieval Europe. In Sanscrit, the zero was called "sunya" or "empty". The Arabs translated the Indian into the Arabic equivalent "sifr". Europeans adopted the concept and symbol but not name, but transformed it into Latin equivalent "cifra" and "cephirium" {Fibonnaci did this}. The Italian equivalent of these words "zefiro", "zefro" and "zevero". The latter was shortened to "Zero".

The French formed the word "chiffre" and conceded the Italian word "zero". The English used "zero" and "Cipher" from the word ciphering as a means of computing. The Germans used the words "ziffer" and "chiffer".

The concept of zero or sifr or cipher was so confusing and ambiguous to common Europeans that in arguments people would say "talk clearly and not so far fetched as a cipher". Cipher came to mean concealment of clear messages or simply encryption. Dr. Al-Kadi concluded that the Arabic word sifr, for the digit zero, developed into the European technical term for encryption. [KADI], [ALKA], [MRAY], [YOUS], [BADE] ,[NIC7]

NOTES ON RUSSIAN LANGUAGE

Reference [DAVI] gives one of the better breakdowns of the modern Russian Alphabet (Soviet, post 1918) for solving Russian Cryptograms in "The Cryptogram".

Friedman presents detailed Russian cryptographic data in Volume 2 of his Military Cryptanalytics series. [FR2]

A prime difficulty for English speaking students of Russian is the scarcity of linguistic cognates in the two languages. Russian is more complex than other romantic languages which have many common word derivatives. The highly inflected Russian grammar aids rather than hinders the cryptographer by supplying him with valuable tools for decrypting.

My keyboard and supporting software does not permit a comfortable translation of the Cyrillic, so I refer you to the September-October 1976 Cryptogram for a survey of Russian and several Xenocrypt examples.

RUSSIAN KRIPTOGRAMMA COLLECTION

ELINT

Radio communications can be heard which vary in frequency from below the broadcast band, to almost the upper edge of the radio spectrum (Ku-band satellite communications.)

Common bands are:

VLF (Very Low Frequency): 3 to 30 kHz
LF (Low Frequency): 30 to 300 kHz
MF (Medium Frequency): 300 kHz to 3 MHz
HF (High Frequency): 3 to 30 MHz
VHF (Very High Frequency): 30 to 300 MHz
UHF (Ultra High Frequency): 300 to 3000 MHz

Whereas, VHF and UHF frequency ranges are occupied by cellular phones, police, fire and government communications, the bulk of HF region is devoted to COMINT signals. You should be able to hear traffic from all over the globe, rather than the 50-75 mile limit on the VHF and UHF bands. Three types of HF radio communications may be heard/intercepted: continuous wave (CW/Morse Code), single side band (SSB), and radio teletype (RTTY). The Cubans seem to favor the latter form of communication, especially from their revitalized center at Lourdes.

Tom Roach [ROAC] has been monitoring Russian messages for some time. He uses a Watkins-Johnson HF-1000 receiver, a Rhombic antenna, a Singer MT-5 Spectrum Analyzer, a Universal —7000 decoder (allows viewing the Russian in its native Cyrillic alphabet) a Sony TCD-07 recorder, and Hitachi V-302F Oscilloscope with X/Y tuning capability for RTTY communications.

[ROAC] suggests that the best hunting grounds for Russian RTTY traffic are:

4205.5 to 4207.0 kHz
6300.5 to 6311.5 kHz
8396.5 to 8414.5 kHz
12560.0 to 12576.5 kHz
16785.0 to 16804.5 kHz
18893.0 to 18898.0 kHz
22352.0 to 22374.0 khz
25193.0 to 25208.0 khz

and

6385 kHz (Morse) at around 1400 UTC

[ROAC] provides the reader with common abbreviations used in Russian RTTY and Morse traffic. His book describes the delicate art (and guess work required) in traffic analysis of Russian Kriptogramma messages between ship to shore.

Roach has identified several types of Russian messages:

SESS KRIPTOGRAMMA - originated by Soviet Space Event Support Ships (SESS).

KRIPTOGRAMMA NA PERFOLENTE - refers to a key additive (originally a paper tape Vernam type series.)

KRIPTOGRAMMA KODA - code book transmissions.

KRIPTOGRAMMA ADMIN - Super enciphered communications.

Other types of messages [ROAC] identified DISP/1 to report disposition of ships, PAGODA messages for weather reports, MORE messages to report administrative and sea conditions, Personal Itinerary, Fuel related, 10 slash, PARTI messages to discuss status of ship's holds and bunkers.

RUSSKAYA KRIPTOLOGIA HISTORICA

Russian achievements in the art of cryptography rank first rate to say the least. Three of my favorite cipher Russian systems are: 1) Nihilist, 2) VIC - Disruption (aka straddling bipartite monoalphabetic substitution super-enciphered by modified double transposition) and 3) the One-Time Pad. Each of these systems introduced tactical advantages for adverse communication and had limited disadvantages for their service.

NIHILIST SUBSTITUTION

For some reason, Russian prisoners were not allowed computers in their cells. Inmates were forbidden to talk, and to outwit their jailers they invented a "knock" system to indicate the rows and columns of a simple checkerboard (Polybius square at 5x5 for English or 6x6 for 35 Russian letters). For ex:

```
   1  2  3  4  5

1  U  N  Ij T  E
2  D  S  A  O  F      KW=United States Of
3  M  R  C  B  G          America
4  H  K  L  P  Q      i/j = same cell
5  V  W  X  Y  Z      repeats omitted


PT: g o t   a   c i g a r e t t e ?
CT: 35 24 14 23 33   13 35 23 32 15    14 14 15
```

Prisoners memorized the proper numbers and "talked" at about 10-15 words per minute. One of the advantages was that it afforded communication by a great variety of media - anything that could be dotted, knotted, pierced, flashed or indicate numerals in any way could be used. The innocuous letter was always suspicious. [KAH1]

Cipher text letters were indicated by the number of letters written together; breaks in count by spaces in handwriting; upstrokes, downstrokes, thumbnail prints, all subtly used to bootleg secrets in and out of prisons. The system was universal in penal institutions. American POW's used it in Vietnam. [LEWY], [SOLZ]

Transposition of the KW provided a further mixed alphabet:

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

taken off by columns:

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

the Polybius square would be:

```
      1  2  3  4  5

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

The Nihilists, so named for their opposition to the czarist regime, added a repeating numerical KW . Making the cipher a periodic similar to the Vigenere but with additional weaknesses.

```
Let KW = ARISE     22 53 45 41 15

PT:   bomb winter palace
NT:   11 42 43 11 21 45 34 52 15 53 44 22 14 22 25 15
Key:  22 53 45 41 15 22 53 45 41 15 22 53 45 41 15 22

CT:   33 97 88 52 36   67 87 97 56 68   66 75 59 63 40   37
```

or with bifurcation:

```
   33978 85236 67879 75668 66755 96340 37774

      nulls=774
```

NIHILIST TRANSPOSITION

A simpler form of the Nihilist was in double transposition. The plain-text was written in by rows (or diagonals); a keyword switched the rows; a same or different keyword switched the columns, and the resulting cipher text was removed by columns or by one of forty (40) or more routes out of the square.

ex: KW = SCOTIA or 524631

PT: let us hear from you at once concerning jewels xxxx

