CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI
December 27, 1995
Revision 0

LECTURE 5
XENOCRYPT MORPHOLOGY

SUMMARY

In Lecture 5, we begin our attack on substitution ciphers created in languages other than English. First, we develop an understanding of cryptography in its role as a cultural universal. Next, we tour the elements of language and the common cryptographic threads that make cryptographic analysis possible. We then look at GERMAN Xenocrypts, applied traffic analysis and the ADFGVX cipher of 1918 WWI vintage.

XENOCRYPTS

Xenocrypts are foreign language substitutions. Solving a Xenocrypt (aka XENO) gives double pleasure; not only do you have the fun of solving, but also the satisfaction of knowing that you are acquiring a bowing acquaintance with other languages.

PHOENIX has compiled and edited a Xenocrypt handbook [XEN1] which brings together material published in The Cryptogram since 1940. The book will be available to the KREWE in 1996. It is an excellent tool. Lectures 5-7 will augment his efforts. Quoted from PHOENIX's Preface in reference [XEN1]:

> " Don't be afraid of Xenocrypts. The languages used should not offer particular difficulties. Comparing an English printers table (ETAINORSH...) with any of these languages will show a lot of resemblance. That's because English contains elements of most of the languages. Spellings and endings will differ, but there often will be solid 'root' that strongly resembles an English word. Most short English words are of Saxon origin, akin to Danish, Swedish, Dutch, and more remotely German. Longer words come to us from Latin or Norman - French in many instances, and all have cognates in common with English, generally differing slightly from the English version, but often not at all, especially in French. "

In New Orleans, I keynoted the 1994 ACA Convention with the possibility that any language could be learned from its cryptographic building blocks. Xenocrypts represent a cultural universal expressed at its common denominator - mathematics. [NICX]

I suggested that languages be taught in schools first via cryptography and then via sound and structure. This is how I taught myself the rudiments of Russian, Japanese and Korean. Cryptography enhanced my passable understanding of French and reasonable efforts with German.

The real enjoyment came when I could understand Goethe in German, and translated parts of Budo Shoshinshu by the 17 Century author Daidoji Yuzan [SADL]. Solving Xeno's can open our eyes to other cultures.

THE STRUCTURE OF LANGUAGE

Linguistic anthropologists have used cryptography to reconstruct ancient languages by comparing contemporary descendants and in so doing make discoveries about history. Others make inferences about universal features of language, linking them to uniformities in the brain. Still others study linguistic differences to discover varied world views and patterns of thought in a multitude of cultures. [KOTT]

The Rossetta Stone found by the Egyptian Dhautpol and the French officer Pierre-Francois Bouchard near the town of Rosetta in the Nile Delta, gave us a look at Syriac, Greek and Egyptian Hieroglyphs all of the same text. The fascinating story of its decipherment is covered in Kahn. [KAHN] Of special interest was the final decipherment of the Egyptian writing containing homophones - different signs standing for the same sound. [ROSE]

Until the late 1950's linguists thought that the study of language should proceed through a sequence of stages of analysis. The first stage was phonology, the study of sounds used in speech. Phones are speech sounds present and significant in each language. They were recorded using the International Phonetic Alphabet, a series of symbols devised to describe dozens of sounds that occur in different languages.

The next stage was morphology, the study of forms in which sound combine, to form morphemes - words and their meaningful constituents. The word cats has two morphemes /cat/ and /s/ indicating the animal and plurality. A lexicon is a dictionary of all morphemes. A morpheme is the smallest meaningful unit of speech. [MAYA] Isolating or analytic languages are those in which words are morphologically unanalyzable, like Chinese or Vietnamese. Agglutinative languages string together successive morphemes. Turkish is a good example of this. Inflection languages change the form of a word to mark all kinds of grammar distinctions, such as tense or gender. Indo-European languages tend to be highly inflectional.

The next step was to study syntax, the arrangement and order of words in phrases and sentences.

PHONEMES and PHONES

No language contains all the sounds in the International Phonetic Alphabet. Nor is the number of phonemes -significant sound contrasts in a given language - infinite. Phonemes lack meaning in themselves but through sound contrasts distinguish meaning. We find them in minimal pairs, words that resemble each in al but one sound. An example is the minimal pair pit/bit. The /p/ and /b/ are phonemes in English. Another example is bit and beat which separates the phonemes /I/ and /i/ in English. [KOTT] Friedman describes a similar phenomena called homologs and uses them to solve a variety of cryptograms. [FR2] A phoneme is the smallest unit of distinctive sound. [MAYA]

Standard (American) English (SE), the region free dialect of TV network newscasters, has about thirty-five phonemes of at least eleven vowels and twenty four consonants. The number of phonemes varies from language to language - from fifteen to sixty, averaging between thirty and forty. The number of phonemes varies between dialects. In American English, vowel phonemes vary noticeably from dialect to dialect. Readers should pronounce the words in Figure 5-1, paying attention to whether they distinguish each of the vowel sounds. We Americans do not generally pronounce them at all. [BOLI]

Figure 5-1

Vowel Phonemes
Standard American English
According to Height of Tongue and Tongue Position
in Front, Center and Back of Mouth

```
                                      Tongue High
          i                u
           I             U
            ea     ua   o
             e         ou                 Mid
              ae       a


                                     Tongue Low


  Tongue           Central           Tongue
   Front                             Back
```

Phonetic symbols are identified by English words that include them; note that most are minimal pairs.

high front (spread)	[i]	as in beat
lower high front (spread)	[I]	as in bit
mid front (spread)	[ea]	as in bait
lower mid front (spread)	[e]	as in bet
low front	[ae]	as in bat
central	[ua]	as in butt
low back	[a]	as in pot
lower mid back (rounded)	[ou]	as in bought
mid back (rounded)	[o]	as in boat
lower high back (rounded)	[U]	as in put
high back (rounded)	[u]	as in boot

Phonetics studies sounds in general, what people actually say in various languages.

Phonemics is concerned with sound contrasts of a particular language. In English /b/ and /v/ are phonemes, occurring in minimal pairs such as bat and vat. In Spanish, the contract between [b] and [v] doesn't distinguish meaning, and are not phonemes. The [b] sound is used in Spanish to pronounce words spelled with either b or v. (Non phonemic phones are enclosed in brackets).

In any language a given phoneme extends over a phonetic range. In English the phoneme /p/ ignores the phonetic contrast between the [pH] in pin and the [p] in spin. How many of you noticed the difference? [pH] is aspirated, so that a puff of air follows the [p]. not true with [p] in spin. To see the difference, light a match and watch the flame as you say the two words. In Chinese the contrast between [p] and [pH] is distinguished only by the contrast between an aspirated and unaspirated [p]. [BOLI]

TRANSFORMATIONAL-GENERATIVE GRAMMAR

Norm Chomsky's influential book Syntactic Structures (1957) advocated a new method of linguistic analysis - Transformational-generative grammar. [CHOM] Chomsky felt that a language is more than the surface phenomena just discussed (sounds, words, word order). He felt that all languages shared a limed set of organizing principles. Chomsky observed that every normal child who grows up in society develops language easily and automatically. This occurs because the brain contains a genetically transmitted blueprint, or basic linguistic plan for building language. Chomsky called this universal grammar. As children learn their native language, they experiment with their blueprint, reject some sections applying to other languages and gradually focus in and accept the principles of their own language. They do this at about the same age. His study also showed that we learn languages at similar rates. There are universal improper generalizations (foot, foots; hit, hitted) which eventually are corrected.

