CLASSICAL CRYPTOGRAPHY COURSE
BY LANAKI
February 4, 1996
Revision 0

LECTURE 7
XENOCRYPT MORPHOLOGY
Part III

SUMMARY

In Lecture 7, we conclude our review of materials related to ciphers created in languages other than English. Lecture 7 will give practical language data for Xenocrypts commonly published in the Cryptogram - French, Italian, Spanish, Portuguese.

Also, we have time for a short review and more homework problems to solve. Lets start with French.

FRENCH - The language of lovers

FRENCH DATA [Based on 55,758 letters of text in FRE2]

Absolute Frequencies

A	4,480	G	624	L	2,737	Q	616	V	801
B	406	H	276	M	1,617	R	4,117	W	6
C	1,944	I	4,230	N	4,406	S	4,564	X	317
D	2,198	J	184	O	3,255	T	4,057	Y	100
E	9,334	K	25	P	1,689	U	3,054	Z	84
F	646								
									55,758

Monographic Kappa Plain, French Language = 0.0777, I.C.= 2.02

Relative Frequencies, based on 55,758 letters of French plain text referenced in FRE2 reduced to 1000 letters:

E	167	T	73	C	35	G	11	J	3
S	82	O	58	P	30	Q	11	Y	2
A	80	U	55	M	29	B	7	Z	2
N	79	L	49	V	14	X	6	K	1
I	76	D	39	F	12	H	5	W	-
R	74								
									1,000

Groups

Vowels: A, E, I, O, U, Y = 43.8%
High-Frequency Consonants: N, R, S, T = 30.7% ; with L =34.0%
Medium-Frequency Consonants: C, D, L, M, P = 18.3%
Low-Frequency Consonants:B,F,G,H,J,K,Q,V,W,X,Z = 7.2 %

8 most frequent letters (E, S, A, N, I, R, T, and O) = 68.9%
(descending order)

Note that group frequencies between German and French are statistically similar.

Initials (based on 10,748 letters of French plain text, One letter words have been omitted.)

D	1,445	L	784	I	315	U	240	H	67		
P	929	S	664	F	313	O	177	Z	7		
E	894	Q	394	T	305	G	146	K	5		
A	866	R	389	N	278	B	115	W	3		
C	816	M	337	V	263	J	98	Y	3		
									9,853		

Digraphs [Frequency Distribution of Digraphs based on 55,758 letters of French plain text reduced to 5,000 digraphs]

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	2	6	20	12	4	6	11		50	1		36	12
B	4				4				4			12	
C	15		6		47			11	20			5	
D	18			1	109			1	20	1			1
E	30	4	49	48	30	15	14	3	13	5		56	58
F	10		2	1	9	6			8			1	
G	6				16		1		2			3	1
H	6				6				4				
I	9	3	12	10	41	4	4			1		27	8
J	4				6								
K													
L	57		1	5	95	1		1	23			26	
M	22	9	1	1	52				23				13
N	19	1	29	40	54	9	11	1	20	1		3	2
O		5	7	3	1	1	2	1	21	1		10	21
P	30		1	1	13			2	3			11	
Q			1										
R	62	2	10	13	127	2	6		24	1		16	11
S	42	2	16	32	75	5	2	1	36	2		15	8
T	40	1	7	22	78	4	1	2	67	11		12	4
U	12	3	10	5	39	14	3	1	24	3		13	6
V	9				24				16				
W													
X	4		3	3	3			1	1				1
Y	2				2								
Z					3				1				

Digraphs [Frequency Distribution of Digraphs based on 55,758 letters of French plain text reduced to 5,000 digraphs]

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	68	1	21	3	41	17	46	29	13			2	1
B		4			5	2	1	2					
C		48			4	1	8	8					
D		10	1		6	2		26					
E	105	4	38	12	89	154	58	27	17		8		3
F		8	1		10	1		1					
G	7	6			8		4	2					
H		3			1			4					
I	49	51	5	12	27	52	47		9		7		1
J		5							2				
K		1											
L	3	10	1			5	4	12				1	
M		8	9			1		4					
N	10	19	6	4	3	53	99	4	7				1
O	109		7		23	13	8	52	2			2	
P		35	9		34	1	6	4					
Q								54					
R	8	27	5	3	7	14	19	6	7				1
S	6	22	24	11	8	41	33	24	4			1	
T	4	14	11	7	44	23	10	11	2				
U	26	1	8	1	48	26	19	1	8		13		1
V		16			5			2					
W													
X	1		4	1	1	2	3		1				
Y		1				2							
Z		1											

Digraphic Kappa plain, French = 0.0093, I.C. = 6.29

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

ES-	154	RA-	62	AI-	50	SS-	41	EA-	30	UI-	24	OM-	21
RE-	127	a)====		EC-	49	ND-	40	EE-	30	SP-	24	NI-	20
ON-	109	ET-	58	IN-	49	b)====		NC-	29	SU-	24	DI-	20
DE-	109	EM-	58	ED-	48	TA-	40	AU-	29	RI-	24	CI-	20
EN-	105	LA-	57	CO-	48	UE-	39	IR-	27	VE-	24	AC-	20
NT-	99	EL-	56	UR-	48	EP-	38	EU-	27	TS-	23	UT-	19
LE-	95	QU-	54	CE-	47	AL-	36	IL-	27	MI-	23	NO-	19
ER-	89	NE-	54	IT-	47	SI-	36	RO-	27	LI-	23	RT-	19
TE-	78	NS-	53	AT-	46	PO-	35	OR-	27	SO-	22	NA-	19
SE-	75	ME-	52	TR-	44	PR-	34	DU-	26	MA-	22	DA-	18
AN-	68	IS-	52	SA-	42	ST-	33	LL-	26	TD-	22	AS-	17
TI-	67	OU-	52	IE-	41	SD-	32	US-	26	AP-	21	EV-	17
		IO-	51	AR-	41	PA-	30	UN-	26	OI-	21	=====	
												3,751	

a) 13 digraphs (1,237 total count, above this line represent 25% of French plain

b) 39 digraphs (2,515 total count, above this line represent 50% of French plain

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

```
ES-  154   SE- 75  LE- 95  EL- 56  RA- 62  AR- 41  IS- 52
RE-  127   ER- 89  TE- 78  ET- 58  EM- 58  ME- 52  EC- 49
DE-  109   ED- 48  TI- 67  IT- 47  LA- 57  AL- 36  AT- 46
EN-  105   NE- 54  SI- 36  CE- 47  TA- 40
```

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

```
NT-   99   TN-  4  QU- 54  UQ- 1  NS- 57  SN-6  OU- 52 UO-1
```

Doublets (based on previous 5,000 digraphs)

```
SS-  41  LL- 26  NN- 10  PP-  9  CC-  6  AA- 2  GG - 1
EE-  30  MM- 13  TT- 10  RR-  7  FF-  6  DD- 1  UU - 1
```

Initial Digraphs 22 digraphs occurring 100 or more times based on 10,748 French plain text words, according to absolute frequencies:

```
DE-  501  RE- 283  PI- 222  SU- 168  AU- 150  DI- 124  SO- 117
CO-  394  PA- 268  IN- 178  CE- 163  NO- 133  AL- 122  VO- 112
QU-  347  LE- 240  SE- 178  ET- 153  TR- 127  UN- 122  FR- 101
PR-  291
```

Trigraphs (top 97 based on 55,758 letters of French text)

```
ENT- 588  CON- 271  EST- 188  ESS- 151  NSE- 130  EUR- 115
ION- 555  ERE- 267  ERA- 185  AIT- 147  REN- 127  NTA- 115
TIO- 433  ANT- 238  ECO- 184  POU- 146  SQU- 124  SER- 115
ONS- 373  ESE- 230  ESD- 179  TER- 146  AIR- 123  ESO- 112
RES- 367  ELA- 227  OND- 175  COM- 143  EPA- 120  DEC- 110
QUE- 338  LLE- 216  LEM- 175  ESP- 139  QUI- 120  EPR- 110
DES- 313  PAR- 213  NCE- 173  OUS- 139  SET- 120  ALL- 109
EDE- 305  NDE- 211  ELE- 172  AIS- 137  REC- 119  ECE- 109
EME- 288  SDE- 210  ESA- 163  EMA- 137  AND- 118  UNE- 108
ATI- 287  DEL- 209  TDE- 163  IER- 136  ETA- 118  RAI- 106
LES- 284  PRE- 206  ITE- 162  NTS- 135  SEN- 118  RLE- 106
NTE- 282  OUR- 205  SSE- 160  TES- 135  PRO- 117  SSI- 106
TRE- 280  RAN- 196  ONT- 157  EQU- 133  ISE- 116  ENE- 105
MEN- 272  IRE- 191  ANC- 153  IQU- 131  REP- 116  SUR- 105

TRA- 105  TEN- 103  BLE- 101  ETE- 100  TAT- 100
ISS- 104  UEL- 102  QUA- 101  ERE- 100
INT- 103  ANS- 101  CES- 101  OMM- 100
```