```
   Transpose by Columns                Transpose by Rows

    S  C  O  T  I  A
    5  2  4  6  3  1                       1  2  3  4  5  6

1   S  E  U  H  T  L  (let us h)      S 5  E  U  J  W  T  O
2   R  A  F  O  R  E                  C 2  R  A  F  O  R  E
3   A  Y  U  T  O  M                  O 4  A  N  E  B  C  O
4   A  N  E  B  C  O                  T 6  X  L  X  X  S  E
5   E  U  J  W  T  O                  I 3  A  Y  U  T  O  M
6   X  L  X  X  S  E                  A 1  S  E  U  H  T  L
```

X= bad choice for nulls

The resulting cryptogram:

E U J W T O R A F O R E A N E B C O X L X X S E A

Y U T O M S E U H T L.

(message length and 5th group are entries to solution)

Clues to cryptanalysis of the Nihilist systems were reconstructing the routes, evenness of distribution of vowels, period determination and digram/trigram frequency in cipher text. The USA Army for many years used a similar system. Reference [COUR] discusses the U.S. Army Double Transposition Cipher in detail.

VIC-DISRUPTION CIPHER

The Vic-Disruption Cipher brought the old Nihilist Substitution to a peak of perfection. It merged the straddling checkerboard with the one-time key. It increased the efficiency of the checkerboard by specifically giving the high frequency letters (O,S,N,E,A; P,G) the single digits (along with two low frequency letters). The seven letters: 'snegopa' comprise about 40% of normal Russian text. Let me focus on interesting elements.

STRADDLING BIPARTITE MONOALPHABETIC SUBSTITUTION SUPER-ENCIPHERED BY MODIFIED DOUBLE TRANSPOSITION or simply, VIC - DISRUPTION or just "VIC."

The VIC algorithm is described as follows:

The plain text is encoded by a Substitution Table (ST). The intermediate cipher text [ICT] is then passed through two (2) transposition tables (TT1 and TT2), each performing a different transposition on the ICT.

TT1 performs a simple columnar transposition: the ICT is placed in TT1 by rows and removed by columns in the order of TT1's columnar key and transcribed into TT2.

TT2 is vertically partitioned into Disruption , or D areas. These partitions are formed by diagonals extending down the table to the right boundary in columnar key order. The first D area begins under column keynumber 1 and extends down to the right border of TT2. A row is skipped. The second D area starts under keynumber 2. The process continues for the entire key. The number of rows in TT2 .ne. TT1 and is calculated by dividing the number of cipher text input digits by the width of the table.

The ICT from TT1 is inscribed into TT2 horizontally from left to right skipping the D areas. When all the non D area is filled , then the D areas are filled in the same way. The cipher text is removed by column per key order without regard to the D areas.

KEYS

The VIC system used four memorized keys. Key 1 - the date of WWII victory over Japan - 3/9/1945; Key 2 - the sequence of 5 numbers like pi - 3.1415; Key 3 - the first 20 letters of the "Lone Accordion", or famous Russian song/poem, and Key 4 - the agent number, say 7. Key 1 was changed regularly. Key 4 was changed irregularly.

DISRUPTION ALGORITHM

The keys were used to generate the keys for transposition and the coordinates for a checkerboard for substitution through a complex LRE (Left to right enumeration) logic. The process injected an arbitrary 5 number group into the cipher text which strongly influenced the end result. This group changed from message to message, so the enciphering keys (and cipher text) would bear no exploitable relationship to each other. Not only did TT1 and TT2 keys differ but also the widths of the blocks did as well.

The coordinates kept changing. The D areas prevented the analyst from back derivation of the first TT1. The D areas increased the difficulty of finding the pattern and the straddling effect on the checkerboard increased the difficulty of frequency counts. Although not impossible to break, in practice a tough monkey indeed. The FBI failed for four years to solve it.

KEY GENERATION

All arithmetic was done modulo 10, without carrying or borrowing.

An English ST table might look like this:

	4	9	1	6	0	8	5	2	3	7
	R	E	A	S	O	N	b			
2	B	C	D	F	G	H	J	K	L	M
3	P	Q	I	U	V	W	X	T	Z	1
7	3	5	7	9	.	,	b	$	%	-

b = space character

top line are among most frequent English letters similar to 'SNEGOPAD' in Russian.

Ambiguity in decipherment is reduced because the last three slots in the first row are empty and the first coordinate of the two coordinate characters is unique.

[VOGE] gives a detailed look at the key generation recursion mathematics for this cipher. It describes the LRE (left to right enumeration) process in nauseating detail.

The TT1 and TT2 are built up on the recursion sequence X(i+5) = X(i) + X(i+1) for i = 1,5 using mod 10 math. Key 1 was used to insert at end of message (5th unit in this example). Key 1 was also the initial point for a series of manipulations with Key 2,3,and 4.

RUSSIAN IMPROVEMENTS

Hayhanen incorporated some nasty refinements. Before encipherment, the plain text was bifurcated and the two halves switched so that the standard beginnings and endings could not be identified. The ST contained a 'message starts' character. The ST was extended to ASCII characters. The VIC encipherment consisted of one round. After 1970, with the advent of programmable hand calculators, a multiple round version was produced.

MERITS

Consisting of simple enough elements, this cipher is one tough monkey.

The complication in substitution was the straddling device on the checkerboard. The irregular alternating of coordinates of two different lengths makes it harder for cryptanalysis by dividing the list into proper pairs and singletons.

The complication in the transposition was the Disruption areas. D areas blocked the reconstruction of the first tableau. A correct sorting of the columns is forestalled by the D areas.

The keying method is brutal on the agent in a hurry. Same with his analyst counterpart. Key recovery does not permit direct anagraming between messages. The four keys are mnemonics.

The cipher text is only 62% increased over plain text because of the high frequency letters in the first row of the ST.

ONE-TIME PAD REVISITED

The One-Time Pad was covered in LECTURE 3 and we are reminded that it is truly an unbreakable cipher system. There are many descriptions of this cipher. Bruce Schneier's discussions are quite relevant. [SCHN] , [SCH2]

FRESH KEY DRAWBACK

The One-Time Pad has a drawback - the quantities of fresh key required. For military messages in the field (a fluid situation) a practical limit is reached. It is impossible to produce and distribute sufficient fresh key to the units. During WWII, the US Army's European theater HQs transmitted, even before the Normandy invasion, 2 million five (5) letter code groups a day! It would of therefore consumed 10 million letters of key every 24 hours - the equivalent of a shelf of 20 average books. [SCHN]

RANDOMNESS

The real issue for the One-Time Pad, is that the keys must be truly random. Attacks against the One-Time Pad must be against the method used to generate the key itself. Pseudo-random number generators don't count; often they have nonrandom properties. Reference [SCHN] Chapter 15, discusses in detail random sequence generators and stream cipher. [SCHN], [KAHN],[RHEE]

CHINESE CRYPTOGRAPHY

ENCIPHERING

Dr. August suggests that the Four Corner System and the Chinese Phonetic Alphabet System lend themselves to manual cryptographic treatment. His treatment of these two systems is easier to understand than some military texts on the subject. [AUG1]

Let a message in Chinese be X1, X2, X3.. Xn, where Xi represents a character. The code for Xi is vector union of three sets, v1, v2, and v3. v1 is a single digit code for tone v2 is a four or five digit Four Corner representation code, and v3 is a 6 digit phonetic code representing 3 phonetic symbols each by two digits. [AUG2]

$$Xj = \bigcup_{1-3}^{3} v1 \qquad \text{eq } 1$$

This union is called an asymmetric code.

The Four Corner System encodes characters into several generic shapes. Each character is broken into four (4) quadrants, and assigned a digit to the generic shape that best corresponds to the actual shape.

The Chinese Phonetic Alphabet is Pinyin with symbols instead of English letters. Each symbol corresponds to one of 37 ordered phonetic sounds. The 21 initial, 3 medial and 13 finals are a unique ordered set - a true alphabet.

The strength of encryption of Chinese is dependent on the specific Chinese encoding character schemes. Three cases are:

1). Phonetic Alphabet Only: The cipher must include both a transposition (to hide cohesion and positional limitations) and a substitution (to hide the frequency patterns.)

2) Four Corner System: The cipher can be based on ring operations [performed on codewords rather than characters, either on an individual basis or over the whole message; the name comes from the algebraic operations involving integers mod 10 or mod 37] which super-encipher the encoded text.

3) Combination of Methods 1) and 2): A text encoded by a combination of both methods will need a cipher employing both transposition and substitution. The transposition needs to mix up the symbols within codewords and the message itself. This prevents a bifurcated analysis. [AUG1], [AUG2]

CRYPTANALYSIS OF CHINESE CIPHERS

A) Phonetic Alphabet:

```
12.6   7   5.7  4.8     4.2   3.8   3.4    3   2.9 2.8 2.4  2.2
 I     U    D   ENG/E   an/en  SH   X/ZH   J/u  G   O   ao   H

2.1   2           1.9  1.8   1.6    1.4  1.3   1.2  1.1
ang   a/b/ai/B/z   ei   Q    ou/M    ie   L     F    R