We master a specific grammar as we learn to speak. These rules let us convert what we want to say into what we do say. People who hear us and speak our language understand our meaning. This works at a cryptographic level also. Chomsky distinguishes between competence (what the speaker must and does know about his language in order to speak and understand) and performance (what a speaker actually says in social situations or writes to someone). Competence develops during childhood and becomes an unconscious structure. The linguist or cryptographer must discover the structure by looking at deep structures (the mental level) and the surface structure (actual speech) to find the transformational rules that link them. Figure 5-2. shows the Chomsky Model.

```
                       Figure 5-2
                     Chomsky Model
          For Message From Speaker to Hearer
               or Writer on Both Sides

      ... Sounds (phonological component)...
      .                                    .
      .                                    .
      .                                    .
Surface-structure sentence       Surface-structure sentence
      .                                    .
      .                                    .
Transformational rule            Transformational rule
      .                                    .
      .                                    .
Deep structure sentence          Deep structure sentence
      .                                    .
      .                                    .
      .                                    .
       Thought                          Thought
(meaning, semantic component     (meaning, semantic component
      ^
     SPEAKER                            HEARER
```

The Chomsky model tells us why Xenos are so valuable. The human brain contains a limited set of rules for organizing language. The fact that people can learn foreign languages and that words and ideas can be translated from one language into another supports the Chomsky model that all humans have similar linguistic abilities and thought processes.

THE SAPIR-WHORF HYPOTHESIS

Other linguists take the view that rather than universal structures as clues to relationships between languages, they belief that different languages produce different thinking and writing. Edward Sapir and Benjamin Whorf argue that speakers think about things in particular ways. For example, the third person singular pronouns of English (he, she, him, her, his, hers) distinguish gender, whereas those of the Palaung of Burma do not. [BURL] [SAPR] [WHOR]

Gender exists in English, although a fully developed noun-gender and adjative-agreement system as in French and other Romance Languages (la belle fille, la beau fils), does not. The Sapir-Whorf hypothesis suggests that English speakers pay more attention to differences between males and females than the Palaung but less than the French and Spanish speakers.

English divides time into past, present, and future. Hopi, a language of the Pueblo region of the Native American Southwest does not. Hopi does distinguish between events that exist or have existed and those don't or don't yet, along with imaginary and hypothetical events. Differing perceptions of time and reality cause difference in spoken and written thought.

FOCAL VOCABULARY

A lexicon or vocabulary is a language's dictionary, its set of names for things, events and ideas. APEX DX can probably confirm that Eskimos have several distinct words for snow. In English all forms of snow are the same (unless you are a dope dealer). The Nuer of the Sudan have an elaborate vocabulary to describe cattle. Specialized distinctions between groups is called focal vocabulary. Cattle vocabulary of Texas ranchers is more extensive than New Yorkers; Aspen ski bums differentiate types of snow that are missing from the lexicons of Florida retirees. Ten years ago who would have 'faxed' anything. Simplification of often used words are called monolexemes and compound expressions are simplified such as tropical storm to rain. A television becomes TV, an automobile a car, and a videocassette recorder becomes a VCR.

Semantics refers to a language meaning system. Language, culture and thought are interrelated. There is considerable difference between female and male Americans in regard to color terms. Distinctions implied by such terms as salmon, rust, peach, beige, teal, mauve, cranberry, and dusk orange aren't in the vocabularies of most American men. Ask a fashionable woman and she will know them all. [LAKE]

HISTORICAL LINGUISTICS

Knowledge of linguistic relationships is often valuable to determine the events of the past 5000 years. By studying contemporary daughter languages, past language features can be reconstructed. Daughter languages descend from the same parent language that has been changing for thousands of years. The original language from which they diverge is called a protolanguage. French and Spanish are daughter languages of Latin. Language evolves over time into subgroups (closely related from a taxonomy point of view) but with distinct cultural differences. Figure 5-3. shows the main languages and subgroups of the Indo European language stock.

All these daughter languages have developed out of the protolanguage (Proto-Indo-European) spoken in Northern Europe about 5,000 years ago. Note subgroupings. English, a member of the Germanic branch, is more closely related to German and Dutch than it is to Italic or Romance languages such as French and Spanish. However, English shares many linguistic features with French through borrowing and diffusion. [FROM]

The doctrine of linguistic relativity is central to cryptographic treatment of language ciphers. It states that all known languages and dialects are effective means of communication. [KOTT] Nichols Theorem states that if they are linguistically related, they can be codified, enciphered, deciphered and treated as cryptographic units for analysis and statistical treatment. [NICX]

```
                          Figure 5 -3
             Main Languages of Indo-European Stock
                       INDO-EUROPEAN
                            .
............................................................
  .             .                .                         .
  .             .                .                         .
CELTIC        ITALIC          GERMANIC                     .
  .             .             .      . . . . .             .
  .             .             .              .             .
o Welsh         .             .              .             .
o Irish         .           West            North          .
o Scots Gaelic  .             .               .            .
o Breton        .             .               .            .
                .             .               .            .
             ROMANCE         o Dutch         o Danish      .
                .            o English       o Icelandic   .
              Latin          o Flemish       o Norwegian   .
                .            o Frisian       o Swedish     .
                .            o German                      .
              o Catalan      o Yiddish                     .
              o French                                     .
              o Italian                                    .
              o Portuguese                                 .
              o Provencal                                  .
              o Rumanian                                   .
              o Spanish                                    .
                                                           .
.............................................................
HELLENIC            Albanian   .              .
   .                           .              .
   .                          Armenian        .
Ancient Greek                                 .
   .                                          .
   .                                          .
 Greek                                        .
                                              .
...............................................
.                     .                    .
.                     .                    .
INDO-IRANIAN        BALTIC                SLAVIC
    .                 .                    .
    .                 .                    .
    .                o Latvian            o Bulgarian
    .                o Lithuanian         o Czech
    .                                     o Macedonian
    .                                     o Polish
o Old Persian                             o Russian
o Persian                                 o Serbo-Croatian
o SANSKRIT                                o Slovak
     .                                    o Slovenian
     .                                    o Ukrainian
     .
  o Bengali
  o Hindi
  o Punjabi
  o Urdu
```

DEAD LANGUAGES

Figure 5-3 pertains to live languages. Professor Cyrus H. Gordon in his fascinating book "Forgotten Scripts" shows how cryptography is used to recover ancient writings. He tells the story of the unraveling of each of these ancient languages: Egyptian, Old Persion, Sumer-Akkadian, Hittite, Ugaritic, Eteocretan, Minoan and Eblaite. He specializes in cuniform and hieroglyphic inscriptions and gives us a glimpse into the ancient societies that gave birth to the Western world. [GORD] See also references [BARB], [POPE] and [STUR].