Initial Trigraphs (The 20 trigraphs appearing 50 or more times as initials of words in 10,748 French words):

CON- 213	COM- 129	FRA- 93	INT- 75	ETA- 69	SER- 61
POU- 144	PRO- 105	PAR- 87	CEN- 72	DAN- 68	TRA- 57
PRE- 135	ALL- 104	QUA- 80	NOU- 69	RED- 65	RES- 56
VOU- 56	FAI- 50				

Tetragraphs (82 top tetragraphs based on 55,758 letters of French plain text)

TION-431	CONS- 98	LEME-83	ERAL-71	EREN-58	RESS-55
MENT-251	EPAR- 98	QUEL-83	ERES-70	ESSE-58	IERE-53
ATIO-220	RESE- 96	LEMA-80	DANS-67	NOUS-58	IRES-53
IONS-208	ENTE- 95	PORT-80	OUVE-67	TRES-58	TEDE-53
EMEN-200	LLEM- 93	ENTS-78	EMAN-66	ENER-57	EQUE-52
POUR-136	FRAN- 91	EPRE-77	SENT-66	NDES-57	NDEL-52
IQUE-128	PRES- 91	EDES-76	ANDE-63	NSEI-57	ECOM-51
IOND-124	ENTA- 90	ESET-76	PART-62	NTDE-57	GENE-51
DELA-120	RANC- 90	INTE-75	SDES-62	CAIS-56	SEIL-51
AIRE-117	ANCE- 89	ALLE-75	ESEN-61	ESTI-56	ELES-50
ONDE-107	SION- 89	ANTE-75	RAIT-61	ITIO-55	ETAT-50
ECON-102	COMM- 88	MAND-75	ENTD-60	NEMA-55	ILLE-50
ESDE-102	ELLE- 84	CENT-74	SSIO-60	NERA-55	SQUE-50
ONSE-101	NTER- 84	QUES-72	ENCE-59		

Look at the above groups. Realize how many apply to English.
Such words as economy, business, energy, genes, firmament, etc.

Average French Word Length = 5.2 letters

One-letter words: A (86%) Y(6%) O(2%)

Two-letter words: DE LA LE ET UN EN NE AU IL DU JE ON SI SE OU SA MA ME CE VA

Three-letter words: LES QUE DES QUI EST PAS UNE AUX PAR DIT ONT
LUI PEU SON SUR CES CET MOT MON VIE BON CAR ILS PUR AMI VIE

Four-letter words: AVEC AVEZ BIEN CEUS COUP DANS DEUX DOIS DOIT
DONT DOUX FAIT FAUT LEUR LUNE MAIS MOIS NOUS PEUT PLUS POUR
QUEL SAIT SONT TOUS TRES TROP VOUS

Common Pattern Words - Three and Four letters: ETE ICI NON SES
TOT D'UN J'AI L'AI L'ON L'OR L'OS M'EN S'EN S'IL; CECI MEME
SAIS SANS SOUS SUIS TOUT ELLE MERE PERE IDEE C'EST D'UNE N'EST
QU'IL QU 'ON N'ONT

Common Initials with apostrophes: C' D' J' L' N'

Peculiarities: In three letter words, U is proceeded by Q and followed by E or I (QUE, QUI) Four or five vowels may be found in sequence. E seldom touches another vowel. D and M contact E about 75% of the time. Four consonants in a row is the most, we usually find ; where five consonants are found sequentially the last is an S of a plural word.

AMCRAS has rearranged the French Frequency Table to:

18	8	8	7	7	7	7	6	6	5	4	3	3	3	2	1	1	1	1	1--
E	A	N	R	S	I	T	U	O	L	D	C	M	P	V	B	F	G	H	JQZXY

Letters have many of the same characteristics as English, with vowels contacting more freely. When LE LA DE etc precede a word beginning with a vowel, the vowel is dropped; an apostrophe is substituted. (C'est for Ce est). This is a big help in finding vowels.

The apostrophe is not used for possession.

Nouns can be of any gender. Adjectives take the same gender as their noun.

A, as a one-letter word, has two meanings. Not accented, it is a verb, has. Accented (not in ciphers) is the preposition ,to.

Ne, pas. The usual way to express negation, is to put ne before the verb, pas, after it. N'est pas means not.

When the masculine form, le or its plural les, is preceded by a A, (to) or de (from), and is followed by a word beginning with a consonant, a le is contracted to au (au pere, to the father); a les, to aux; de le, to du; de les to des.

Some Short Words:

Y, there	Ces, these	Ceci, this	Ce, cet,cette,this
Au, to the	Est, is	Cela, that	Le,la,les the
De, of, from	Lui,to him	Dans, in	Un,una,a,an,one
En, in, by	Mon,my	Elle,she	Par, through,by
Et, and	Non,no	Fait, does	Aller, go
Il, he it	Oui,yes	Leur, them	Dire, say,tell
Je, I	Peu,few	Mais,but	Donne, give
Me, me	Que, that	Nous,we	Faire,make,do
On, people	Qui, who	Plus,more	Lire, read
Ou, or where	Son, his	Pour, for	Mourir, die
Se, himself	Sur, on	Tout, all	Penser, think
Si, if	Tot, soon	Vous, you	Respondre, answer

from [XEN1]

SOLUTION OF FRENCH ARISTOCRAT

FRE-1 [FIDDLE]

```
      1              2          3          4        5
F'  U O N Y O L   M'  Y M N   Y Z Z I L W Y   X Y   Z U C L Y

6        7            8             9           10
O H   W B I C R   L U C M I H H Y   Y N   G Y N B I X C K O Y

 11       12       13       14       15             16
X Y M   G I N M   F Y M   J F O M   O M C N Y M,    F Y M

  17              18            19  20           21
J F O M   H Y W Y M M U C L Y M   U   F U    W I H P Y L M U -

           22   23  24              25
N C I H    Y N   U   F U    W I L L Y M J I H X U H W Y.
```

Set up the normal and cipher text alphabets as a cross check on each other.

```
18 8  8  7  7  7  7  6  6  5  4  3  3  3  2  1 1 1 1   1--
E  A  N  R  S  I  T  U  O  L  D  C  M  P  V  B F G H JQZXY
                                                    normal

21 16 10 9  8  8  8  7  7  7  6  3  3  3  2  2  1  1  1
Y  M  U  I  H  L  N  C  F  O  W  J  X  Z  B  G  K  P  R
                                                    cipher
```

The letters in the Normal table should be over or close to their cipher equivalents, if the message is reasonably normal wording.

Take the gimmes. The 1 letter word U=a (has,to) and the repeated U F U should be a la (to the), so F=l. Y is the highest frequency and most likely an E. M is most likely an S from position and frequency. So FYM = les (the). XYM, es may be either des or ces with X=d or c. Using the pattern table above, word 2 should be s'est.

Words 3 and 8 give us another vowel because YZZI and IHHY I is a vowel , probably U or O but not I. remember that Y=e and I in word 8 follows an S. (maybe) Word 21 implies an ending of t-o- which could be -tion (a very popular ending according to reference FRE2. So we may have H=n and C=i as well as I=O. Let us look at our guesses in the xenocrypt.