0.8   0.7  0.6    0.3  0.1
 t    n/c   ch    k/s   p/el
```

Initials: sh, d

Medials: i

Finals: e, en, eng, in, un, ing, ong

Phi for monalphabetic substitution = 0.051
(random text = 0.027)

Common Digraphs: ji, ieng, ueng, gu, de, ian, iie, li, ien, qi, xi, uo, izh, zu, shi

Positional Limitations:

1. Initials follow a medial or final.
2. Finals follow an initial or medial.
3. [zh, ch, sh] do not combine with i or u'.
4. [j, q, x] do not combine with a or e finals.
5. qa, qan = no but quan, qian, qia = yes
6. no double phonetics in a single codeword.
7. medials double frequently.
8. 13 limits on combinations within a codeword.

Approximately 63% of characters require 2 phonetic symbols.
About 1/3 were three long, and about 4% are one symbol.

Tone indicator digits were about 22--23% likely.

B) Four Corner

Digital frequencies: 0 = .30
1 = .14
2 = .15
3 = .07
4 = .10
5 = .03
6 = .07
7 = .08
8 = .04
9 = .02

Phi value = 0.160 compared to random text value of 0.100

Dr. August presents a table of digraphs. [AUG2] Combinations of Xn - Ym where n= 0-9 and m=0,1,2,3,4,7 showed highest frequencies of text encoded with 5 digit scheme.

DEPENDENCE

In Chinese there is more dependence between encoding and enciphering operations than in English. The choice of the encoding system influences the type of enciphering operations. Dr. August provides solved examples of the above systems. [AUG2]

HISTORICAL PERSPECTIVES

China appears to have had a much delayed entry into the cipher business. Partially because so many Chinese did not read or write, and partially because the language was so complex, Chinese cryptography was limited until the 19 century. But there were seeds:

The Chinese strategist Sun Tzu (500 b.c.) recommended a true but small code, which limited the plaintext to 40 elements and assigned them to the first 40 characters of a poem, forming a substitution table. Richard Deacon describes a method of code encryption which the secret society Triads used in the early 1800's. [DEAC] The Tong's in San Francisco used the same system. This method limited the plaintext space and based codewords on multiples of three.

The "Inner Ring" techniques taught to Sa Bu Nim's (teachers) by the masters of Korean Tae Kwon Do (which came from the Ancient Tae Kwan and before that Kung Fu) were passed on by means of codeword transposition ciphers. [CHOI] In 1985, Sun Yat-Sen used codes to transmit information by telegraph. [TUKK]) During WWII, Herbert Yardley taught Kuomintang soldiers to cryptanalyze Japanese ciphers. However, the Japanese had already outpaced the Chinese in cryptanalytical abilities.

Japan's Chuo tokujobu (Central Bureau Of Signal Intelligence) was responsible for crypto-communication and signal intelligence, including cryptanalysis, translation, interception, and direction finding against the Soviet Union, China and Britain. It began operations in 1921. [YUKI],[YAR1]

In May 1928, the Angohan (Codes and Ciphers Office) obtained excellent results in intercepting and decoding Chinese codes during the Sino-Japanese clash at Tsinan between Chiang Kaishek's Northern Expeditionary Army and the IJA (Imperial Japanese Army). [FUMI]

The warlord Chang Tso-lin was murdered in June 1928. Angohan succeeded in decoding "Young Marshal" Chang Hsueh-liang's secret communications and made a substantial contribution to the understanding of the warlord politics of Manchuria. [SANB]

The Anjohan not only mastered the basics of Chinese codes and ciphers but also broke the Nanking Government and the Chinese Legation codes in Tokyo. [YOKO]

The Chinese codes in 1935 were called "Mingma". They were basically made up of four digit numbers. The Chinese did not encode the name of either the sender or receiver, nor the date or the time of the message. The China Garrison Army's Tokujohan office was able to disclose the composition, strength, and activities of Chiang Kai-shek's branch armies, such as those led by Sung Che-yuan and Chang Hseuh-liang. It was not able to decode the Chinese Communist or Air Force messages. [HIDE]

By the time of the 1937 Sino-Japanese War, Japanese cryptanalytical experts had been able to greatly expand their knowledge of the Chinese system of codes and ciphers, as well as improve their decoding skills. About 80% of what was intercepted was decoded. This included military and diplomatic codes but not the Communist code messages. [EIIC]

Chinese Nationalists upgraded their Mingma codes in 1938. They adopted a different system, called tokushu daihon (special code book) in Japanese which complicated by mixing compound words. By October, 1940, Chiang Kai-shek's main forces were using a repeating key system. This stumped the Japanese cryptanalysts for a short time, then they returned to a 75% decoding level during the war. They continued to make great contributions to major military operations in China. [HIDE]

The Japanese broke the Kuomintang codes during the Chungyuang Operation in the Southern Shansi or Chungt'iao Mountain Campaign. [CHUN] In February 1941, significant penetration of Communist signal traffic was obtained. [YOKO]

The tokujo operations against the North China Area Army and the Chinese Communist codes was tragic failure. [HISA] The IJA's China experts held a highly negative image towards the Chinese.

This may have prejudiced their attitude towards intelligence estimates of China and the Chinese which in turn adversely affected their operational (crypto-intelligence) thinking on China in general. [THEO]

When the Sian mutiny broke out and Chiang Kai-shek was kidnapped in December 1936, Major General Isogai (IJA's leading expert in COMINT for China) toasted (more like roasted) the demise of Chiang. Colonel Kanji Ishiwara (Japan's chief military strategist) deplored the incident because he felt China was on the brink of unity because of Chiang Kai-shek's efforts. He considered the ability to read Chiang's codes just a matter of doing the business of war. [SHIN]

LATIN

BRASSPOUNDER gives us a good introduction to Latin in Reference [LATI]. Until modern times Latin was a dominant language in schools, churches, and state in Western Europe. Professionals use Latin to confuse the general populace. Latin is closely related to all of the Romance languages.

The Latin alphabet is the same as the English-language alphabet, except that it has no equivalents for K, W, J, or U. These have crept into current usage for their phonetic value. The J replaced I as in hic jacet instead of the classical hic iacet. The letter W has no equivalent. The letter U was the Greek Y, and in classical times was written as a U. C is now used to form the hard sound as in CEL instead of KEL. A double UU approximated a W. Latin therefore is a 25 letter alphabet.

The order of frequency according to Kluber, reduced to percentages, taken from reference [TRAI]:

I - 10.1	M - 3.4	V - 0.7
E - 9.2	C - 3.3	X - 0.6
U - 7.4	P - 3.0	H - 0.5
T - 7.2	L - 2.1	J - 0
A - 7.2	D - 1.7	K - 0
S - 6.8	G - 1.4	Y - 0
R - 6.8	Q - 1.3	Z - 0
N - 6.0	B - 1.2	
O - 4.4	F - 0.9	

Vowels: I E U A O

Consonants: T S R N M C P L D Q B F V X H

Initials: S I A P E Q C V M D N F H R T U L O G J
Finals: S E T M A I O N D R L C U

Doubled Letters: S L M P T C N R U Z

Vowel Combinations:
AE AU AI ; EA EI EO ; IA IO IE IAE ; OA OE OI OAE OIA ; UA UE UI UO UU UAE UIA UIU

Consonant combinations:
NT ST ND SP PB CT SG NS NP LT

Frequent reversals:
UM EN ER NT TI TE ON RT RE ES IS ME IT TA US SE IC TU ST IE PE CI RU

Digraph endings:

IS UM US AM AE TA NT EN RE OS AS UE ES RA AT IT ET IA IO OB ST SE TE RI OR UR ER NI RI UI NO EL DI PE NA VA NS ED IN NE SA MO SI SO RO

Trigraph word endings:
ERE QUE UNT RIS RUS IUM LIS LUM TIS UAM UOD NTA ARE IAM NIS RAT NEM ROS TAS TES TIO ANT ATA CAE CUM ENT ITA IUS LAE NAM NES NIA RUM URA VIS TEM TAE TUS

Favorite letter positions:

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

H=head, first letter, 2H = second letter, E=last letter, 2E= next to last letter

Common short words:

IN ET AD SI PER UBI SED UNA VIA HIC PRO CUM QUI QUO QUOD IPSE ATQUE QUARE QUIDEM

Pattern words:
NON BENE FERE QUISQUE

Vowel percentage: 44%
Vowel / consonant ratio: 8/10
Average word length: 7

One-letter words: A E I O

Two-letter words:
AB AC AD AB AT DA DE DO EA EI EN EO ES ET EX HI ID II IN IS IT ME NE NI OB OS RE SI TE TU UT

Three letter words:
AGO ARA AUT AVE BIS COR CUM CUR DIU DUO DUX EGI EGO FIO HIC HOC
HUC IAM IBI IRA ITA IUS LEX LUX MOX MUS NAM NEC NIX NON NOX NUM
PAR PAX PER PES PRO QUA QUI QUO RES REX RUS SED SEX SIC SOL STO
SUM SUS TAM TUM UBI VAE VEL VIA VIR VIS VIX

Latin Bigram Table

Basis 10,000 letters and spaces from Reference [ALBE]

First Letter	Second Letter												
		A	E	I	O	U	B	C	D	F	G	H	K
	-	156	145	146	36	60	11	99	65	39	7	35	4
A	113		77	8		20	42	15	58		6		
E	197	27		7	7	1	5	26	18	4	11	1	
I	89	43	12	6	59	68	51	60	34	12	26	4	
O	61	1	3				10	37	19	1	2		
U	8	73	61	50	22	2	17	2	11				
B	15	12	26	33	3	22							
C	29	49	28	31	68	3		4				3	
D	53	16	61	87	9	17			3		1		
F	3	7	9	23	11	9				5			
G	2	5	18	14	4	10					1		
H		23	3	14	8	4							
K	4					8							
L	10	46	39	106	10	13			2		1		
M	248	28	33	28	22	23	1						
N	57	48	49	59	40	38		33	39	4	19		
P	2	12	34	12	43	14						1	
Q	4					167							
R	87	96	76	101	30	56	4	6	7	1	2	1	
S	276	14	64	83	30	47		34	1	2			
T	191	96	125	142	20	91						6	
V	3	7	42	24	27	1							
X	28	1	2	7				2					
Y										5			
Z	1												

First Letter	Second Letter											
	L	M	N	P	Q	R	S	T	V	X	Y	Z
	53	36	79	113	92	36	151	46	68	3		1
A	63	89	62	12	4	59	45	81	4	2		
E	18	78	85	11	21	175	84	93	3	35		
I	25	49	143	24	9	10	137	113	3	4		
O	13	27	134	6	4	65	46	13	5	2		
U	37	119	63	9		60	105	70	1			
B	1					4	5					
C	2					24		40			5	
D		2		1		1	2		2			
F	1					12						
G	1		13			8						
H												
K												
L	33							12				
M		7	10	13		5			2			
N			4			3		56	136	10		
P	17			3			42	15	11			
Q												
R	1	6	1	3		2	2	9	26	3	1	
S		7		5		11		39	72	3		7
T						19	23		35			
V												
X				6				1				
Y												
Z												

NORWEGIAN

Norwegian is a beautiful language which consists of two forms, Bokmal (Book Language) and Nynorsk. Book language is the generally read form. Norwegian is similar to English with the addition of three vowels AE, 0, A'. Foreign consonant letters are C, Q, W, X and Z. Based on 5153 letters, a frequency analysis reduced to 100 letters is:

16	8	7	6	5	4	2	1	-	0
E	RNS	T	AI	LDO	GKM	UVFHPA'	JBO	Y AE C	WXZQ

Average word length - 4.77 letters. Compound words are long.

IC = .0647

Vowels A, E I O - 33%
Consonants D L N R S T - 41% of letters

One- Letter Words:
I 81% A' 16% A 2% O A AE 0 1%

Two letter words:
OG 23% ER 14% EN 10% AV /DE 9% ET PA' AT FA' SA'
DA NA' OM VI JO SA JA MA' SE TO UT VE

Three letter words:
OPP 38% ENN 23% INN 15% OSS 15% ALL 8%

Four letter words:
OSGA' 15% BARE 12% ALLE 9% FOLK 9% HVEM SINE
STOR GATE GODT HVIS IDAG LAND MENS MIDT

Doubles:
LL KK NN TT MM SS PP GG RR DD FF

Digraphs:
EN ER DE ET TE ST NE OR RE KE AN ME SE SK

Reversals:
EN ER DE ET ES EL LI AV GE

Initials:
S FM D HAENT BKV GI JLP RU A0

Finals:
E RT N G S KM A A'DLV IO BPYAE FHU0

Phoenix's soon to be published ACA Xenocrypt Handbook gives further data on digraphs and trigraphs representing less than 2% of totals.

HUNGARIAN

Hungarian (aka Magyar) is related to Finnish and Estonian. Hungarian has 38 sounds based on a Latin alphabet. Reference [HUNG] shows the full alphabet as a combination of letters. There is no Q, W, or X in Hungarian. Only 23 Latin letters are used. Reference [HUNG] also gives Xenocrypt examples.

Hungarian has four special characteristics:

1. It agglutinates - adjectives, possessives are expressed by suffixes.

2. It has vowel harmony - they fall into high and low vowel categories. High - E, I, OE, UE and Low- A O U. In a word they are all either high or low.

3. It assimilates consonants - usually the third or fourth letter from the end. Many doubles.

4. It has no gender differentiation.

Per cent letter frequencies based on 10,001 letters:

E	16.04	K	4.47	D	1.93
A	12.55	I	4.29	B	1.78
T	8.35	M	4.11	H	1.42
O	6.56	R	3.48	J	0.99
S	6.56	G	3.16	F	0.94
L	5.66	U	2.33	C	0.52
N	5.49	Y	2.03	P	0.52
Z	4.79	V	1.94		

Doubles (in 10,001 letter count):

TT	104	BB	25	RR	10
SS	42	KK	24	II	9
LL	35	NN	22	GG	7
AA	31	ZZ	11		
EE	27	MM	11		

Most frequent bigrams:

OE	229	AL	126	SA	94
EL	225	AS	123	KA	91
TA	219	LE	118	ZA	90
SZ	207	NE	110	LA	89
ES	201	UE	110	ZO	88
EN	185	EM	110	AK	87
EG	155	GY	108	KE	87
ET	151	AZ	101	AM	86
TE	149	EK	97	KO	86
AN	145	LA	96	EZ	80
AT	136	AR	95	MA	79
ER	133	SE	95	RE	79
ME	127	TO	95		

Initials:
V E M K S A H T F N L B I O J C U P R G D

Finals:
T N K E A S I M L G Y Z R D O B U P C

Groups:

Vowels A E I O U	41.77 %
LNRST	29.54
JKQYZ	9.93
EATOS	50.06
EATOSLNZK	70.47
HJFCP	4.39

Simple words based on a count of 1,000 words:

ES - and (before vowels) 96
AZ - that 20
EGY - one 14
S - and 11
MEG - 6
EL - away 5
TE - thou 5
HA - if 4
ITT - here 3
A - one 68
EZ - this 17
NEM - no 6

Hungarian Bigram Table

Basis 10,000 letters and spaces from Reference [HUNG]

Second Letter

First Letter	A	B	C	D	E	F	G	H	I	J	K
A	31	41	4	22	15	22	56	55	33	28	87
B	57	25			52			1	3	1	
C	6				3				5		
D	28	1	1	3	48	3		3	15		1
E	28	26	3	47	27	21	155	19	19	21	97
F	7				21	3			25		
G	40	9			46	4	7	11	13	3	6
H	67				21				15		
I	34	7	6	16	9	1	26	2	9	5	59
J	35	1		6	16					3	1
K	91	6	3	1	87	6	4	2	38	1	24
L	96	5	3	7	118	7	6	4	15	10	18
M	79	18	5	1	127	5		9	58	5	3
N	59	7	8	40	110	7	9	2	18	1	38
O	3	11	1	13	229	1	25	2	1		51
P	7				16				3	3	3
R	50	1	13	10	79	5	6	1	19	1	10
S	94	3	1	5	95	5	1	8	18	5	22
T	219	10	3	3	149	1	6	14	59	5	19
U	4	1		12	110	1	9	2	4	4	1
V	89	5			61				13		
Y	41	1	1	1	43	1		5	18		2
Z	90			6	122	1	6	2	28	3	3

First Letter

First Letter	L	M	N	O	P	R	S	T	U	V	Y	Z
A	126	86	145	1	18	95	123	136	3	27		101
B	5	3	3	14		5	5	1	3			
C				3		1	34					
D	1	9	1	41		3	1	15	13	6		
E	225	110	185	1	18	133	201	151		37		80
F				18					19			1
G	4	7	1	15		7	6	6	7	12	108	4
H		1		37					1			
I	18	7	56	1	7	9	71	35	10	28		13
J			1	22			3	7	1			3
K	4	21	6	86		9	9	14	28	4		
L	35	31	15	57	4	6	7	73	6	13	24	6
M	6	11	7	35		2	17	9	14	8		2
N	6	11	22	22		3	19	72	11	12	57	15
O	65	33	62	1	1	41	37	49		4		26
P			1	11	1		2		2	2		1
R	9	11	4	42		10	18	41	16			
S	4	18	13	29		4	42	43	15	14	10	207
T	22	42	6	95	1	4	20	104	37	12	4	
U	19	3	12	2		9	7	24		3		6
V				21		2			3			
Y	6	15	3	14	2		2	16	6	23	3	
Z	11	2	6	88			3	18	49	21	9	11

LECTURE 5 HOMEWORK ANSWERS

Ger-3. Kalenderblatt August. K2 (Sonne) BRASSPOUNDER

QV FHOHIC ICMPC KQM IXWWM QW KML WFMPM KMI

*IQLQHI, KMI *PHWKICMLWI, KFPML KQM "*PHWKIC-

FOMI," KQM AMKML VMWIJP WXJP CQMLM VXMOMW.

Kw= LICHT

Im August steht die Sonne in der Naehe des Sirius, des Hundsterns daher die "Hundstages," die weder Mensch noch Tiere moegen.

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

After placing the crib at the 5th word, der, dess, and die were immediately identified.

Ger-4. Ungerechtes Schicksal. Eng. K4 GEMINATOR

Kw's = question /unfair

Student besteht Pruefung zum zweiten mal nicht wieso fragt der Freund Schicksalsschlag das selbe zimmer der selbe Professor die selben fragen.