CRYPTOGRAPHIC THREAD

There is a common cryptographic thread for most languages. All known writing systems are partly or wholly phonetic, and express the sounds of a particular language. Writing is speech put in visible form, in such a way that any reader instructed in its conventions can reconstruct the vocal message. Writing as "visible speech" was invented about five thousand years ago by Sumerians and almost simultaneously by ancient Egyptians.

The ancient Mayan knew that it was 12 cycles, 18 katuns, 16 tuns, 0 uinals, and 16 kins since the beginning of the Great Cycle. The day was 12 Cib 14 Uo and was ruled by the seventh Lord of the Night. The moon was nine days old. Precisely 5,101 of our years and 235 days had passed. So said the ancient Mayan scribes. We remember the day as 14 May 1989.

WRITING SYSTEMS

Three kinds of writing systems have been identified: Rebus which is a combination of logograms and phonetic signs; Syllabic such as CV - consonant vowel such as Cherokee or Inuit; and Alphabetic, which is phonemic, the individual consonants and vowels make up the sounds of the language.

Table 5-2 differentiates writing systems by the number of signs used. [MAYA]

TABLE 5-3

Writing System	No. of Signs
Logographic	
Sumerian	600+
Egyptian	2,500
Hittite Hieroglyphic	497
Chinese	5,000+
"Pure" Syllabic	
Persian	40
Linear B	87
Cypriote	56
Cherokee	85
Alphabetic or Consonantal	
English	26
Anglo-Saxon	31
Sanskrit	35
Etruscan	20
Russian	36
Hebrew	22
Arabic	28

Michael D. Coe classifies the entire Proto- Mayan languages. In fourteen daughter divisions of Proto-Mayan, there are thirty one sub languages from Huastec to Tzuthil. Extraordinary story of applied cryptanalysis and applied linguistics. [MAYA]

XENOCRYPTS

I used to think that Xenocrypts - non English cryptograms, were very difficult to solve. The 'aha' light came on several years ago, when I realized that most languages share the common framework of mathematics and statistics. To be able to solve Xenocrypts, it is only necessary to learn the basic (group) mathematical structure of the language, to use a bidirectional translation dictionary and to recognize the underlying cipher construct. [NICX]

Many challenge ciphers start with the problem of recognizing the language and then the distribution of characters within the particular language. The legendary W. F. Friedman once remarked: "treating the frequency distribution as a statistical curve, when such treatment is possible, is one of the most useful and trustworthy methods in cryptography." [FR1], [FRE]

Table 1 gives the frequency distributions of ten of my favorite languages (sans Russian, Chinese and Japanese which require character sets that will not transfer via my e-mail). The frequencies in Table 5-1 have been developed from various sources. Table 5-1 frequencies may differ from other published data, based on text derived solely from literature or military sources, because I have included the practical text from my solved Xeno's over the years. Letters used in cryptograms tend to shift the frequency distribution. Frequencies of letters, and their order, are not fixed quantities in any language. Group frequencies, however, are fairly constant in every language. This is the common thread - the linguistic relativity of all languages. [NICX], [NIC1]

TABLE 5-1
Partial Frequency Distribution For Cracking Xenocrypts

	16	8	7	6	5	4	2	<1		
NORWEGIAN:	E	RNS	T	AI	LDO	GKM	UVFHPA'	JBO' YAECWXZQ		
	10	9	7	6	4	3	<2			
LATIN:	I	E	UTA	SRN	OM	CPL	(bal)			
	18	8	7	6	5	4	3	2	<1	
FRENCH:	E	AN	RSIT	UO	L	D	CMP	VB	F-Y	
	14	13	12	8	6	5	4	3	2	<1
PORTUGUESE:	A	E	O	RS	IN	DMT	UCL	P	QV	(bal)
	18	11	8	7	5	4	3	2	<1	
GERMAN:	E	N	I	RS	ADTU	GHO	LBM	CW	(bal)	
	15	12	8	7	5	4	3	1	<1	
CATALAN:	E	A	S	ILRNT	OC	DU	MP	BVQGF	(bal)	
	16	13	8	6	5	4	3	<2		
HUNGARIAN:	E	A	T	OS	LNZ	KIM	RGU	(bal)		
	13	12	11	9	7	6	5	3	2	<1
ITALIAN:	E	A	I	O	L	NRT	SC	DMO'U	VG	(bal)
	20	10	7	6	5	4	3	2	<1	
DUTCH:	E	N	IAT	O	DL	S	GKH	UVWBJMPZ	(bal)	
	13	9	8	7	5	4	3	1	<1	
SPANISH:	EA	O	S	RNI	DL	CTU	MP	GYB	(bal)	

ENGLISH REVISITED

English has its characteristic frequencies and sequence data (based on 10,000 letters):

```
%        12   10 8   8 7 7 7 6 5   4-3     2      1     < 1
ENGLISH: E / T  A / O N I S R H / LDCU / PFMW / YBGV /  KQXJZ
```

GROUP PERCENTAGES:

A E I O U	38.58%
L N R S T	33.43%
J K Q X Z	1.11%
E T A O N	45.08%
E T A O N I S R H	70.02%

ORDER

Digram Order: TH / HE / AN / IN / ER / RE / ES / ON / EA / TI / AT / ST / EN / ND / OR

Trigram Order: THE / AND / THA / ENT / ION / TIO / FOR / NDE

Reversals: ER RE / ES SE / AN NA /TI IT /ON NO / IN NI

Initials: T A O S H I W C B P F D M R

Finals: E S T D N R O Y

Vowel % 40% (y included)

The ACA Xenocrypt Handbook compiled by PHOENIX, develops similar mathematical data on fifteen languages presented in The Cryptogram on a regular basis. [XEN1]

Review Lecture 2 Kullback's tests and Friedman's I.C. test.

Kullback gives the following tables for Monoalphabetic and Digraphic texts for eight languages:

Note that the English plain text value is slightly less than Friedman's. [KULL] [SINK]

	Monoalphabetic Text	Digraphic Text
English	0.0661N(N-1)	0.0069N(N-1)
French	0.0778N(N-1)	0.0093N(N-1)
German	0.0762N(N-1)	0.0112N(N-1)
Italian	0.0738N(N-1)	0.0081N(N-1)
Japanese	0.0819N(N-1)	0.0116N(N-1)
Portuguese	0.0791N(N-1)	
Russian	0.0529N(N-1)	0.0058N(N-1)
Spanish	0.0775N(N-1)	0.0093N(N-1)

Random Text

Monographic	Digraphic	Trigraphic
.038N(N-1)	.0015N(N-1)	.000057N(N-1)

XENO's - foreign language substitutions, as given in the Xenocrypt Department of The Cryptogram, are usually quotations, or simple normal wording. Thus the Frequency Table of a Xenocrypt will follow closely to the normal Frequency Table of its language. Arranging these two tables in order of frequency, rather than alphabetically, may be used for testing probable equivalents. When words are found, if the meaning is not known, a dictionary helps.