FRE-1 [FIDDLE]

```
      1              2          3          4        5
F'  U O N Y O L  M'  Y M N  Y Z Z I L W Y  X Y  Z U C L Y
l ' a  t e      s ' e s t  e    o    e  d e    a i  e
               himself is              of
6       7          8           9          10
O H  W B I C R  L U C M I H H Y  Y N  G Y N B I X C K O Y
  n      n i      a i s u n n e  e t    e t  o d i    e
         o                      and        u c

 11      12       13       14       15          16
X Y M  G I N M  F Y M  J F O M  O M C N Y M,   F Y M
d e s    u t s  l e s    l  s     s i t e s    l e s
of the          the                          the

  17             18           19  20          21
J F O M  H Y W Y M M U C L Y M  U  F U   W I H P Y L M U -
  l  s   n e   e s s a i   e s  a  l a     o n  e  s a
                              to the     u

          22  23  24             25
N C I H   Y N  U  F U   W I L L Y M J I H X U H W Y.
t i o n   e t  a  l a     o    e s  o n d a n  e
    u     and to the     u         u
```

where:

```
18 8  8  7  7  7  7  6  6  5  4  3  3  3  2  1 1 1 1   1--
E  A  N  R  S  I  T  U  O  L  D  C  M  P  V  B F G H JQZXY
Y  U  H     M  C  N     I  F  X normal

21 16 10 9  8  8  8  7  7  7  6  3  3  3  2  2  1  1  1
Y  M  U  I  H  L  N  C  F  O  W  J  X  Z  B  G  K  P  R
e  s  a  o  n     t  i  l          d
         u                       c              cipher
```

Word 6 demands O to be a vowel; as a e i o are already identified, O=u, for un (a,one). Word 14 and 17 are common in French. It is plus (more). The first word is auteu (author.) So L=r in terms of frequency. Word 8 is raisonne (reasonably, rational). The word necessaires (necessary) also becomes visible. The last word is correspondence (same in English). P=v because we pick up on conversation in Word 21.

Z B G R are not identified. A run down of the remanding letters or use of a dictionary gives us Word 5 as faire, (to make) and Word 3 as efforce (force). Word 12 becomes mots (words) and Word 7 = choix (choice).

The final solution is:
l'auteur s'est efforce de faire un choix raisonne methodique des mots les plus usites, les plus necessaires a la conversation et a la correspondence.

"An author forces himself to make a reasonable and methodical choice of words most used, most necessary to conversation and correspondence.

KERCKHOFF

Kerckhoff (aka Jean-Guillaume-Hubert-Victor-Francois-Alexandre-Auguste Kerckhoffs von Nieuwenhof, Holland) was not French but Flemish. His influence was cryptographically significant for selecting usable field ciphers. Kerckhoff was first to separate the general system from the specific key. He told us about superimposition to solve polyalphabetic systems. He told us about the symmetry of position to glean more plain text from the cipher text. He invented the St-Cyr slide and named it after the French national military academy where he studied. "La Cryptographie militaire" gave the French a commanding lead in cryptography in World War I. He was the impetus for those that followed. [KERC] , [KAHN]

FRENCH INFLUENCES - VALERIO, de VIARIS, DELASTELLE, BAZERIES

Letter Frequencies for French, German, English, Russian, Spanish, and Italian (page 9) given by General Givierge in his Course In Cryptography [GIVI] differ from those presented in [FRE2]. Friedman's work is more authoritative and based on significantly more modern plain text. General Givierge borrowed from Paul Louis Eugene Valerio, a captain of Artillery who wrote in the Journal des Sciences militaires in 1892. Valerio published a book called "De la cryptographie" in 1895. The General also borrowed from de Viaris (aka Marquis Gaetan Henri Leon Viarizio di Lesegno) who is famous for one of the first printing cipher devices, in 1874. The General may have included the work of Felix Marie Delastelle, who wrote Traite Elementaire de Cryptographie in 1902. Delastelle's most famous cipher is the bifid and will be covered at a later lecture. Delastelle expanded Kerkhoff's symmetry of position principles published in "La Cryptographie militarie" in 1883. Lastly, Etienne Bazeries influence the General quite heavily. Bazeries invented cylinder device for polyalphabetic encipherment. de Viaris solved the Bazeries cylinder in 1893. Bazeries was miffed to say the least. His device was accepted for use by the U.S. Army in 1922 as a field cipher device. [USAA], [BOWE], [DELA], [BAZE], [VIAR], [VIA1], [LEAU],[VALE]

The French have brought us some talented Cryptographers. [KAHN] tells us about the famous Rossignol and his English counterpart. Problem FRE-4 is taken from reference [GIVI], General Marcel Givierge classic "Cours De Cryptographie." The reader can find many French cryptogram problems in it.

ROSSIGNOL

Rossignol served with swashbuckling facility in the Court of Louis XIV. His cryptographic successes gave him access to secrets of state and the court. The poet Boisrobert (who originated the idea of 'Academie Francaise') wrote the first poem ever written to a cryptologist entitled "Epistres en Vers." He was the court cryptologist of France in the time when Moliere was her dramatist, Pascal her philosopher, La Fontaine her fabulist and the supreme autocrat of the world her monarch. They were influenced accordingly. [MAVE], [MAGN]

Rossignol's technical improvements to the nomenclator systems of the time were quite important. When Rossignol began his career, nomenclators were one-part, listing both the plain and the code elements in alphabetical order or numerical order if the code was numerical. Plain and code paralleled each other. This arrangement existed since the beginning of the Renaissance. Rossignol destroyed the parallel arrangements and mixed the code elements relative to the plain. Two lists were required, one in which the plain elements were in alphabetical order and the code elements were randomized. The second facilitated decoding in which the code elements were alphabetized and the plain equivalents were disarranged. The two tables were called 'tables a chiffrer' and 'tables a dechiffrer'. The two part codes are similar to a bilingual dictionary. The two part construction spread rapidly to others countries and the nomenclator systems grew in numbers and size.

His son Bonaventure, and his grandson Antoine-Bonadventure both carried on the tradition started by their father. Both were raised from King's counselor to president of the Chamber of Accounts. The Cabinet Noir, founded under Louvois, Frances Minister of War, at the urging of Antoine Rossignol, took extra ordinary precautions (switching systems, introducing 18 new nomenclator series) was the start of Frances ironclad control over the cipher business. It still has a tight access policy today. [PERR], [BROG]

Actually it was a good policy. The Vienna Black Chamber -the Geheime Kabinets - Kanzlei regularly read French ciphers up to the cabinet level. [VAIL], [STIX]

WALLIS

England had its Black Chamber. John Wallis was Rossignol's contemporary. He was first a mathematician, giving us the germ of the binomial theorem, the symbol and concept of infinity, a calculation of pi by interpolation and the beginnings of calculus for Newton to do his thing with. John Wallis' solution of Louis XIV of France letter of 9 June 1693 put in the record books.

Their careers parallel each other. They were almost contemporaries, Rossignol was 16 years older. Both made their start on civil war ciphers in their twenties. Both had a mathematical bent. Both were self-taught. Both lived into their eighties. Both owed their worldly success to cryptanalysis. Both became their countries' Fathers of Cryptology in both the literal and figurative sense. But they were different too. Rossignol worked at court while Wallis worked at Oxford. Rossignol introduced new systems for the French and supervised their use. Wallis apparently prescribed only one English cipher and that was done informally. [SMIH]

It is unlikely that these cryptologic experts ever clashed cryptologically despite the contentious natures of both countries. [WALL] , [NIC6]

ITALIAN - the language like music

ITALIAN DATA [Based on 57,906 letters of text in FRE2]

Absolute Frequencies

A	6,771	G	1,168	L	3,592	Q	227	V	1,024
B	527	H	493	M	1,441	R	4,037	W	13
C	2,367	I	6,568	N	4.094	S	2,967	X	9
D	2,258	J	18	O	5,022	T	4,139	Y	14
E	6,784	K	28	P	1,616	U	1,547	Z	527
F	655								======
									57,906

Monographic Kappa Plain, Italian Language = 0.0745, I.C.= 1.94

Relative Frequencies, based on 57,906 letters of Italian plain text referenced in FRE2 reduced to 1000 letters:

E	117	R	70	P	28	F	11	K	-
A	117	L	62	U	27	B	11	J	-
I	113	S	51	M	25	Z	9	Y	-
O	87	C	41	G	20	H	9	W	-
T	72	D	39	V	18	Q	4	X	-
N	71								=======
									1,000

Groups

Vowels: A, E, I, O, U, Y = 46.1%
High-Frequency Consonants: L, N, R, T = 27.4%
Medium-Frequency Consonants: C, D, G, M, P, S = 22.2%
Low-Frequency Consonants:B,F,H,J,K,Q,W,X,Z = 4.3 %

8 most frequent letters (E, A, I, O, T, N, R and L) = 70.8%
(descending order)
Note again that similarities of group frequencies for German, French, English and Italian are statistically significant.

Initials (based on 10,481 letters of Italian plain text, One letter words have been omitted.)