```
PT: z q u e s t i o n a b c d f g h j k l m p r v w x y
CT: U N F A I R B C D E G H J K L M O P Q S T V W X Y Z
```

IRFJA DRGAI RAMRT VFAKF DLUFS UXABR ADSEQ

DBHMR XBAIC KVELR JAVKV AFDJI HMBHP IEQII

HMQEL JEIIA QGAUB SSAVJ AVIAQ GATVC KAIIC

VJBAI AQGAD KVELA D. hints: (zum zw-; zimm-)

The three part crib can only be located in one position. A first guess of ZIMMER gives der, die, and zweit. A guess of FREUND yields much of the in the rest of the text. Schicksalsschlag can be found in the dictionary.

Fre-1.

MON NOM square looks like this:

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

Split the cipher text after message group 13. Message reads: Que Noel vous soit des plus agreables et l'an nouve aplein de desirs accomplis.

HOMEWORK PROBLEMS

Lat-1 K2. (105) (sallust) Wars and Victors? SCARLET

F C D R J R B B Q C O Q C N T Z U N B R,
U R P R M Q C Z R H R M M Q C R G R O N D R M R.
N D U N K R M R U Q N S N O, R P N Z C N H D Z S F
B N U R M R, G R K F D N, U Q C S N U P F M R O
S R B N D P. * O Z B B Q O P [cum, bdghj=JGHIE]

Nor-1. K2 Cosmology. (*qwx, verden) NIL VIRONUS

I K P N H E R A M C K D A O A G P K M K N N K M K
M E K O K M Z L A G G K Q P H E V K M M K G K O K
G P D A O V F I I K G H K R F D O I F V F G N C F
J P K R K M I K G N F E K G G K N C K P F D Y K M
P K A G N P K A G.

REFERENCES / RESOURCES

[ACA] ACA and You, "Handbook For Members of the American Cryptogram Association," ACA publications, 1995.

[ACA1] Anonymous, "The ACA and You - Handbook For Secure Communications", American Cryptogram Association, 1994.

[AFM] AFM - 100-80, Traffic Analysis, Department of the Air Force, 1946.

[ALAN] Turing, Alan, "The Enigma", by A. Hodges. Simon and Shuster, 1983.

[ALBA] Alberti, "Treatise De Cifris," Meister Papstlichen, Princton University Press, Princeton, N.J., 1963.

[ALKA] al-Kadi, Ibrahim A., Origins of Cryptology: The Arab Contributions, Cryptologia, Vol XVI, No. 2, April 1992, pp 97-127.

[ANDR] Andrew, Christopher, 'Secret Service', Heinemann, London 1985.

[ANNA] Anonymous., "The History of the International Code.", Proceedings of the United States Naval Institute, 1934.

[AS] Anonymous, Enigma and Other Machines, Air Scientific Institute Report, 1976.

[AUG1] D. A. August, "Cryptography and Exploitation of Chinese Manual Cryptosystems - Part I:The Encoding Problem", Cryptologia, Vol XIII, No. 4, October 1989.

[AUG2] D. A. August, "Cryptography and Exploitation of Chinese Manual Cryptosystems - Part II:The Encrypting Problem", Cryptologia, Vol XIV, No. 1, August 1990.

[BADE] Badeau, J. S. et. al., The Genius of Arab Civilization: Source of Renaissance. Second Edition. Cambridge: MIT Press. 1983.

[BARB] Barber, F. J. W., "Archaeological Decipherment: A Handbook," Princeton University Press, 1974.

[B201] Barker, Wayne G., "Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Course #201, Aegean Park Press, Laguna Hills, CA. 1982.

[BALL] Ball, W. W. R., Mathematical Recreations and Essays, London, 1928.

[BAR1] Barker, Wayne G., "Course No 201, Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Aegean Park Press, Laguna Hills, CA. 1975.

[BAR2] Barker, W., ed., History of Codes and Ciphers in the U.S. During the Period between World Wars, Part II, 1930 - 1939., Aegean Park Press, 1990.

[BAR3] Barker, Wayne G., "Cryptanalysis of the Hagelin Cryptograph, Aegean Park Press, 1977.

[BARK] Barker, Wayne G., "Cryptanalysis of The Simple Substitution Cipher with Word Divisions," Aegean Park Press, Laguna Hills, CA. 1973.

[BARR] Barron, John, "'KGB: The Secret Work Of Soviet Agents," Bantom Books, New York, 1981.

[BAUD] Baudouin, Captain Roger, "Elements de Cryptographie," Paris, 1939.

[BEES] Beesley, P., "Very Special Intelligence", Doubleday, New York, 1977.

[BLK] Blackstock, Paul W. and Frank L Schaf, Jr., "Intelligence, Espionage, Counterespionage and Covert Operations," Gale Research Co., Detroit, MI., 1978.

[BLOC] Bloch, Gilbert and Ralph Erskine, "Exploit the Double Encipherment Flaw in Enigma", Cryptologia, vol 10, #3, July 1986, p134 ff. (29)

[BLUE] Bearden, Bill, "The Bluejacket's Manual, 20th ed., Annapolis: U.S. Naval Institute, 1978.

[BODY] Brown, Anthony - Cave, "Bodyguard of Lies", Harper and Row, New York, 1975.

[BOLI] Bolinger, D. and Sears, D., "Aspects of Language," 3rd ed., Harcourt Brace Jovanovich,Inc., New York, 1981.

[BOSW] Bosworth, Bruce, "Codes, Ciphers and Computers: An Introduction to Information Security," Hayden Books, Rochelle Park, NJ, 1990.

[BP82] Beker, H., and Piper, F., " Cipher Systems, The Protection of Communications", John Wiley and Sons, NY, 1982.

[BRAS] Brasspounder, "Language Data - German," MA89, The Cryptogram, American Cryptogram Association, 1989.

[BRIT] Anonymous, "British Army Manual of Cryptography", HMF, 1914.

[BRYA] Bryan, William G., "Practical Cryptanalysis - Periodic Ciphers -Miscellaneous", Vol 5, American Cryptogram Association, 1967.

[BURL] Burling, R., "Man's Many Voices: Language in Its Cultural Context," Holt, Rinehart & Winston, New York, 1970.

[CAND] Candela, Rosario, "Isomorphism and its Application in Cryptanalytics, Cardanus Press, NYC 1946.

[CAR1] Carlisle, Sheila. Pattern Words: Three to Eight Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1986.

[CAR2] Carlisle, Sheila. Pattern Words: Nine Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1986.

[CASE] Casey, William, 'The Secret War Against Hitler', Simon & Schuster, London 1989.

[CAVE] Cave Brown, Anthony, 'Bodyguard of Lies', Harper & Row, New York 1975.

[CCF] Foster, C. C., "Cryptanalysis for Microcomputers", Hayden Books, Rochelle Park, NJ, 1990.

[CHOI] Interview with Grand Master Sin Il Choi.,9th DAN, June 25, 1995.

[CHOM] Chomsky, Norm, "Syntactic Structures," The Hague:Mouton, 1957.

[CHUN] Chungkuo Ti-erh Lishih Tangankuan, ed "K'ang-Jih chengmien chanch'ang," Chiangsu Kuchi Ch'upansheh, 1987., pp993-1026.

[CI] FM 34-60, Counterintelligence, Department of the Army, February 1990.

[COUR] Courville, Joseph B., "Manual For Cryptanalysis Of The Columnar Double Transposition Cipher, by Courville Assoc., South Gate, CA, 1986.

[CLAR] Clark, Ronald W., 'The Man who broke Purple', Weidenfeld and Nicolson, London 1977.

[COLF] Collins Gem Dictionary, "French," Collins Clear Type Press, 1979.

[COLG] Collins Gem Dictionary, "German," Collins Clear Type Press, 1984.

[COLI] Collins Gem Dictionary, "Italian," Collins Clear Type Press, 1954.

[COLL] Collins Gem Dictionary, "Latin," Collins Clear Type Press, 1980.

[COLP] Collins Gem Dictionary, "Portuguese," Collins Clear Type Press, 1981.

[COLR] Collins Gem Dictionary, "Russian," Collins Clear Type Press, 1958.

[COLS] Collins Gem Dictionary, "Spanish," Collins Clear Type Press, 1980.

[COVT] Anonymous, "Covert Intelligence Techniques Of the Soviet Union, Aegean Park Press, Laguna Hills, Ca. 1980.