The Contact and Position Tables are used just as in solving English cryptograms.

Lets start off with German Xenocrypts.

GERMAN DATA [Based on 60,046 letters of text in FRE2]

Absolute Frequencies

A	3,601	G	1,921	L	1,988	Q	6	V	523
B	1,023	H	2,477	M	1,360	R	4,339	W	899
C	1,620	I	4,879	N	6,336	S	4,127	X	12
D	3,248	J	192	O	1,635	T	3,447	Y	24
E	10,778	K	747	P	499	U	2,753	Z	654
F	958								======
									60,046

Monographic Kappa Plain, German Language = 0.0787, I.C. = 2.05

Relative Frequencies reduced to 1000 letters

E	180	T	57	G	32	F	16	P	8
N	106	D	54	O	27	W	15	J	3
I	81	U	46	C	27	K	13	Y	-
R	72	H	41	M	23	Z	11	X	-
S	69	L	33	B	17	V	9	Q	-
A	60								=======
									1,000

Groups

Vowels: A, E, I, O, U, Y = 39.4%
High-Frequency Consonants: D, N, R, S, T = 35.8%
Medium-Frequency Consonants: B, C, F, G, H, L, M, W = 20.4%
Low-Frequency Consonants: J, K, P, Q, V, X, Z = 4.4 %

8 most frequent letters (E, N, I, R, S, A, T, and D) = 67.9%
(descending order)

Initials (based on 9,568 letters of text)

D	1,716	U	550	Z	343	K	263	O	135
A	762	W	544	M	339	P	181	T	106
S	698	G	461	N	306	R	167	C	22
E	686	B	460	F	280	L	158	Q	2
I	581	V	408	H	265	J	135		======
									9,568

Digraphs [Based on 60,046 letters reduced to 5,000 digraphs]

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	4	14	10	4	33	7	9	7	1	1	2	33	13
B	6				48		1	1	5			3	
C								130			5		
D	29	2		8	127	1	2	2	60		1	3	2
E	13	22	10	31	13	12	32	24	90	2	6	28	25
F	7	1		3	15	7	2		2			2	1
G	10	1		8	78	1	2	2	8		2	7	1
H	29	1		8	64	1	2	1	14		2	8	3
I	3	1	39	7	91	2	18	7	2		7	12	11
J	4				8								
K	12	1		1	11		1	1	1			5	
L	26	3	1	6	27	1	2		37		3	20	1
M	16	3		4	26	2	22	1	14	1	2	1	11
N	39	12	118	58	9	57	8	35	4	10	6	10	18
O	1	3	5	3	11	3	3	3			1	18	6
P	10				5	4		1	2			1	
Q													
R	34	11	5	35	60	9	12	9	37	2	11	6	8
S	14	6	55	13	46	3	7	3	30	1	5	4	7
T	25	3		17	88	2	4	6	40	1	3	7	3
U	1	2	8	2	37	15	5	1			2	2	11
V	1				19				3				
W	16				24				20	3			
X													
Y													
Z	1			1	8				5			1	

Digraphs [Based on 60,046 letters reduced to 5,000 digraphs]

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	48		2		22	27	23	36	1	1			1
B		3			11	2	1	3		1			1
C													
D	2	4	1		5	6	2	9	2	2			2
E	235	3	6		195	68	28	24	9	15			7
F	1	3			10	2	10	12					
G	3	1			11	8	5	8	2	1			1
H	6	6	1		20	4	23	7	2	3			1
I	84	13	1		7	53	44	1	2	1			1
J									3				
K		9			10	1	5	4					
L	2	4				10	12	6	1				1
M	1	8	5		1	3	3	9	1	1			1
N	18	8	5		4	36	27	20	10	17			14
O	33	1	5		18	12	4	1	1	5			1
P		7	2		7		1	1					
Q								1					
R	12	19	3		6	22	18	26	6	8			5
S	3	16	6		2	40	57	9	5	5		1	5
T	4	4			14	20	7	16	2	10			13
U	76		2		18	28	14	1	1	2			1
V		21											
W		6						6					
X													
Y													
Z		2					4	27		4			

Digraphic Kappa plain = 0.0111, I.C. = 7.50

95 Digraphs comprising 75% of German plain text based on 5,000 digraphs arranged according to relative frequencies.

EN- 235	RE- 60	NA- 39	ED- 31	TA- 25	HR- 20	TU- 16
ER- 195	DI- 60	LI- 37	SI- 30	EM- 25	LL- 20	WA- 16
CH- 130	NE- 58	UE- 37	HA- 29	EH- 24	VE- 19	UF- 15
DE- 127	NG- 57	RI- 37	DA- 29	EU- 24	RO- 19	FE- 15
ND- 118	ST- 57	AU- 36	EL- 28	WE- 24	OR- 18	EW- 14
IE- 91	SC- 55	NS- 36	US- 28	HT- 23	UR- 18	AB- 14
EI- 90	IS- 53	NI- 35	ET- 28	AT- 23	NN- 18	HI- 14
TE- 88	BE- 48	RD- 35	AS- 27	AR- 22	RT- 18	TR- 14
IN- 84	AN- 48	RA- 34	LE- 27	RS- 22	OL- 18	SA- 14
GE- 78	SE- 46	AE- 33	NT- 27	EB- 22	IG- 17	MI- 14
-----	IT- 44	------	ZU- 27	VO- 21	NW- 17	NZ- 14
a) 1,236	SS- 40	2,508 b)	LA- 26	NU- 20	TD- 16	UD- 14
	TI- 40		ME- 26	WI- 20	MA- 16	SD- 13
UN- 76	IC- 39	ON- 33	RU- 26	TS- 20	SO- 16	------
ES- 68		AL- 33				3,750
HE- 64		EG- 32				

a) 10 digraphs before this line represent 25% of German Plain

b) 37 digraphs before this line represent 50% of German Plain

Frequent Digraph Reversals (based on table of 5,000 digraphs)

EN- 235	NE- 58	IE- 91	EI- 90	ES- 68	SE- 46	AN- 48
ER- 195	RE- 60	IN- 84	NI- 35	IS- 53	SI- 30	IT- 44
DE- 127	ED- 31	GE- 78	EG- 32		NA- 39	TI- 40

Rare Digraph Reversals (based on previous 5,000 digraphs)

CH- 130 HC- 0 ND-113 DN- 2 NG- 57 GN-3 SC- 55 CS-0

Doublets (based on previous 5,000 digraphs)

SS- 40	EE- 13	FF- 7	RR- 6	GG- 2	PP- 2	OO - 1
LL- 20	MM- 11	TT- 7	AA- 4	II- 2	HH- 1	UU - 1
NN- 18	DD- 8					

Initial Digraphs (based on 9,568 words)