D	1,381	L	500	T	337	U	217	J	13
C	1,041	R	403	G	333	Q	172	W	9
S	885	N	396	F	298	B	153	K	6
P	830	E	374	V	263	H	69	Y	3
A	822	M	371	O	235	Z	29	X	2
I	685								======
									10,481

Digraphs [Frequency Distribution of Digraphs based on 57,847 letters of Italian plain text reduced to 5,000 digraphs]

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	18	9	39	41	14	12	22	1	19			76	24
B	10	7			7				10			1	
C	32		10		20			33	33			2	
D	31			1	65				64				
E	23	7	31	53	15	8	22	2	25			66	18
F	9				11	7			11			1	
G	9				11		8	2	20			17	
H	6				27				9				
I	66	8	52	30	31	11	11	2	11			35	31
J													
K													
L	62	3	8	6	49	2	7		56			52	4
M	31	5			35				17				4
N	32	1	15	26	51	6	11	1	37			3	1
O	17	4	22	27	10	5	10	1	20			45	24
P	23				30				14			2	
Q													
R	64	1	8	8	71	1	7		63			4	13
S	20		15	1	32	2			45			2	3
T	83		1		65	1			59			1	
U	12	2	4	3	15	1	3		10			6	3
V	26				23				23				
W													
X													
Y													
Z	13				4				20				

Digraphs [Frequency Distribution of Digraphs based on 57,847 letters of Italian plain text reduced to 5,000 digraphs]

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	78	5	24	4	57	36	63	6	24				12
B		4			4			2					
C		64		1	5			6					
D		23			2			9					
E	73	6	22	4	96	62	27	6	17				4
F		10			6			3					
G	8	9			11			6					
H													
I	62	44	20	3	20	48	45	15	16				7
J								1					
K													
L	2	21	5	1	3	6	15	7	3				
M		18	13					2					
N	10	50	4	5	2	11	66	8	4				11
O	86	4	25	2	55	40	14	3	18				2
P		28	11		23			7					
Q								20					
R	9	45	2		12	9	16	10	3				3
S		25	9			31	58	12	1				
T	1	56			43	1	37	10					
U	24	8	6		9	11	150						1
V		10			2			2	2				
W													
X													
Y													
Z		3											5

Digraphic Kappa plain, Italian = 0.0081, I.C. = 5.48

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

ER-	96	RI-	63	LL-	52	AC-	38	MA-	31	HE-	25	VE- 23
ON-	86	IA-	63	IC-	51	TT-	37	SS-	31	OP-	25	OC- 22
TA-	78	LA-	62	NE-	50	b)====		DA-	31	AM-	24	AG- 22
AN-	78	IN-	62	NO-	50	NI-	37	EC-	30	UN-	24	EG- 22
AL-	76	a)====		LE-	49	ME-	35	PE-	30	EI-	24	EP- 22
EN-	73	RA-	62	IS-	48	AS-	35	ID-	30	AV-	24	LO- 21
RE-	71	ES-	61	IT-	45	IL-	35	IE-	30	OM-	24	IP- 20
NT-	66	TI-	59	OL-	45	CH-	33	PO-	28	PA-	23	ZI- 20
DE-	65	ST-	58	RO-	45	CI-	33	OD-	27	DO-	23	SA- 20
TE-	65	AR-	57	SI-	44	RA-	32	ET-	27	VI-	23	CE- 20
EL-	65	TO-	56	IO-	43	SE-	32	VA-	26	AP-	23	QU- 20
DI-	64	LI-	56	TR-	43	CA-	32	ND-	26	PR-	23	GI- 20
CO-	64	OR-	55	OS-	40	IM-	31	SO-	25	EA-	23	=======
AT-	63	ED-	52	AD-	39							3,762

a) 18 digraphs (1,260 total count, above this line represent 25% of Italian plain

b) 43 digraphs (2,495 total count, above this line represent 50% of Italian plain

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

```
ER-   96   RE- 71    EL- 66    LE- 49    LI- 56    IL- 35
ON-   86   NO- 50    DE- 65    ED- 53    OR- 55    RO- 45
TA-   83   AT- 63    RA- 64    AR- 57    IC- 52    CI- 33
AN-   78   NA- 32    IN- 62    NI- 37    IS- 48    SI- 45
AL-   76   LA- 62    ES- 62    SE- 32    AD- 41    DA- 31
EN-   73   NE- 51    TI- 59    IT- 45    AC- 39    CA- 32
```

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

```
NT-   66   TN-  1  ST- 58  TS- 1  CH- 33  HC-0
```

Doublets (based on previous 5,000 digraphs)

```
LL-  52  AA- 18  II- 11  NN- 10  FF-  7  MM- 4  VV - 2
TT-  37  EE- 15  PP- 11  GG-  8  ZZ-  5  OO- 4  DD - 1
SS-  31  RR- 12  CC- 10  BB-  7
```

Initial Digraphs (26 digraphs occurring 100 or more times based on 10,481 Italian plain text words, according to absolute frequencies:)

```
CO- 543   PE- 210  PR- 184  NO- 154  SE- 121  MA- 112  RE- 108
DE- 505   CH- 197  QU- 172  PA- 153  SO- 121  UN- 111  ES- 107
ST- 222   AL- 186  NE- 169  PO- 141  TR- 121  SU- 109  TE- 103
DI- 215   IN- 185  RI- 162  CA- 132  DA- 120
```

Trigraphs (top 90 based on 57,906 letters of Italian text)

```
DEL- 348  STA- 215  ERE- 169  ICA- 145  SSI- 130  ODI- 114
ENT- 348  ALI- 213  ZIO- 166  RAN- 145  NEL- 127  ORI- 114
ELL- 314  EDI- 212  ATO- 165  STR- 145  ACO- 125  RMA- 114
CON- 306  ALL- 201  NTI- 165  ALE- 144  ATI- 125  AME- 113
CHE- 276  ITA- 198  ANT- 163  IDI- 143  IDE- 123  ETT- 113
LLA- 274  ANO- 197  ERA- 163  COM- 139  ADI- 121  ODE- 113
ION- 265  OST- 196  TRA- 160  ECO- 137  AND- 121  PRE- 112
ONE- 247  ERI- 187  ESS- 158  LLE- 137  TEN- 120  NDO- 110
PER- 238  ARE- 186  ATT- 157  ONT- 136  ONO- 119  ONI- 110
EDE- 228  TAL- 184  NTO- 156  TER- 136  ARI- 117  AZI- 109
NTE- 227  LIA- 180  ADE- 155  TAT- 134  NTR- 117  ENE- 109
ICO- 216  IST- 174  EST- 151  TTA- 132  PAR- 116  ELA- 107
MEN- 216  CLI- 171  RES- 146  ATA- 130  TRO- 116  ERO- 107

ESI- 107
COR- 106
IAN- 106
TAN- 105
ATE- 104
NON- 103
VER- 103
ICA- 101
OLA- 101
STI- 101
OCO- 100
RIA- 100
```

Initial Trigraphs (The 19 trigraphs appearing 50 or more times as initials of words in 10,481 Italian words):

```
DEL- 217  STA- 106  QUA-  83  PRE-  62  DAL-  57  PER-  55
CON- 195  ALL- 100  PRO-  75  NEL-  57  ANC-  56  RUS-  55
COM- 137  ITA-  94  QUE-  74

GRA-  53  STO-  51
```

Tetragraphs (57 top tetragraphs based on 57,906 letters of Italian plain text)

```
DELL-209  ALIA- 99  ICON-74   AGLI-66   LIAN-59   OPER-56
MENT-188  CONT- 93  VANO-74   ICHE-66   TORI-59   RUSS-56
IONE-160  ADEL- 92  ECON-73   IDEL-64   ALLE-58   TATO-55
ELLA-150  OSTR- 88  IONI-71   ELLE-63   ANDO-58   TEDE-55
ZION-147  ENTO- 87  STAT-70   NELL-63   DALL-58   OCON-54
TALI-125  AMEN- 83  STRA-70   IMEN-61   NTRO-58   SION-53
AZIO-106  ALLA- 81  GLIA-69   ANTI-60   OCHE-58   TANT-53
EDEL-106  ENZA- 75  ISTA-68   ATTA-60   ANTE-57   STOP-52
ITAL-106  ONTR- 75  ODEL-68   PART-60   EPER-57   NOST-51
ENTE-105  ENTI- 74  ACON-66
```

Average Italian word length = 5.2 letters

One-letter words: E (56%) A (22%) I (14%) O (8%)

Two-letter words: DI LA UN IL SI LE DA MA IN AL VI SE HA NE HO LO AD ED VA IO

Three-letter words: CHE UNA PER CON DEL PIU GLI NEL DEI MIA SIA DUE ERA MIO MAI CHI;

Four-letter words: BUON COME COSA COSI DICE DIRE DOVE ERAN FARE GREAN OGNI PERO QUEL VITA

Common Pattern Words - Three and Four letters: NON ; ALLA ANNI ANO BENE ESSA ESSE MODO POCO SONO UOMO VEDE

Common Initials with apostrophes: D' I' L' S'

Common words with apostrophes: C'E CH' GL' OR' PO' EN' DOV' VID' ALL' TIEN' DOV'E BUON' DELL' NELL'

Peculiarities: Vowels constitute about half of the language letters. Highest contacts are with L N R T. H is preceded by C or G. Q is followed by U and another vowel. See [XENO] for additional rules. [SACC] gives data on consonant sequences.