[CULL] Cullen, Charles G., "Matrices and Linear Transformations," 2nd Ed., Dover Advanced Mathematics Books, NY, 1972.

[DAGA] D'agapeyeff, Alexander, "Codes and Ciphers," Oxford University Press, London, 1974.

[DAN] Daniel, Robert E., "Elementary Cryptanalysis: Cryptography For Fun," Cryptiquotes, Seattle, WA., 1979.

[DAVI] Da Vinci, "Solving Russian Cryptograms", The Cryptogram, September-October, Vol XLII, No 5. 1976.

[DEAC] Deacon, R., "The Chinese Secret Service," Taplinger, New York, 1974.

[DEAU] Bacon, Sir Francis, "De Augmentis Scientiarum," tr. by Gilbert Watts, (1640) or tr. by Ellis, Spedding, and Heath (1857,1870).

[DEVO] Devours, Cipher A. and Louis Kruh, Machine Cryptography and Modern Cryptanalysis, Artech, New York, 1985.

[DOW] Dow, Don. L., "Crypto-Mania, Version 3.0", Box 1111, Nashua, NH. 03061-1111, (603) 880-6472, Cost $15 for registered version and available as shareware under CRYPTM.zip on CIS or zipnet.

[EIIC] Ei'ichi Hirose, ",Finland ni okeru tsushin joho," in Showa gunji hiwa: Dodai kurabu koenshu, Vol 1, Dodai kurabu koenshu henshu iinkai, ed., (Toyko: Dodai keizai konwakai, 1987), pp 59-60.

[ELCY] Gaines, Helen Fouche, Cryptanalysis, Dover, New York, 1956.

[ENIG] Tyner, Clarence E. Jr., and Randall K. Nichols, "ENIGMA95 - A Simulation of Enhanced Enigma Cipher Machine on A Standard Personal Computer," for publication, November, 1995.

[EPST] Epstein, Sam and Beryl, "The First Book of Codes and Ciphers," Ambassador Books, Toronto, Canada, 1956.

[EYRA] Eyraud, Charles, "Precis de Cryptographie Moderne'" Paris, 1953.

[FL] Anonymous, The Friedman Legacy: A Tribute to William and Elizabeth Friedman, National Security Agency, Central Security Service, Center for Cryptological History,1995.

[FREB] Friedman, William F., "Cryptology," The Encyclopedia Britannica, all editions since 1929. A classic article by the greatest cryptanalyst.

[FR1] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part I - Volume 1, Aegean Park Press, Laguna Hills, CA, 1985.

[FR2] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part I - Volume 2, Aegean Park Press, Laguna Hills, CA, 1985.

[FR3] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part III, Aegean Park Press, Laguna Hills, CA, 1995.

[FR4] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part IV, Aegean Park Press, Laguna Hills, CA, 1995.

[FR5] Friedman, William F. Military Cryptanalysis - Part I, Aegean Park Press, Laguna Hills, CA, 1980.

[FR6] Friedman, William F. Military Cryptanalysis - Part II, Aegean Park Press, Laguna Hills, CA, 1980.

[FRE] Friedman, William F. , "Elements of Cryptanalysis," Aegean Park Press, Laguna Hills, CA, 1976.

[FREA] Friedman, William F. , "Advanced Military Cryptography," Aegean Park Press, Laguna Hills, CA, 1976.

[FRAA] Friedman, William F. , "American Army Field Codes in The American Expeditionary Forces During the First World War, USA 1939.

[FRAB] Friedman, W. F., Field Codes used by the German Army During World War. 1919.

[FR22] Friedman, William F., The Index of Coincidence and Its Applications In Cryptography, Publication 22, The Riverbank Publications, Aegean Park Press, Laguna Hills, CA, 1979.

[FROM] Fromkin, V and Rodman, R., "Introduction to Language," 4th ed.,Holt Reinhart & Winston, New York, 1988.

[FRS] Friedman, William F. and Elizabeth S., "The Shakespearean Ciphers Examined," Cambridge University Press, London, 1957.

[FUMI] Fumio Nakamura, Rikugun ni okeru COMINT no hoga to hatten," The Journal of National Defense, 16-1 (June 1988) pp85 - 87.

[GARL] Garlinski, Jozef, 'The Swiss Corridor', Dent, London 1981.

[GAR1] Garlinski, Jozef, 'Hitler's Last Weapons', Methuen, London 1978.

[GERM] "German Dictionary," Hippocrene Books, Inc., New York, 1983.

[GIVI] Givierge, General Marcel, " Course In Cryptography," Aegean Park Press, Laguna Hills, CA, 1978. Also, M. Givierge, "Cours de Cryptographie," Berger-Levrault, Paris, 1925.

[GRA1] Grandpre: "Grandpre, A. de--Cryptologist. Part 1 'Cryptographie Pratique - The Origin of the Grandpre', ISHCABIBEL, The Cryptogram, SO60, American Cryptogram Association, 1960.

[GRA2] Grandpre: "Grandpre Ciphers", ROGUE, The Cryptogram, SO63, American Cryptogram Association, 1963.

[GRA3] Grandpre: "Grandpre", Novice Notes, LEDGE, The Cryptogram, MJ75, American Cryptogram Association,1975

[GODD] Goddard, Eldridge and Thelma, "Cryptodyct," Marion, Iowa, 1976

[GORD] Gordon, Cyrus H., " Forgotten Scripts: Their Ongoing Discovery and Decipherment," Basic Books, New York, 1982.

[HA] Hahn, Karl, " Frequency of Letters", English Letter Usage Statistics using as a sample, "A Tale of Two Cities" by Charles Dickens, Usenet SCI.Crypt, 4 Aug 1994.

[HAWA] Hitchcock, H. R., "Hawaiian," Charles E. Tuttle, Co., Toyko, 1968.

[HEMP] Hempfner, Philip and Tania, "Pattern Word List For Divided and Undivided Cryptograms," unpublished manuscript, 1984.

[HIDE] Hideo Kubota, " Zai-shi dai-go kokugun tokushu joho senshi." unpublished manuscript, NIDS.

[HILL] Hill, Lester, S., "Cryptography in an Algebraic Alphabet", The American Mathematical Monthly, June-July 1929.

[HINS] Hinsley, F. H., "History of British Intelligence in the Second World War", Cambridge University Press, Cambridge, 1979-1988.

[HIN2] Hinsley, F. H. and Alan Strip in "Codebreakers -Story of Bletchley Park", Oxford University Press, 1994.

[HISA] Hisashi Takahashi, "Military Friction, Diplomatic Suasion in China, 1937 - 1938," The Journal of International Studies, Sophia Univ, Vol 19, July, 1987.

[HIS1] Barker, Wayne G., "History of Codes and Ciphers in the U.S. Prior to World War I," Aegean Park Press, Laguna Hills, CA, 1978.

[HITT] Hitt, Parker, Col. " Manual for the Solution of Military Ciphers," Aegean Park Press, Laguna Hills, CA, 1976.

[HOFF] Hoffman, Lance J., editor, "Building In Big Brother: The Cryptographic Policy Debate," Springer-Verlag, N.Y.C., 1995. (A useful and well balanced book of cryptographic resource materials.)

[HOM1] Homophonic: A Multiple Substitution Number Cipher", S-TUCK, The Cryptogram, DJ45, American Cryptogram Association, 1945.

[HOM2] Homophonic: Bilinear Substitution Cipher, Straddling," ISHCABIBEL, The Cryptogram, AS48, American Cryptogram Association, 1948.

[HOM3] Homophonic: Computer Column:"Homophonic Solving," PHOENIX, The Cryptogram, MA84, American Cryptogram Association, 1984.

[HOM4] Homophonic: Hocheck Cipher,", SI SI, The Cryptogram, JA90, American Cryptogram Association, 1990.

[HOM5] Homophonic: "Homophonic Checkerboard," GEMINATOR, The Cryptogram, MA90, American Cryptogram Association, 1990.

[HOM6] Homophonic: "Homophonic Number Cipher," (Novice Notes) LEDGE, The Cryptogram, SO71, American Cryptogram Association, 1971.

[HUNG] Rip Van Winkel, "Hungarian," The Cryptogram, March -April, American Cryptogram Association, 1956.

[IBM1] IBM Research Reports, Vol 7., No 4, IBM Research, Yorktown Heights, N.Y., 1971.