DE- 805	EI- 300	DA- 244	WE- 192	ER- 153	ZU- 124	ST- 112
DI- 567	GE- 299	VO- 214	VE- 172	HA- 140	MI- 117	IN- 111
UN- 428	BE- 252	SI- 197	WI- 155	AL- 134	SN- 112	SE- 111
AU- 318						

Trigraphs (top 102 based on 60,046 letters of German text)

SCH- 666	ERE- 313	NEN- 198	AUS- 162	IST- 142	HRE- 124
DER- 602	ENS- 270	SSE- 191	TIS- 159	STA- 141	HER- 122
CHE- 599	CHT- 264	REI- 190	BER- 157	DES- 140	ACH- 119
DIE- 564	NGE- 263	TER- 188	ENI- 157	FUE- 139	GES- 118
NDE- 541	NDI- 259	REN- 185	ENG- 155	NTE- 139	ABE- 117
EIN- 519	IND- 254	EIT- 184	ION- 154	UER- 138	ERA- 117
END- 481	ERD- 248	EBE- 178	SEN- 152	ERU- 137	BEN- 116
DEN- 457	INE- 247	ENE- 175	ITI- 151	TUN- 136	MEN- 115
ICH- 453	AND- 246	LIC- 175	AUF- 149	SEI- 133	RIE- 112
TEN- 425	RDE- 239	EGE- 173	IES- 149	ESE- 132	VER- 110
UNG- 377	ENA- 214	DAS- 172	ASS- 148	ERT- 128	LAN- 109
HEN- 332	ERS- 212	ENU- 171	ENW- 148	NDA- 127	ENB- 108
UND- 331	EDE- 209	NUN- 169	ENT- 146	IED- 126	ESS- 108
GEN- 321	STE- 205	NER- 166	ERI- 143	ERN- 125	LLE- 108
ISC- 317	VER- 204	RUN- 163	EST- 142	NAU- 108	TSC- 107
ENN- 106	ERG- 106	RIT- 106	EHR- 105	CHA- 104	VON- 104
SIC- 103	IGE- 102	ITE- 101	ENZ- 100	ERB- 100	EUT- 100

Initial Trigraphs (based on 9,568 word beginnings)

EIN- 242	DAS- 79	SCH- 73	AUF- 64	DEU- 61	UNT- 57
VER- 170	BRI- 79	AUS- 69	NER- 63	GES- 60	GRO- 56
FUE- 89	DIE- 76	SEI- 68	IND- 62	GEG- 59	AUC- 55
SIC- 86	NIC- 73	STA- 65	ALL- 61	UEB- 53	POL- 52
WIR- 51					

Tetragraphs (50 top based on 60,046 letters)

SCHE-398	NUND-106	NICH- 80	ATIO- 65	RSCH- 60	ENZU- 54
ISCH-317	ITIS-104	UNGD- 80	GEND- 65	EDEN- 59	ITEN- 54
CHEN-296	SICH-103	EITE- 79	TEND- 65	ERGE- 59	KRIE- 54
NDER-243	RUNG-101	DEUT- 78	EBER- 67	ESSE- 59	RIEG- 54
EINE-218	ANDE-100	FUER- 78	GEGE- 65	UNTE- 59	SDIE- 54
ENDE-216	UNGE-100	CHTE- 77	POLI- 64	EICH- 58	URCH- 53
NDIE-176	EREI- 94	EGEN- 76	SIND- 64	TLIC- 58	ALLE- 52
LICH-168	TION- 93	NEIN- 76	TUNG- 64	INER- 57	DERS- 52
ICHT-151	SEIN- 92	IESE- 75	ENSI- 64	EBEN- 56	ENWE- 52
TISC-146	IEDE- 91	ERST- 74	FUTS- 64	ENDA- 56	HABE- 52
ERDE-144	LAND- 91	RDIE- 74	LITI- 62	ENST- 56	ONEN- 52
ENDI-141	SSEN- 90	ERDI- 72	UEBE- 62	IGEN- 56	SCHI- 52
NDEN-136	BRIT- 89	STEN- 72	UTSC- 62	ONDE- 56	DEND 51
RDEN-133	DASS- 86	CHER- 71	AUCH- 62	TENS- 56	DISC- 51
ENUN-120	NTER- 86	INDI- 71	DENS- 62	EDIE- 55	ENEN- 51
ICHE-120	EDER- 83	REIN- 71	EIND- 61	ERTE- 55	NACH- 51
INDE-111	EREN- 83	DERE- 70	OLIT- 61	HREN- 55	NDAS- 51
NGEN-110	ENGE- 81	NGDE- 70	SCHA- 61	TDIE- 55	UNGS- 51
ERUN-109	ENAU- 80	ENBE- 68	SCHL- 61	ATEN- 55	ABEN- 50
DIES-108	ENIN- 80	RITI- 66	WERD- 61	DIEB- 54	NBER- 50
TSCH-107					

One-letter words: O (very rare)

Two-letter words: ZU SO ER ES DU DA IN AN IM AM UM WO OB JA

Three-letter words: DER DIE UND IST DAS EIN ICH SIE MAN MIT DEN
DEM VON WAR WAS NUR MIR ALS AUF AUS BEI BIS

Four-letter words: SICH ABER WIRD SIND ODER AUCH NACH NOCH MICH
ALSO DOCH DREI FAST SEHR WELT ZWEI WERT OHNE

Common Pattern words: TUT NUN SEE ALLE EINE NEIN DASS DENN DANN
KANN MUSS WENN WILL SOLL KOMM HERR NEUE GING ALLES IMMER EINES
EINEN LEBEN KEINE JETZT

Common prefixes: BE- GE- AUF- ER- VER- HER- UN- HIN- ZU- VOR-

Common suffixes: -LICH -HEIT -KEIT -ISCH -SCHAFT --EN -ER -IG

Pecularities: C generally followed by H or K; SC invariably by H giving SCH

Common articles:

	masc	fem	neut	plu		masc	fem	neut
the	der	die	das	die	a, one	ein	eine	ein
of the	des	der	des	der	of a	eines	einer	eines
in the	dem	der	dem	den	in a	einem	einer	einen
by the	den	die	das	die	by a	einen	eine	ein

True Diphthongs: AI AU EI EU

Consonant Rules

B. May appear in any position.
C. Combines with other consonants. CH, CK, SCH.
D. Forms gerund ending, -ende, -ende; similar to ing in English. Doubles occasionally.
F. Doubles freely.
G. Occasionally doubles.
H. Does not form SH.
J. Initial letter only. Rare.
K. Doubles with CK if separated by - as in bakken
L. Not followed by CK or TZ.
M, N, P, R, T. Doubles freely.
Q. Same as English.
S. Freely doubled, forms SP ST SK not SC nor SH. SCH acts as a single consonant.
V. Initial.
W. Does not form Wh.
X. Very infrequent. Sound of X is CHS
Y. Not a final.
Z. Never doubles. Follows vowels, changes to TZ. Rare as a final.