Consonant doubling is frequent: L T S C R G P N B M Z F V I D

Finals in order: O E A I; Rare R L D N

[SACC] gives us the following common consonant three letter sequences: STR NTR LTR TTR NDR SCR NGL NFL NGR SPL NCH RCH SCH MPR PPR FFR BBL MBR CCH

R S L may be found in any one of these groups, rarely H.

Common prepositions: A CON DA DI IN PER SU

The Italian Frequency Table rearranged:

```
18 12 11 9  7  6  6  6  5  5  3  3  3  3  2  2 1 1 1 1 -
E  A  I  O  L  N  R  T  S  C  D  M  P  U  V  G Z F B H Q
```

SOLUTION OF ITALIAN ARISTOCRAT

```
ITA -1.                MON NOM
1    2          3        4   5    6    7    8         9    10
YT  GNLYJO  *LSISVAS,  KN  JH  TST  JY  MHOLYKEY   IOY  JHSY

11       12    13     14    15       16       17   18    19
GYBYY,  JH  AYTYLOY  OI  HRRYIYLN  VSLS,  ESUN  HTS  KEZYOGS

20     21         22  23     24
EZN   HRRYIYKEN  YV  KHS  QOILSTN.
```

Listing the short words:

YT KN JH-2 JY OI YV TST IOY EZN KHS HTS

Take a frequency count of finals:

Y-7 N-6 S-5 H-2 T-2 O I V -1

Since highest frequency finals are usually vowels, Y N S and H may be vowels and word 6 TST could be NON. If this assumption is correct then word 18 is UNO. Further YT = in and YY =ii in word 11. Word YV = il.

Substituting our guesses:

```
1    2         3       4   5    6    7    8        9    10
YT  GNLYJO  *LSISVAS,  KN  JH  TST  JY  MHOLYKEY   IOY  JHSY
in   eri     ro ol o   se   u  non   i   u ris i     i   uoi

11      12    13     14    15      16      17   18    19
GYBYY,  JH  AYTYLOY  OI  HRRYIYLN  VSLS,  ESUN  HTS  KEZYOGS
 i ii    u   inir i      u  i ire  loro   co e  uno  s hi  o

20     21        22  23     24
EZN   HRRYIYKEN  YV  KHS  QOILSTN.
che   u  i is e  il  suo     rone
```

Word 17 L=r for loro.

The initals are S or P. Word 23 is Suo or or Puo. But word 4 would be Se or Sa but not pe or pa. Try K=s. We should look for CHE (that) and the likely candidate is EZN.

Substituting again in above we have four additional words. OI and IOY suggest ad and dal. By frequency J=t.

The solution reads: In verita Rodolfo, se tu non ti guaristi dai tuoi vizii, tu finirai ad ubbidire loro, come uno schiavo che ubbidisce il suo padrone.

GENERAL LUIGI SACCO

One of Italy's most brilliant cryptographers, his manual gives detailed solutions of various transposition, monoalphabetic and polyalphabetic systems. His appendix details the equations used for such interesting problems as de Viaris polyalphabetic substitution, Kerckhoff's ciphers and the Hill algebraic problem. [SACC] [The reading is difficult and a little disorganized but the digging is rewarding.]

SPANISH - The language of passion. [SPAN]

SPANISH DATA [Based on 60,115 letters of text in [FRE2] and [SPAN]

Absolute Frequencies

A	6,681	G	823	L	2,174	Q	346	V	602
B	799	H	367	M	1,740	R	4,628	W	36
C	3,137	I	4,920	N	4,823	S	4,140	X	127
D	2,687	J	190	O	5,859	T	3,180	Y	413
E	7,801	K	22	P	1,785	U	2,172	Z	182
F	481								
									60,115

Monographic Kappa Plain, Spanish Language = 0.0747, I.C.= 1.94

Relative Frequencies, based on 60,115 letters of Spanish plain text referenced in [FRE2] and [SPAN] reduced to 1000 letters:

E	130	S	69	U	36	V	10	J	3
A	111	T	53	P	30	F	8	Z	3
O	97	C	52	M	29	Y	7	X	2
I	82	D	45	G	14	H	6	W	1
N	80	L	36	B	13	Q	6	K	-
R	77								
									1,000

Groups

Vowels: A, E, I, O, U, Y = 46.3%
High-Frequency Consonants: N, R, S = 22.6%
Medium-Frequency Consonants: C, D, L, M, P, T = 24.5%
Low-Frequency Consonants:B,F,G,H,J,K,Q,V,W,X,Z = 6.6 %

7 most frequent letters (E, A, O, I, N, R, S) = 64.6%
(descending order)
Note that group frequencies between German and Spanish are statistically similar.

Initials (based on 10,129 letters of Spanish plain text, One letter words have been omitted.)

P	1,128	L	435	Q	286	V	183	Y	27
C	1,081	R	425	I	281	F	177	W	19
D	1,012	M	403	H	230	O	169	Z	2
E	989	N	346	U	219	B	124	K	1
S	789	T	298	G	206	J	47	X	
A	761								
									10,129

Digraphs [Frequency Distribution of Digraphs based on 60,115 letters of Spanish plain text reduced to 5,000 digraphs]

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	12	14	54	64	15	5	8	4	10	8		41	30
B	11				5				14	1		12	
C	39		5		17			8	80			3	
D	32		1	2	84			1	30				
E	20	5	47	26	17	8	21	6	9	3		44	26
F	2				9				12			1	
G	12				12				5			1	
H	15				3				5				
I	43	8	42	29	40	5	8			1		14	16
J	4				5								
K					1								
L	44		5	5	35	1	3		28			9	5
M	32	10			42				30				
N	41	2	33	37	41	10	6	2	28	1		5	4
O	19	17	28	26	16	6	5	5	4	1		22	33
P	30		1		16				5			8	
Q													
R	74	1	12	10	94	1	12		45	1	1	6	15
S	32	2	18	15	57	3	2	4	41	1		5	7
T	60		1		67				35				
U	13	6	11	5	52	1	3		9			9	6
V	12			1	15				15				
W	1				1								
X			1		4								
Y	5	1	3	2	5	1	1					1	1
Z	6		1	1									

Digraphs [Frequency Distribution of Digraphs based on 60,115 letters of Spanish plain text reduced to 5,000 digraphs]

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	64	4	24	5	81	62	18	9	9			11	4
B		5			12	2	1	3					
C		69			6		13	18					
D	1	59	2	1	3	1		6				1	
E	126	5	23	4	94	119	17	5	10	1	8	2	3
F		7			4			5					
G	2	15			11		1	11					
H		6						1					
I	50	67	4	1	16	27	24	1	8				5
J		3						3					
K													
L	1	17	5	1	2	4	5	5	3			1	
M		15	10					6					
N	3	43	10	2	4	21	91	12	6			1	1
O	104	4	29	7	58	73	12	3	5		2	9	1
P		31			34	1	3	19					
Q								29					
R	11	43	7	3	10	10	15	9	6			1	1
S	5	22	26	4	6	10	57	23	2			4	
T		56			34			11					
U	34	1	3		9	10	4		1			2	
V		7											
W												1	
X			3				2						
Y	1	5	2	1	1	3	1	1					
Z		3						2					