[INDE] PHOENIX, Index to the Cryptogram: 1932-1993, ACA, 1994.

[JAPA] Martin, S.E., "Basic Japanese Coversation Dictionary," Charles E. Tuttle Co., Toyko, 1981.

[JOHN] Johnson, Brian, 'The Secret War', Arrow Books, London 1979.

[KADI] al-Kadi, Ibrahim A., Cryptography and Data Security: Cryptographic Properties of Arabic, Proceedings of the Third Saudi Engineering Conference. Riyadh, Saudi Arabia: Nov 24-27, Vol 2:910-921., 1991.

[KAHN] Kahn, David, "The Codebreakers", Macmillian Publishing Co. , 1967.

[KAH1] Kahn, David, "Kahn On Codes - Secrets of the New Cryptology," MacMillan Co., New York, 1983.

[KAH2] Kahn, David, "An Enigma Chronology", Cryptologia Vol XVII,Number 3, July 1993.

[KAH3] Kahn, David, "Seizing The Enigma", Houghton Mifflin, New York, 1991.

[KOBL] Koblitz, Neal, " A Course in Number Theory and Cryptography, 2nd Ed, Springer-Verlag, New York, 1994.

[KONH] Konheim, Alan G., "Cryptography -A Primer" , John Wiley, 1981, pp 212 ff.

[KOTT] Kottack, Phillip Conrad, "Anthropology: The Exploration Of Human Diversity," 6th ed., Mcgraw-Hill, Inc., New York, N.Y. 1994.

[KOZA] Kozaczuk, Dr. Wladyslaw, "Enigma: How the German Machine Cipher was Broken and How it Was Read by the Allies in WWI", University Pub, 1984.

[KULL] Kullback, Solomon, Statistical Methods in Cryptanalysis, Aegean Park Press, Laguna Hills, Ca. 1976

[LAFF] Laffin, John, "Codes and Ciphers: Secret Writing Through The Ages," Abelard-Schuman, London, 1973.

[LAKE] Lakoff, R., "Language and the Womans Place," Harper & Row, New York, 1975.

[LANG] Langie, Andre, "Cryptography," translated from French by J.C.H. Macbeth, Constable and Co., London, 1922.

[LATI] BRASSPOUNDER, "Latin Language Data, "The Cryptogram," July-August 1993.

[LAUE] Lauer, Rudolph F., "Computer Simulation of Classical Substitution Cryptographic Systems" Aegean Park Press, 1981, p72 ff.

[LEDG] LEDGE, "NOVICE NOTES," American Cryptogram Association, 1994. [One of the best introductory texts on ciphers written by an expert in the field. Not only well written, clear to understand but as authoritative as they come!]

[LEWI] Lewin, Ronald, 'Ultra goes to War', Hutchinson, London 1978.

[LEWY] Lewy, Guenter, "America In Vietnam", Oxford University Press, New York, 1978.

[LEVI] Levine, J., U.S. Cryptographic Patents 1861-1981, Cryptologia, Terre Haute, In 1983.

[LISI] Lisicki, Tadeusz, 'Dzialania Enigmy', Orzet Biaty, London July-August, 1975; 'Enigma i Lacida', Przeglad lacznosci, London 1974- 4; 'Pogromcy Enigmy we Francji', Orzet Biaty, London, Sept. 1975.'

[LYNC] Lynch, Frederick D., "Pattern Word List, Vol 1.," Aegean Park Press, Laguna Hills, CA, 1977.

[LYSI] Lysing, Henry, aka John Leonard Nanovic, "Secret Writing," David Kemp Co., NY 1936.

[MANS] Mansfield, Louis C. S., "The Solution of Codes and Ciphers", Alexander Maclehose & Co., London, 1936.

[MARO] Marotta, Michael, E. "The Code Book - All About Unbreakable Codes and How To Use Them," Loompanics Unlimited, 1979. [This is a terrible book. Badly written, without proper authority, unprofessional, and prejudicial to boot. And, it has one of the better illustrations of the Soviet one-time pad with example, with three errors in cipher text, that I have corrected for the author.]

[MARS] Marshall, Alan, "Intelligence and Espionage in the Reign of Charles II," 1660-1665, Cambridge University, New York, N.Y., 1994.

[MART] Martin, James, "Security, Accuracy and Privacy in Computer Systems," Prentice Hall, Englewood Cliffs, N.J., 1973.

[MAYA] Coe, M. D., "Breaking The Maya Code," Thames and Hudson, New York, 1992.

[MAZU] Mazur, Barry, "Questions On Decidability and Undecidability in Number Theory," Journal of Symbolic Logic, Volume 54, Number 9, June, 1994.

[MEND] Mendelsohn, Capt. C. J., Studies in German Diplomatic Codes Employed During World War, GPO, 1937.

[MILL] Millikin, Donald, " Elementary Cryptography ", NYU Bookstore, NY, 1943.

[MM] Meyer, C. H., and Matyas, S. M., " CRYPTOGRAPHY - A New Dimension in Computer Data Security, " Wiley Interscience, New York, 1982.

[MODE] Modelski, Tadeusz, 'The Polish Contribution to the ultimate Allied Victory in the Second World War', Worthing (Sussex) 1986.

[MRAY] Mrayati, Mohammad, Yahya Meer Alam and Hassan al- Tayyan., Ilm at-Ta'miyah wa Istikhraj al-Mu,amma Ind al-Arab. Vol 1. Damascus: The Arab Academy of Damascus., 1987.

[MYER] Myer, Albert, "Manual of Signals," Washington, D.C., USGPO, 1879.

[NIBL] Niblack, A. P., "Proposed Day, Night and Fog Signals for the Navy with Brief Description of the Ardois Hight System," In Proceedings of the United States Naval Institute, Annapolis: U. S. Naval Institute, 1891.

[NIC1] Nichols, Randall K., "Xeno Data on 10 Different Languages," ACA-L, August 18, 1995.

[NIC2] Nichols, Randall K., "Chinese Cryptography Parts 1-3," ACA-L, August 24, 1995.

[NIC3] Nichols, Randall K., "German Reduction Ciphers Parts 1-4," ACA-L, September 15, 1995.

[NIC4] Nichols, Randall K., "Russian Cryptography Parts 1-3," ACA-L, September 05, 1995.

[NIC5] Nichols, Randall K., "A Tribute to William F. Friedman", NCSA FORUM, August 20, 1995.

[NIC6] Nichols, Randall K., "Wallis and Rossignol," NCSA FORUM, September 25, 1995.

[NIC7] Nichols, Randall K., "Arabic Contributions to Cryptography,", in The Cryptogram, ND95, ACA, 1995.

[NIC8] Nichols, Randall K., "U.S. Coast Guard Shuts Down Morse Code System," The Cryptogram, SO95, ACA publications, 1995.

[NIC9] Nichols, Randall K., "PCP Cipher," NCSA FORUM, March 10, 1995.

[NICX] Nichols, R. K., Keynote Speech to A.C.A. Convention, "Breaking Ciphers in Other Languages.," New Orleans, La., 1993.

[NORM] Norman, Bruce, 'Secret Warfare', David & Charles, Newton Abbot (Devon) 1973.

[NORW] Marm, Ingvald and Sommerfelt, Alf, "Norwegian," Teach Yourself Books, Hodder and Stoughton, London, 1967.

[NSA] NSA's Friedman Legacy - A Tribute to William and Elizabeth Friedman, NSA Center for Cryptological History, 1992, pp 201 ff.

[OP20] "Course in Cryptanalysis," OP-20-G', Navy Department, Office of Chief of Naval Operations, Washington, 1941.

[PIER] Pierce, Clayton C., "Cryptoprivacy", 325 Carol Drive, Ventura, Ca. 93003.

[POPE] Pope, Maurice, "The Story of Decipherment: From Egyptian Hieroglyphic to Linear B., Thames and Hudson Ltd., 1975.

[RAJ1] "Pattern and Non Pattern Words of 2 to 6 Letters," G & C. Merriam Co., Norman, OK. 1977.

[RAJ2] "Pattern and Non Pattern Words of 7 to 8 Letters," G & C. Merriam Co., Norman, OK. 1980.

[RAJ3] "Pattern and Non Pattern Words of 9 to 10 Letters," G & C. Merriam Co., Norman, OK. 1981.

[RAJ4] "Non Pattern Words of 3 to 14 Letters," RAJA Books, Norman, OK. 1982.

[RAJ5] "Pattern and Non Pattern Words of 10 Letters," G & C Merriam Co., Norman, OK. 1982.

[REJE] Rejewski, Marian, "Mathematical Solution of the Enigma Cipher" published in vol 6, #1, Jan 1982 Cryptologia pp 1-37.