SOLUTION OF GERMAN ARISTOCRAT

Ger-1 K1. [BRASSPOUNDER]

```
GD   QSMJ   TE  GSK  EVGHSIEKSDNRGK-OGFJDNRGH  EVEJGFH
HFKOPFKI   KGJL  SV   VSJJGUAGDJUSNRG   DJEEJGK  EV
*Z.  *D.  EUUGK  PFKIGHK  DXHGNRGK MGSOG  GKQUSDNR  FKO
OGFJDNR.
```

A frequency analysis of Ger-1 yields:

```
G   - 20    16.1%           Try G=e.
K   - 13    10.5%           Try K=n.
J   - 10     8.1%           Try J=i.
S   -  9     7.3%
D,E - 9      7.3%
F - 7        5.6%
N,R,H - 6    4.8%
V,O,U - 5    4.0%
I - 3
P,Q,M - 2
X,Z,A,T,L - 1
B,C,W,Y - 0
```

```
1     2     3    4         5                    6
e     i          ein    e i  ni   en  e     e       e
GD   QSMJ   TE  GSK  EVGHSIEKSDNRGK-OGFJDNRGH  EVEJGFH

   7       8     9           10             11
  n   n    ne    i      i  e  e   i  e        en
HFKOPFKI   KGJL  SV   VSJJGUAGDJUSNRG   DJEEJGK  EV

12  13   14      15         16        17       18       19
           en      e n      e  en    gi e   en  i       n
Z.  D.  EUUGK  PFKIGHK   DXHGNRGK   MGSOG   GKQUSDNR   FKO

   20
 e
OGFJDNR.
```

So the first three letters follow the German frequency table. Note we have ein. Word 19 is und? and word 1 might be es. The frequencies match. Try these substitutions.

```
1     2     3    4         5                    6
es    i          ein    e i  nis  en deu s  e       eu
GD   QSMJ   TE  GSK  EVGHSIEKSDNRGK-OGFJDNRGH  EVEJGFH

   7       8     9           10             11
 und  n    ne    i      i  e  es  i  e   s    en
HFKOPFKI   KGJL  SV   VSJJGUAGDJUSNRG   DJEEJGK  EV

12  13   14      15         16        17       18       19
 u   s      en    u e n   s  e  en    eide   en  i s    und
*Z. *D.  EUUGK  PFKIGHK   DXHGNRGK   MGSOG   GKQUSDNR   FKO

   20
deu s
OGFJDNR.
```

A common trigram is sch. Word 20 might be deutsch. Word 1 could be es followed by gibt. Word 17 might be beide.

```
1     2     3    4         5                    6
es   gibt        ein    e i  nischen deutscher     teur
GD   QSMJ   TE  GSK  EVGHSIEKSDNRGK-OGFJDNRGH  EVEJGFH

   7       8     9           10             11
rund  n    net   i      ittel estlic e   st  ten
HFKOPFKI   KGJL  SV   VSJJGUAGDJUSNRG   DJEEJGK  EV

12  13   14      15         16        17       18       19
 u   s      en   un e n   sprechen   beide   englisch   und
*Z. *D.  EUUGK  PFKIGHK   DXHGNRGK   MGSOG   GKQUSDNR   FKO

   20
deutsch
OGFJDNR.
```

Word 18 becomes english and word 16 could be speaks in german = sprechen. (insert above)

I note that I have missed a high frequency letter pair E=a. Inserting brings three additional words.

```
1     2     3    4        5                    6
es   gibt    a  ein  americanischen-deutscher  amateur
GD   QSMJ   TE  GSK  EVGHSIEKSDNRGK-OGFJDNRGH  EVEJGFH

   7       8     9          10            11
rund  n    net   im   mittelwestliche   staaten  am
HFKOPFKI   KGJL  SV   VSJJGUAGDJUSNRG   DJEEJGK  EV

12  13   14      15        16        17       18       19
 u   s   allen   un e n   sprechen   beide   englisch   und
*Z. *D.  EUUGK  PFKIGHK   DXHGNRGK   MGSOG   GKQUSDNR   FKO

   20
deutsch
OGFJDNR.
```

The flow of the german now is clear. A little worterbuch gives us the balance of letter relationships.

```
1     2     3    4        5                    6
es   gibt   ja  ein  americanischen-deutscher  amateur
GD   QSMJ   TE  GSK  EVGHSIEKSDNRGK-OGFJDNRGH  EVEJGFH

   7       8     9          10            11
rundfunk   netz  im   mittelwestliche   staaten  am
HFKOPFKI   KGJL  SV   VSJJGUAGDJUSNRG   DJEEJGK  EV

12  13   14      15        16        17       18       19
 u   s   allen  funkern   sprechen   beide   englisch   und
*Z. *D.  EUUGK  PFKIGHK   DXHGNRGK   MGSOG   GKQUSDNR   FKO

   20
deutsch
OGFJDNR.
```

The keyword = sauerkraut.

Note the simularities to English Aristocrat solving and to English endings and words.   Note the group statistics of the two languages and my comments on common threads. Do you see how this commonality flows from Figure 5-1?

SOLUTION OF GERMAN PATRISTOCRAT

Lets remove the word divisions and try a German Patristocrat.

Ger-2. Traurige Wahrheit. (zwei ewige) Eng K4   GEMINATOR

```
     1       2       3       4       5       6       7
   JGKMH   FDZJM   JZMKJ   IMRKJ   ICGXR   MYJWG   XQXRI

     8       9      10      11      12      13      14
   IMJQJ   RGELP   MELJI   XQQLJ   MFCHJ   WQMFI   JQXRM

    15      16       17     18       19     20      21
   YJWGX   QMGFI   CGRME   LFKCR   DGMEL   JWCPH   JWFJM

    22     23
   RGFJM   R.
```

The hint tells us that the words [zwei ewige] is in the cryptogram plain text. We also know that K4 password scheme has been used. Nichols rule says ignore the descriptive part in the title as a red hering.