Digraphic Kappa plain, Spanish = 0.0091, I.C. = 6.15

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

EN- 126	TE- 67	IN- 50	NA- 41	MA- 32	IS- 27	EA- 20
ES- 119	AN- 64	EC- 47	IE- 40	SA- 32	EM- 26	OA- 19
ON- 104	a)====	RI- 45	b)====	PO- 31	SP- 26	PU- 19
ER- 94	AD- 64	EL- 44	CA- 39	MI- 30	ED- 26	SC- 18
RE- 94	AS- 62	LA- 44	ND- 37	PA- 30	OD- 26	AT- 18
NT- 91	TA- 60	RO- 43	TI- 35	AD- 30	AP- 24	CU- 18
DE- 84	DO- 59	NO- 43	LE- 35	DI- 30	IT- 24	EE- 17
AR- 81	OR- 58	IA- 43	TR- 34	ID- 29	EP- 23	OB- 17
CI- 80	SE- 57	IC- 42	UN- 34	QU- 29	SU- 23	CE- 17
RA- 74	ST- 57	ME- 42	PR- 34	OP- 29	SO- 22	ET- 17
OS- 73	TO- 56	AL- 41	OM- 33	LI- 28	OL- 22	LO- 17
CO- 69	AC- 54	SI- 41	NC- 33	NI- 28	NS- 21	
IO- 67	UE- 52	NE- 41	DA- 32	OC- 28	EG- 22	=====
						3,753

a) 15 digraphs (1,287 total count, above this line represent 25% of Spanish plain

b) 40 digraphs (2,513 total count, above this line represent 50% of Spanish plain

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

```
EN-  126   NE- 41  AR- 81  RA- 74  AS- 62  SA- 32  LA- 44
ES-  119   SE- 57  CI- 80  IC- 42  OR- 58  RO- 43  EL- 44
ON-  104   NO- 43  AN- 64  NA- 41  AC- 54  CA- 39  MA- 32
ER-   94   RE- 94  AD- 64  DA- 32  AL- 41  LE- 35  AM- 30
```

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

NT- 91 TN- 0 ST- 57 TS- 0 ND- 37 DN-1 NC- 33 CN-0 IO- 67 OI- 4

Doublets (based on previous 5,000 digraphs)

EE- 17 AA- 12 RR- 10 SS- 10 LL- 9 CC- 5 OO - 4 NN- 3 DD- 2

Initial Digraphs 21 digraphs occurring 100 or more times based on 10,129 Spanish plain text words, according to absolute frequencies:

```
CO-  684  PR- 307  PA- 263  SE- 189  CA- 151  PE- 111  MA- 101
RE-  335  ES- 286  PO- 247  DI- 175  SI- 137  UN- 109  CU- 100
DE-  323  QU- 286  IN- 235  PU- 157  MI- 117  HA- 108  SO- 100
```

Trigraphs (top 105 based on 60,115 letters of Spanish text)

```
ENT- 596  ARA- 229  POR-  176  OSE- 147   ERO- 131   NDE- 121
ION- 564  ONE- 227  TER-  174  ONS- 144   ONT- 131   RAN- 121
CIO- 502  ESE- 202  ODE-  168  REC- 144   ANA- 130   STE- 119
NTE- 429  ADE- 293  ERE-  166  ORE- 143   ARE- 129   REN- 118
CON- 415  PAR- 190  ERA-  165  OCO- 142   UNT- 127   ARI- 117
EST- 355  CIA- 190  TRA-  165  EDE- 141   ANO- 127   TEN- 116
RES- 335  ENC- 188  AME-  165  ICI- 140   TAR- 126   OND- 115
ADO- 307  NCI- 184  ERI-  163  END- 139   ANT- 126   RIA- 115
QUE- 294  PRE- 183  MER-  162  SEN- 139   ESA- 126   ECI- 114
ACI- 277  DEL- 183  ELA-  159  TAD- 138   IER- 125   IST- 113
NTO- 270  NDO- 183  PRO-  158  ECO- 135   ADA- 125   ONA- 113
IEM- 267  NES- 183  ACO-  155  STR- 134   DEN- 124   DAD- 112
COM- 246  DOS- 182  ENE-  153  TOS- 133   AND- 123   INT- 112
ICA- 242  MEN- 181  UES-  151  IDA- 132   DES- 121   NTR- 112
STA- 240  NTA- 176  ESP-  149  SDE- 132   IDO- 121   ESI- 111

PER- 111
ASE- 109
CAN- 109
UNI- 108
OSI- 107
GEN- 105
NCO- 105
RIO- 105
ERN- 104
OMI- 104
SCO- 104
TES- 103
BIE- 101
NTI- 100
TOR- 100
```

Tetragraphs (86 top tetragraphs based on 60,115 letters of Spanish plain text)

```
CION- 444 CONS- 104 ERNO-  79 AMER- 72  FORM- 62  EEST- 55
ACIO- 252 CONT-  99 IERN-  78 IEND- 72  SENT- 62  SCON- 55
ENTE- 233 PUNT-  95 OQUE-  78 IDAD- 71  ICIO- 61  SIDE- 55
ESTA- 174 ANDO-  91 IONA-  77 ENDO- 70  ONTR- 60  CIEN- 54
IONE- 159 TADO-  91 UEST-  77 ERIC- 70  SION- 60  NFOR- 54
MENT- 150 ACON-  90 BIER-  76 NTOS- 70  CCIO- 59  OPOR- 54
ONES- 146 ANTE-  89 ICAN-  76 MIEN- 69  GENT- 58  RESP- 54
IENT- 141 NTER-  85 RESE-  76 IOND- 67  COMA- 57  ARIO- 53
ENTO- 137 INTE-  84 GOBI-  75 MERI- 67  ESDE- 57  ESTR- 53
ENCI- 128 NTES-  82 OBIE-  75 NTRA- 67  ORES- 57  ARGE- 51
PARA- 117 ADOS   81 ECON-  74 DELA- 65  RECI- 57  ECTO- 51
ENTA- 115 AMEN-  81 RGEN-  73 ENTI- 64  AQUE- 56  PART- 51
NCIA- 115 OCON-  81 RICA-  73 NTIN- 64  IONP- 56  POSI- 51
PRES- 111 ESEN-  80 STAD-  73 COMI- 63  QUES- 56  EPRE- 50
UNTO- 111 ONDE-  80
```

Look at the above groups. Realize how many apply to English. Such words as economy, business, energy, genes, firmament, etc.

Initial Trigraphs (The 19 trigraphs appearing 50 or more times as initials of words in 10,129 Spanish words):

```
CON- 298  PAR- 154  PUN-  93  INT-  72  UNI-  55  CUA-  52
COM- 218  PRO- 139  PER-  80  RES-  72  DES-  53  TRA-  52
EST- 194  PRE- 114  GOB-  66  NUE-  66  INF-  53  REP-  51
ARG-  50
```

Average Spanish Word Length = 5.9 letters

One-letter words: Y(63%) A(32%) O(4%) N(1%) E

Two-letter words: DE LA EL EN ES UN NO SE SU LO LA HA MI ME AL YO

Three-letter words: QUE LOS UNA POR DEL CON LAS MAS SON SER UNO SIN HAY MIS SUS ESE

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

Finals: O A S E N R B D L I Z

Rearranged Frequency:

```
13 13 9  8 7 7 7 5 5 4 4 4 3 3 1 1 1 1 1 1 1 - - - - - - - - -
E  A  O  S R N I D L C T U M P G Y B Q V H F Z J X CH LL RR N^
```

The Spanish alphabet consists of 24 letters (sans K W rare) plus four distinct ones: n^ (counted as n) ch, ll, rr. These four additional are alphabetized as single letter consonants. My keyboard does not have the appropriate symbol the tilde to put over the n so I have used the hat symbol.

Peculiarities:

The apostrophe is not used.

The question and exclamation marks appear at the end of the sentence, and are inverted at the beginning.

Q is followed by UE or UI.

The article the and pronouns he, she, it, they, are expressed by: el=the, he; la=the, she; lo=the, it; los =the, they;las =the, they (fem).

Some Short Words:

A. at, to, on, by, in, up,as, if, for, like, with of
E. and
O. or, repeated
U. before o or ho
Y. and
Ni. nor
Mas. but, yet, more, over
Como. How
Un, una. an, one.
Este, estos, estas, esta. this, these
Yo, I; mi=me; mia=my, mine
Usted. you
La, elle. she, the
Su. possesive pronoun
Ese,esa,eso. who
Quien. who, whom
Cual. which
Estar. to be
haber. to have

SOLVING SPANISH CRYPTOGRAMS

A good place to initially attack a Spanish cryptogram is through short words that appear in the cryptogram, especially single-letter and double letter words. A single letter word will usually be A or Y with a rare O. Look at the frequencies. Move on to the two and three letter words and cross reference the plain text with the cipher text alphabet. Reference [SPAN] has many practice cryptograms with hints. And now for our last foray with Xenocrypts we look at Portuguese.