[RHEE] Rhee, Man Young, "Cryptography and Secure Communications," McGraw Hill Co, 1994

[ROAC] Roach, T., "Hobbyist's Guide To COMINT Collection and Analysis," 1330 Copper Peak Lane, San Jose, Ca. 95120-4271, 1994.

[ROBO] NYPHO, The Cryptogram, Dec 1940, Feb, 1941.

[ROHE] Jurgen Roher's Comparative Analysis of Allied and Axis Radio-Intelligence in the Battle of the Atlantic, Proceedings of the 13th Military History Symposium, USAF Academy, 1988, pp 77-109.

[ROOM] Hyde, H. Montgomery, "Room 3603, The Story of British Intelligence Center in New York During World War II", New York, Farrar, Straus, 1963.

[ROSE] Budge, E. A. Wallis, "The Rosetta Stone," British Museum Press, London, 1927.

[RUNY] Runyan, T. J. and Jan M. Copes "To Die Gallently", Westview Press 1994, p85-86 ff.

[RYSK] Norbert Ryska and Siegfried Herda, "Kryptographische Verfahren in der Datenverarbeitung," Gesellschaft fur Informatik, Berlin, Springer-Verlag1980.

[SADL] Sadler, A. L., "The Code of the Samurai," Rutland and Tokyo: Charles E. Tuttle Co., 1969.

[SACC] Sacco, Generale Luigi, " Manuale di Crittografia", 3rd ed., Rome, 1947.

[SANB] Sanbohonbu, ed., "Sanbohonbu kotokan shokuinhyo." NIDS Archives.

[SAPR] Sapir, E., "Conceptual Categories in Primitive Language," Science: 74: 578-584., 1931.

[SASS] Sassoons, George, "Radio Hackers Code Book", Duckworth, London, 1986.

[SCHN] Schneier, Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code C," John Wiley and Sons, 1994.

[SCH2] Schneier, Bruce, "Applied Cryptography: Protocols, Algorithms, and Source Code C," 2nd ed., John Wiley and Sons, 1995.

[SCHW] Schwab, Charles, "The Equalizer," Charles Schwab, San Francisco, 1994.

[SHAN] Shannon, C. E., "The Communication Theory of Secrecy Systems," Bell System Technical Journal, Vol 28 (October 1949).

[SHIN] Shinsaku Tamura, "Myohin kosaku," San'ei Shuppansha, Toyko, 1953.

[SIG1] "International Code Of Signals For Visual, Sound, and Radio Communications," Defense Mapping Agency, Hydrographic/Topographic Center, United States Ed.Revised 1981

[SIG2] "International Code Of Signals For Visual, Sound, and Radio Communications," U. S. Naval Oceanographic Office, United States Ed., Pub. 102, 1969.

[SINK] Sinkov, Abraham, "Elementary Cryptanalysis", The Mathematical Association of America, NYU, 1966.

[SISI] Pierce, C.C., "Cryptoprivacy," Author/Publisher, Ventura Ca., 1995. (XOR Logic and SIGTOT teleprinters)

[SMIT] Smith, Laurence D., "Cryptography, the Science of Secret Writing," Dover, NY, 1943.

[SOLZ] Solzhenitsyn, Aleksandr I. , "The Gulag Archipelago I-III, " Harper and Row, New York, N.Y., 1975.

[STEV] Stevenson, William, 'A Man Called INTREPID', Macmillan, London 1976.

[STIN] Stinson, D. R., "Cryptography, Theory and Practice," CRC Press, London, 1995.

[STUR] Sturtevant, E. H. and Bechtel, G., "A Hittite Chrestomathy," Linguistic Society of American and University of Pennsylvania, Philadelphia, 1935.

[SUVO] Suvorov, Viktor "Inside Soviet Military Intelligence," Berkley Press, New York, 1985.

[TERR] Terrett, D., "The Signal Corps: The Emergency (to December 1941); G. R. Thompson, et. al, The Test (December 1941 - July 1943); D. Harris and G. Thompson, The Outcome;(Mid 1943 to 1945), Department of the Army, Office of the Chief of Military History, USGPO, Washington,1956 -1966.

[THEO] Theodore White and Annalee Jacoby, "Thunder Out Of China," William Sloane Assoc., New York, 1946.

[TILD] Glover, D. Beaird, Secret Ciphers of The 1876 Presidential Election, Aegean Park Press, Laguna Hills, Ca. 1991.

[TM32] TM 32-250, Fundamentals of Traffic Analysis (Radio Telegraph) Department of the Army, 1948.

[TRAD] U. S. Army Military History Institute, "Traditions of The Signal Corps., Washington, D.C., USGPO, 1959.

[TRAI] Lange, Andre and Soudart, E. A., "Treatise On Cryptography," Aegean Park Press, Laguna Hills, Ca. 1981.

[TRIB] Anonymous, New York Tribune, Extra No. 44, "The Cipher Dispatches, New York, 1879.

[TRIT] Trithemius:Paul Chacornac, "Grandeur et Adversite de Jean Tritheme ,Paris: Editions Traditionelles, 1963.

[TUCK] Harris, Frances A., "Solving Simple Substitution Ciphers," ACA, 1959.

[TUKK] Tuckerman, B., "A Study of The Vigenere-Vernam Single and Multiple Loop Enciphering Systems," IBM Report RC2879, Thomas J. Watson Research Center, Yorktown Heights, N.Y. 1970.

[TUCM] Tuckerman, B., "A Study of The Vigenere-Vernam Single and Multiple Loop Enciphering Systems," IBM Report RC2879, Thomas J. Watson Research Center, Yorktown Heights, N.Y. 1970.

[VERN] Vernam, A. S., "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," J. of the IEEE, Vol 45, 109-115 (1926).

[VOGE] Vogel, Donald S., "Inside a KGB Cipher," Cryptologia, Vol XIV, Number 1, January 1990.

[WAL1] Wallace, Robert W. Pattern Words: Ten Letters and Eleven Letters in Length, Aegean Park Press, Laguna Hills, CA 92654, 1993.

[WAL2] Wallace, Robert W. Pattern Words: Twelve Letters and Greater in Length, Aegean Park Press, Laguna Hills, CA 92654, 1993.

[WATS] Watson, R. W. Seton-, ed, "The Abbot Trithemius," in Tudor Studies, Longmans and Green, London, 1924.

[WEL] Welsh, Dominic, "Codes and Cryptography," Oxford Science Publications, New York, 1993.

[WELC] Welchman, Gordon, 'The Hut Six Story', McGraw-Hill, New York 1982.

[WHOR] Whorf, B. L., "A Linguistic Consideration of Thinking In Primitive Communities," In Language, Thought, and Reality: Selected Writings of Benjamin Lee Whorf, ed. J. B. Carroll, Cambridge, MA: MIT Press, pp. 65-86., 1956.

[WINK] Winkle, Rip Van, "Hungarian: The Cryptogram,", March - April 1956.

[WINT] Winterbotham, F.W., 'The Ultra Secret', Weidenfeld and Nicolson, London 1974.

[WOLE] Wolfe, Ramond W., "Secret Writing," McGraw Hill Books, NY, 1970.

[WOLF] Wolfe, Jack M., " A First Course in Cryptanalysis," Brooklin College Press, NY, 1943.

[WRIX] Wrixon, Fred B. "Codes, Ciphers and Secret Languages," Crown Publishers, New York, 1990.

[XEN1] PHOENIX, "Xenocrypt Handbook," American Cryptogram Association, 1 Pidgeon Dr., Wilbraham, MA., 01095-2603, for publication March, 1996.

[YARD] Yardley, Herbert, O., "The American Black Chamber," Bobbs-Merrill, NY, 1931.

[YAR1] Yardley, H. O., "The Chinese Black Chamber," Houghton Mifflin, Boston, 1983.

[YOKO] Yukio Yokoyama, "Tokushu joho kaisoka," unpublished handwritten manuscript.

[YOUS] Youshkevitch, A. P., Geschichte der Mathematik im Mittelatter, Liepzig, Germany: Teubner, 1964.

[YUKI] Yukio Nishihara, "Kantogan tai-So Sakusenshi," Vol 17., unpublished manuscript, National Institute for Defense Studies Military Archives, Tokyo.,(hereafter NIDS Archives)

[ZIM] Zim, Herbert S., "Codes and Secret Writing." William Morrow Co., New York, 1948.

[ZEND] Callimahos, L. D., Traffic Analysis and the Zendian Problem, Agean Park Press, 1984. (also available through NSA Center for Cryptologic History)