Start with the frequency analysis:

```
J - 17  15.3%   K -  5  4.5%   O - 0
M - 15  13.5%   C -  5  4.5%   A - 0
R -  9   8.1%   W -  5  4.5%   B - 0
G -  9   8.1%   E -  4  3.6%   N - 0
I -  7   6.3%   H -  3  2.7%   T - 0
Q -  7   6.3%   Z -  2  1.8%   S - 0
X -  6   5.4%   Y -  2  1.8%   V - 0
F -  6   5.4%   P -  2  1.8%   U - 0
L -  5   4.5%   D -  2  1.8%
```

Let J=e and note the patterns at groups 2 and 3 for the hint zwei ewige. So Z=w, D=z, M=i K=g.

```
     1       2       3       4       5       6       7
   e gi     zwei   ewige    i ge           i e
   JGKMH   FDZJM   JZMKJ   IMRKJ   ICGXR   MYJWG   XQXRI

     8       9      10      11      12      13      14
    ie e           i  e        e   i   e     i     e   i
   IMJQJ   RGELP   MELJI   XQQLJ   MFCHJ   WQMFI   JQXRM

    15      16       17     18       19     20      21
    e       i         i      g     z i     e       e  ei
   YJWGX   QMGFI   CGRME   LFKCR   DGMEL   JWCPH   JWFJM

    22     23
      ei
   RGFJM   R.
```

The G is a high frequency letter and could be S, A, or N. Try 'es gibt' in groups 1 and 2. s works, b works, t might.

```
  1      2      3      4      5      6      7
esgib  tzwei  ewige   i ge    s     i e s
JGKMH  FDZJM  JZMKJ  IMRKJ  ICGXR  MYJWG  XQXRI

  8      9     10     11     12     13     14
 ie e    s    i  e       e  it be    it   e   i
IMJQJ  RGELP  MELJI  XQQLJ  MFCHJ  WQMFI  JQXRM

 15     16     17     18     19     20     21
 e s    i t    s i    tg    z i    e   b  e tei
YJWGX  QMGFI  CGRME  LFKCR  DGMEL  JWCPH  JWFJM

 22     23
 stei
RGFJM  R.
```

Now we must find the n, r and the a.   R might be our n. (see last group). And QQ = mm, A long leap for C=a by frequency only - later to confirm by digrams. A short leap lets us assume W=r.   Placing these guesses in temporarily, we find the following:

```
  1      2      3      4      5      6      7
esgib  tzwei  ewige  dinge  dasun  ivers  umund
JGKMH  FDZJM  JZMKJ  IMRKJ  ICGXR  MYJWG  XQXRI

  8      9     10     11     12     13     14
dieme  nschl  iched  ummhe  itabe  rmitd  emuni
IMJQJ  RGELP  MELJI  XQQLJ  MFCHJ  WQMFI  JQXRM

 15     16     17     18     19     20     21
versu  mistd  asnic  htgan  zsich  eralb  ertei
YJWGX  QMGFI  CGRME  LFKCR  DGMEL  JWCPH  JWFJM

 22     23
nstei  n
RGFJM  R.
```

Our digram table helps us with cipher text L and X. X is a good candidate for u and L = h is a reasonable guess, because EL = ch brings us two words.   Note group 12 now gives us the W=r and I = d!   A little help from the dictionary yields Y=v and P=l.

Putting the word divisions back in we have a quote by Dr. Einstein.

Es gibt zwei ewige dinge das universum und die menschliche dummheit aber mit dem universum ist das nicht ganz sicher. == Albert Einstein.

The kewords are (facts; SAD). The plain text x is over the cipher text S for the initial position of the keying alphabets.

GERMAN REDUCTION CIPHERS - TRAFFIC ANALYSIS

A small sister to cryptanalysis is the applications of traffic analysis. Traffic analysis was the forerunner to differential cryptanalysis and a primary reason for the cracking of the German Codes in WWII. {Unfortunately, the same principles worked on the British and American Codes as well.} The German Army (maybe even the German Soul) was dedicated to unquestioned organization. Paperwork and radio messages must flow to the various military units in a prescribed manner. Traffic Analysis is the branch of signal intelligence analysis which deals with the study of external characteristic of signal communications.

The information is used: 1) to effect interception, 2) to aid cryptanalysis, 3) to rate the level and value of intelligence in the absence of the specific message contents and 4) to improve the security in the communication nets. [AFM]

COMPONENTS

Allowing for differences in language and procedure signs and signals, there are six standard elements for military radio communications systems. These are: 1) call-up, 2) order of traffic, 3) transmission of traffic, 4) receipting for traffic, 5) corrections and services, and 6) signing off. [TM32]

In order to insure proper handling of messages in the field and message center, some information was sent in the clear or using simple coding. This information about routing and accounting was usually in the preamble or message postamble. This included: 1) Serial numbers, message center number, 2) Group Count, 3) File Date and Time [like a PGP signature] 4) Routing System - origin, destination and relay, (distinction is made as to action or FYI locations) 5) Priority (important stuff was originally signal flashed - hence the term FLASH message for urgent message) 6) transmission and delivery procedure, 7) addresses and signatures, 8) special instructions. As a general rule, German high-echelon traffic contained most of these items and German low-echelon traffic cut them to a minimum.

The German penchant for organization could be seen in the way they handled serial numbers. Any radio message flowing from division level to soldier in the field would have a reference serial number attached in clear or matrix cipher, by the writer, the HQ message center, the signal center or code room, the "in desk" , the transmitter, linkage, and/or operator. The routing system usually consisted of a code and syllabary that represented the location or unit. [HIN1]

An example taken from WWII U. S. Army procedure:

```
A45  BR6  B  STX-O-P  P-A45  BR6-T-N-A45  A-79K  011046Z
A-45-W-F2P  SLW  BR6

GR 28

BT TEXT

BT  011046Z  K
```

where:

A45 BR6 - multiple callup; receiving calls

STX-O-P - transmitting call with precedence designation, OP= operational priority

P-A45 - message priority to A45 only; to others routine

BR6-T-N-A45 - BR6 to relay to all except A45

A-79K - originator of message

011046 - Date and Time Zulu used pre and postamble

A-45 - action destination

W-F2P SLW BR6 - Information destinations

GR 28 Group Count.. note how small for such external information envelope

You can see where modern E-Mail and word processing systems have made some of this information easier to handle by the portable desk idea but traffic analysis would still apply.

American "cryptees' were adept in determining the German Order of Battle from their cryptonets (ex. from intercepts re limited distribution from corp to a theater). Traffic analysis not only gave the locations but the communication relationships between units or groups of units in the field. Some German commands were allowed latitude in their compositions of codes and ciphers. This proved to be an exploitable fault in the German security.

ANALYSIS OF ROUTING

American success in reconstructing German communication networks was partly do to the appropriate (and sometimes lucky) analysis of the routing system. The radio station could be tied into the code group. Crib techniques included focusing on the relay point, recognizing a book message crib to several locations, correlating the address and signature cribs, tagging the operational chatter, separating the addresses, using solved messages to give outright routing assignments, syllabary solutions and changes in the system itself.

The textual features of the message gave valuable information. Tabulations of messages, text type, and volumes helped discriminate the practice and dummy traffic. Recognition of the communications net as order of battle often gave away the crypto-entity.

APPLICATIONS TO CRYPTANALYSIS

Traffic analysis yields information via Crib messages, Isologs and Chatter. Crib messages assume a partial knowledge of the underlying plain text through recognition of the external characteristics. Command sitrep reports, up and down German channels, were especially easy for American crypees. The origin, serial number range, the cryptonet id, report type, the file date and time, message length and error messages in the clear, gave a clear picture of the German command process. German order of battle, troop dispositions and movements were deduced by traffic analysis. [TM32]

An Isolog exists when the underlying plain text is encrypted in two different systems. They exist because of relay repetition requirements, book messages to multiple receivers (spamming would have been a definite no-no), or error by the code clerk. American crypees were particularly effective in obtaining intelligence from this method.