PORTUGUESE One of the world's toughest languages. [PORT]

PORTUGUESE DATA [Based on 45,106 letters of text in FRE2]

Absolute Frequencies

A	5,362	G	724	L	1,245	Q	348	V	737
B	470	H	304	M	1,699	R	3,292	W	24
C	2,285	I	3,314	N	2,912	S	3,409	X	166
D	1,900	J	160	O	5,001	T	2,679	Y	22
E	5,441	K	17	P	1,377	U	1,491	Z	207
F	520								======
									45,106

Monographic Kappa Plain, Portuguese Language = 0.0746, I.C.= 1.940

Relative Frequencies, based on 45,106 letters of Portuguese plain text referenced in FRE2 reduced to 1000 letters:

E	121	N	65	U	33	F	11	X	4
A	119	T	59	P	30	B	10	J	3
O	111	C	51	L	28	Q	8	W	1
S	76	D	42	V	16	H	7	Y	-
I	73	M	38	G	16	Z	5	K	-
R	73								=======
									1,000

Groups

Vowels: A, E, I, O, U, Y = 45.8%
High-Frequency Consonants: N, R, S, =21.3%
Medium-Frequency Consonants: C, D, L, M, P, T= 24.8%
Low-Frequency Consonants:B,F,G,H,J,K,Q,V,W,X,Y,Z = 8.1 %

8 most frequent letters (E, A, O, S, I, R, N, and T) = 69.7%
(descending order)
Note that group frequencies between French, Spanish, Italian and Portuguese are statistically similar.

Initials (based on 7,058 letters of Portuguese plain text, One letter words have been omitted.)

P	847	M	405	I	264	B	113	Z	14
C	731	T	348	F	222	G	111	W	11
E	608	R	316	Q	222	J	92	K	7
S	601	N	299	O	187	U	77	Y	4
A	597	V	271	L	143	H	60	X	2
D	506								7,058

Digraphs [Frequency Distribution of Digraphs based on 45,106 letters of Portuguese plain text reduced to 5,000 digraphs]

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	11	11	52	60	15	9	14	2	18	2		38	36
B	11			1	10				5			2	1
C	60		2		30			4	39			5	
D	45				61				33				1
E	15	5	48	22	11	11	23	1	27	6	1	31	44
F	9				14				13			1	
G	15				14				4			1	
H	10				8				3				
I	42	3	34	31	6	7	9		1			16	22
J	7				2								
K													
L	24	1	4	4	24	1	5	9	21			2	4
M	41	10	3	4	51	1			26	1		1	2
N	31		29	35	14	7	8	12	18				
O	21	9	32	25	27	10	7	3	20	4		20	36
P	26		2		25				2			4	
Q					1								
R	75	2	14	9	86	3	7	1	46	1		2	18
S	41	6	22	10	62	6	3	2	23	2		3	12
T	65		1	1	69	1			26				
U	22	5	5	7	26	1	4		18	1		14	11
V	11				37				23				
W	1												
X	10		3		1				2				
Y													
Z	7		1		9				2				1

Digraphs [Frequency Distribution of Digraphs based on 45,106 letters of Portuguese plain text reduced to 5,000 digraphs]

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	56	49	23	8	68	72	22	8	16	1			5
B		9			9	2	1	2					
C	1	85			7		8	12					
D		61			2	1	1	5					
E	97	6	18	6	76	95	20	7	12	1	15		5
F		15			2			3					
G	1	14			14			15					
H		11						1					
I	53	26	5	2	25	39	27	2	10		2		7
J		2						7					
K													
L	2	14	4	2	1	4	7	6	2				
M	1	16	15	1	3	5	2	6	2				
N		25	1			19	114	4	4				1
O	79	5	35	8	71	85	18	12	22	1	1	1	1
P	1	60	1	1	28	1	1	3					
Q								37					
R	8	34	7	3	11	8	18	4	6				1
S	5	23	35	7	4	40	47	18	5				
T	1	88			33		1	13					
U	17	2	4	7	9	6	11		1				2
V		9			1								
W													
X			3				1						
Y													
Z		1		1	1								

Digraphic Kappa plain, Portuguese = 0.0084, I.C. = 5.68

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

NT-	114	TA-65	ST-	47	AM-	36	CE-	30	OD-	25	AT-	22
EN-	97	a)====	RI-	46	b)====		NC-	29	NO-	25	UA-	22
ES-	95	SE-62	DA-	45	ND-	35	PR-	28	LA-	24	GA-	21
TO-	88	DO-61	EM-	44	OP-	35	IT-	27	LE-	24	LI-	21
RE-	86	DE-61	IA-	42	SP	35	OE-	27	AP-	23	OL-	20
CO-	85	AD-60	MA-	41	RO-	34	EI-	27	EG-	23	ET-	20
OS-	85	PO-60	SA-	41	IC-	34	UE-	26	VI-	23	OI-	20
ON-	79	CA-60	SS-	40	TR-	33	MI-	26	SO-	23	NS-	19
ER-	76	AN-56	CI-	39	DI-	33	IO-	26	SI-	23	SU-	18
RA-	75	IN-53	IS-	39	OC-	32	PA-	26	OV-	22	RT-	18
AS-	72	AC-52	AL-	38	EL-	31	TI-	26	SC-	22	EP-	18
OR-	71	ME-51	VE-	37	ID-	31	PE-	25	IM-	22	UI-	18
TE-	69	AO-49	QU-	37	NA-	31	IR-	25	ED-	22	=====	
AR-	68	EC-48	OM-	36							3,755	

a) 15 digraphs (1,224 total count, above this line represent 25% of Portuguese plain

b) 42 digraphs (2,505 total count, above this line represent 50% of Portuguese plain

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

```
ES-   95   SE- 62  OR- 71  RO- 34  ME- 51  EM- 44
RE-   86   ER- 76  CA- 60  AC- 48  EC- 48  CE- 40
CO-   85   OC- 32  AD- 60  DA- 41  MA- 41  AM- 36
RA-   75   AR- 58  PO- 60  OP- 39  CI- 39  IC- 34
AS-   72   SA- 41  AN- 56  NA- 33  DI- 33  ID- 31
```

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

```
NT-  114   TN-  1  ST- 47  TS- 0  ND- 35  DN-0
```

Doublets (based on previous 5,000 digraphs)

SS- 40 EE- 11 OO- 5 LL- 2 II- 1 PP- 1 TT - 1 AA- 11 RR- 11 CC- 2 MM- 2

Initial Digraphs 20 digraphs occurring 100 or more times based on 6,803 Portuguese plain text words, according to absolute frequencies:

```
CO-  464  RE- 276  IN- 188  PA- 143  MA- 130  ME- 111  TR- 103
PO-  386  DE- 259  ES- 173  NA- 133  PE- 122  MI- 105  DI- 102
SE-  333  QU- 220  PR- 169  TE- 132  VE- 115  NO- 104
```

Trigraphs (top 59 based on 45,106 letters of Portuguese text)

```
ENT- 474  TOS- 191  ERE- 150  IDA- 133  OSE- 126  ECE- 115
NTO- 457  EST- 186  CIA- 145  TER- 132  ARE- 125  NCI- 114
ONT- 303  ACA- 182  ADE- 143  OPO- 130  ESE- 124  REC- 113
NTE- 284  PES- 181  STA- 143  SPO- 130  OVE- 124  PAR- 112
CON- 255  QUE- 172  ICA- 142  ADA- 129  SSA- 124  ESS- 110
PON- 236  NTA- 167  OCO- 140  TRA- 129  DES- 123  DAD- 109
CAO- 227  POR- 159  ARA- 136  NDO- 127  ECO- 121  ORE- 108
ADO- 211  ACO- 158  DOS- 134  ENC- 126  ODE- 118  EDI- 107
MEN- 205  COM- 154  OES- 134

ASE- 105
ITO- 104
ELE- 103
ERI- 103
PRO- 102
AME- 101
OSS- 101
IME- 100
```

Initial Trigraphs (The 19 trigraphs appearing 50 or more times as initials of words in 6,803 Portuguese words):

```
CON- 224  QUE- 109  PRO-  93  QUA-  83  TRA-  66  VEX-  53
PON- 213  EST- 105  POR-  88  DES-  71  MIL-  61  IND-  52
COM- 136  PAR-  93  NAO-  86  SER-  70  REF-  56  RES-  52

REC-  51
```

Tetragraphs (38 top tetragraphs based on 45,106 letters of Portuguese plain text)

```
ONTO-233  ENTA- 97  AMEN-81   CONT-58   CONS-58   RENT-52
PONT-221  NCIA- 95  PARA-81   FORM-57   NTES-58   TELE-52
MENT-183  PORT- 87  COES-73   OCON-66   ANDO-57   EGRA-51
ENTO-173  DADE- 86  IDAD-71   ELEG-61   ANTE-57   NFOR-51
ENTE-147  ESTA- 85  CENT-70   ADOS-60   ORMA-54   OPON-51
ACAO-142  ENCI- 83  INTE-70   IMEN-60   VEXA-54   LEGR-50
NTOS-141  SPON- 83
```

Look at the above groups. Realize how many apply to English. Such words as economy, business, energy, genes, firmament, etc.