Traffic analysis boils down to finding the contact relationships among units, tracking their movements, building up the cryptonet authorities, capitalizing on lack of randomness in their structures, and exploiting book and relay cribs. I submit that American intelligence was quite successful in this endeavor against the Germans in WWII.

ADFGVX

"Weh dem der leugt und Klartext funkt" - Lieutenant Jaeger German 5th Army. ["Woe to him who lies and radios in the clear"]

Jaeger was a German code expert sent to stiffen the German Code discipline in France in 1918. Ironically, the double "e" in Jaeger's name gave US Army traffic analysis experts a fix on code changes in 1918.

ADFGVX, is one of the best known field ciphers in the history of cryptology. Originally a 5 x 5 matrix of just 5 letters, ADFGX, the system was expanded on June 1, 1918 to a 6th letter V. The letters were chosen for their clarity in Morse: A .-, D -.., F ..-., G --., V ...-, and X -..-.

W. F. Friedman describes one of the first traffic analysis charts regarding battle activity from May to August, 1918 at Marne, and Rheims, France. It was based solely on the ebb and flow of traffic in the ADFGVX cipher. This cipher was restricted to German High Command communications between and among the headquarters of divisions and army corps.

The ADFGVX cipher was considered secure because it combined both a good substitution (bipartite fractionation) and an excellent transposition in one system. During the eight month history of this cipher, only 10 keys were recovered by the Allies (in 10 days of heavy traffic) and fifty percent of the messages on these days were read. These intercepts effected the reverse of the German advances (15 divisions) under Ludendorff at Montdidier and Compiegne, about 50 miles North of Paris. Solution by the famed French Captain Georges Painvin was based on just two specialized cases. No general solution for the cipher was found by the Allies. In 1933, William Friedman and the SIS found a general solution. French General Givierge, of the Deuxieme Bureau also published a solution to the general case.

The June 3 message that Painvin cracked which changed the course of WWI:

From German High Command in Remaugies: Munition-ierung beschleunigen Punkt Soweit nicut eingesehen auch bei Tag

"Rush Munitions Stop Even by day if not seen."

CT starts: CHI-126: FGAXA XAXFF FAFFA AVDFA GAXFX FAAAG

This told the Allies where and when the bombardment preceding the next major German push was planned.

ENCIPHERING ADFGVX

26 letters and 10 digits of the ADFGVX were placed into a 6 x 6 Bipartite Square:

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

```
PT:  a  l  l    q  u  i  e  t    o  n     t  h  i  s
CT:  AG AD AD   GF DX FD GX XV   AV XD    XV XF FD XA
PT:  f   r   o   n   t     t   o   d   a   y
CT:  AA  GA  AV  XD  XV    XV  AV  DD  AG  FF
```

The bilateral cipher which results is transposed with a keyed matrix, written in by row and removed by column.

G	E	R	M	A	N
3	2	6	4	1	5
A	G	A	D	A	D
G	F	D	X	F	D
G	X	X	V	A	V
X	D	X	V	X	F
F	D	X	A	A	A
G	A	A	V	X	D
X	V	X	V	A	V
D	D	A	G	F	F

and the final CT is:

AFAXA XAFGF XDDAV DAGGX FGXDD XVVAV VGDDV FADVF ADXXX
AXA

Known decipherment was accomplished with the Key and possession of the original matrix.   Fine and dandy but cryptanalysis in 1918, was another thing.

ADFGVX CRYPTANALYSIS

According to William Friedman, there were only three viable ways to attack this cipher. The first method required 2 or messages with identical plain text beginnings to uncover the transposition. Under the second method, 2 or more messages with plain text endings were required to break the flat distribution shield of the substitution part of the cipher. The German addiction to stereotyped phraseology was so prevalent in all German military communications that in each days traffic, messages with similar endings and beginnings were found (sometimes both). The third method required messages with the exact same number of letters. Painvin used the first two methods when he cracked the 5 letter ADFGX version in April, 1918.   [FRAA], [FRAB]

Lest we underestimate the difficulty of this cipher, I think we might step behind Painvin shoulders as he worked. At 4:30 am on March 21, 6000 guns opened fire on the Allied line at Somme. Five hours later, 62 German Divisions pushed forward on a 40 mile front. Radio traffic increased dramatically, Painvin had just a few intercepts in the ADFGX cipher and the longer ones had been split in three parts to prevent anagraming.

Five letters, therefore, a checkerboard? Simple mono cipher - too flat a distribution.

The German oddity of first parts of messages with identical bits and pieces of text larded in the same order in the cryptograms begin to show. Painvin feels the oddity could most likely have resulted from transposed beginnings according to the same key; the identical tops of the columns of the transposition tableau. Painvin sections the cryptograms by timeframe:

```
chi-110:  (1) ADXDA  (2) XGFXG  (3) DAXXGX  (4) GDADFF
chi-114:  (1) ADXDD  (2) XGFFD  (3) DAXAGD  (4) GDGXD
```

He does this with 20 blocks to reconstruct the transposition key. Using the principle - long columns to the left, he finds segments 3,6,14, 18 to left. Balance clustered to right. Using other messages with common endings (repeated) He segments the columns to the left. Correctly? No. He uses 18 additional intercepts to juxtaposition 60 letters AA's, AD's, etc. Using frequency count, he finds a monoalphabetic substitution. He finds column 5-8 and 8-5 are inverted.

Painvin sets up a skeleton checkerboard - he assumes correctly the order to be side-top:

```
      A   D   F   G   X

   A
   D              e
   F
   G
   X
```

Since the message was 20 letters, the order might be side-top, repeated, meaning side coordinates would fall on 1st, 3rd, 5th.. positions during encipherment, so he separates them by frequency characteristics. In 48 hours of incredible labor, Painvin pairs the correct letters and builds the checkerboard, solving the toughest field cipher the world had yet seen. A cipher that defends itself by fractionation - the breaking up of PT letters equivalents into pieces, with the consequent dissipation of its ordinary characteristics. The transposition further scatters these characteristics in a particularly effective fashion, while dulling the clues that normally help to reconstruct a transposition.

HOMEWORK PROBLEMS

Solve these:

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.

Ger-4. Ungerechtes Schicksal. Eng. K4 GEMINATOR

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-)

Fre-1. French digraphic. Christmas Greeting. MON NOM

DBAAB AADBB BBBAB CABAA BBCDC ACCAA BABAC

AABBD ACBAA AAACA CABAC BCCCB BAAAB IJGFG

GKJGJ FFGJH JGFIK JFGFH GGFKG FGHKG FFGJJ

GGJIK GJFJG JGFJH FGIIG KIKJF.

hints: (noel, plus). Look out for disruption area in cipher square.

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.

[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.

[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.

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

[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.

[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.

[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.

[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.

[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.

[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.

[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.

[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.

[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.

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

[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.

[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

[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.

[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).

[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.

[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.

[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.

[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.

[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.

[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)