Average Portuguese Word Length = 6.48 letters

One-letter words: A O E D'

Two-letter words: DE UM AS SE DO OS EM NA NO

Three-letter words: QUE NAO UMA COM POR TAO MAS MEU DAS ERA LHE NEM NOS SER SIM SUA; ELE

Four-letter words: AZUL DIAS DUAS ESTA MAIS MEUS NOME PODE QUEM TRES VIDA; SEUS SUAS COMO PARA TODO

Common Pattern Words - Three and Four letters:

Normal frequency rearranged:

```
14 13 12 8 8 6 6 5 5 5 4 4 4 3 2 2 1 1 1 1 1 - -
A  E  O  R S I N D M T U C L P Q V F G H B J Z X
                    from [XENO]
```

Peculiarities:

The Portuguese language uses the standard Roman alphabet, but the letters K W Y are used in foreign words. Like Spanish, however the cion becomes cal, the ll goes to lh. Articles drop the inital l; the Spanish las and los become as and os in Portuguese.

Plurals end in -s; such as -es,-is, -oes, and -aes are common.
Adjectives carry the plural along with the noun they modify.

SOLUTION OF PORTUGUESE ARISTOCRAT

POR-1. (156) Flying very high. BARKER

```
1                    2                    3

P J    G J R B P H G Y R G J    I C W Q G B G B G A

3        4             5                6       7

U Y C    G    B C W Y X C B G W G P     I C    I P D J

8                    9           10

Y G R C Q D R C J     G    I C B D Z G

         11              12        13          14

W P H J R D R Y D G     Y A G    X B P Z G     I G

         15                  16         17       18

Z C B J G R D Q D I G I C     I G     H G Z  C     C

  19      20          21        22      23

A G D J    Y A    X G J J P    X G B G    G

           24          25          26          27

W P H J R B Y W G P     H P      C J X G W P     I C

 28              29               30

Y A G     C J R G W G P      X C B A G H C H R C.
```

Set up the cross reference alphabets:

```
31 18 14 12 11 10 9  8  8  8  7  6  6  4  3  1     0
G  C  J  P  B  R  I  Y  W  D  H  A  X  Z  Q  U  EFKLMNOSTV
                                                 -Cipher
14 12 12 8  8  6  6  5  5  5  4  4  4  3  2  2  1  1     0
A  E  O  R  S  I  N  D  M  T  U  C  L  P  Q  V  F  GHBJ ZX
                                                 -Normal
```

I made an assumption that the tip might refer to astronaut or astronomy. Let G= a, J=s, C=e. On my worksheet I draw lines between the normal and cipher alphabets to show relationships between letters.

```
1                    2                  3
  s    a           a     a s      e     a   a   a
P J    G J R B P H G Y R G J    I C W Q G B G B G A

3        4             5                 6       7
    e    a      e       e   a   a         e          s
U Y C    G    B C W Y X C B G W G P     I C    I P D J

8                    9           10
  a   e       e s     a      e       a
Y G R C Q D R C J     G    I C B D Z G

         11              12        13          14
      s           a         a           a       a
W P H J R D R Y D G     Y A G    X B P Z G     I G

         15                   16         17       18
  e   s a           a   e       a       a    e     e
Z C B J G R D Q D I G I C     I G     H G Z  C     C

  19      20          21        22      23
  a   s             a s s       a   a    a
A G D J    Y A    X G J J P    X G B G    G

           24          25          26          27
      s         a                 e s   a          e
W P H J R B Y W G P     H P      C J X G W P     I C

 28              29                30
    a     e s   a   a          e     a   e     e
Y A G     C J R G W G P      X C B A G H C H R C.
```

Word two falls in line with my assumption = astronautas and word 1 could be PJ= os. Word 30 might be permanente. Other words appear uma, para, passo, espaco. Filling in the blanks we have the following:

```
1                   2                3
o s   a s t r o n a u t a s   d e c l a r a r a m
P J   G J R B P H G Y R G J   I C W Q G B G B G A

3       4            5               6       7
q u e   a   r e c u p e r a c a o   d e   d o i s
U Y C   G   B C W Y X C B G W G P   I C   I P D J

8                   9          10
s a t e l i t e s   a   d e r i v a
Y G R C Q D R C J   G   I C B D Z G

        11             12        13         14
c o n s t i t u i a   u m a   p r o v a   d a
W P H J R D R Y D G   Y A G   X B P Z G   I G

        15                  16        17       18
v e r s a t i l i d a d e   d a   n a v e   e
Z C B J G R D Q D I G I C   I G   H G Z C   C

  19      20          21        22      23
m a i s   u m   p a s s o   p a r a   a
A G D J   Y A   X G J J P   X G B G   G

          24          25          26          27
c o n s t r u c a o   n o   e s p a c o   d e
W P H J R B Y W G P   H P   C J X G W P   I C

 28              29              30
u m a   e s t a c a o   p e r m a n e n t e
Y A G   C J R G W G P   X C B A G H C H R C.
```

Note the -cao endings

REVIEW OF LECTURES 1-7

We have studied the simple substitution case in detail. We have focused on the similarities between languages - especially the group frequencies. We have attempted to show a cultural universality for cryptography and the learning of languages. We have presented procedures to cryptanalyze most single alphabet substitution systems, including the more difficult variants. We have searched for historical significance as we proceeded in our cryptographic tour.

WHAT'S NEXT?

Two guest lecturers NORTH DECODER and ESSAYONS will present materials on the Hill Cipher, and ENIGMA 95. I shall open up the polyalphabetic substitution case. Remember, that the trick in solving a polyalphabetic substitution cipher is its reduction to simpler terms, i.e. reduction to a series of one or more mon-alphabetic sub-systems. The concept of periodicity will be introduced. I will cross the lines and introduce transposition ciphers. The most famous Playfair that saved a U. S. Presidents life will be detailed. The resource section will be improved again by about 100 solid references.

OTHER STUFF

By the way, our class as of this writing is 109! Four others have requested access. I thank you all for your confidence and support. Those who wish to present a special cipher or to have your guest lecture included in this course need to contact me soon, so that I can schedule them. If you want to construct a few problems (based any material covered) for presentation in the final "book", go for it. E-mail/snail mail them to me with complete solutions and sources. Again thank you for your trust and interest.

HOMEWORK FROM LECTURE 6

FRE-2. K2. (105) Another species. {sauvage,fp=ST] MELODE

P Q N X B M H Q I Q A B C I Q D K E X Q B Q O Q

P' W M R R Q; D K E X Q B Q O Q U Q I Q E Q Q M C

T E X R X B X D Q , X P Q A B K P' W M R R Q N Q

V C Q N W K B O Q U M C B B X Q E Q Q A B K C

N W K B A K C D K U Q.

FRE-3. K2. (87) (jamais, A=b) It's fun trying. GUNG HO

D G X Z Q N J D P M C J P U P L S U E' Z D

Z D H U Q J S E J S N P U Q E Z H Z D P M J H -

K N D P: G Z K U D I Q S N U , G Z H S P D L S U,

U Q G U P O Z H U P . * R J I Q U I U G G U

FRE-4. PAT from [GIVI] page 13.and ff. (130)

Solve and recover key(s).

YJXMG XBXUF JGECU JEBZD XAMNM ZDFLG FAFNJ OFNDJ

GVJXE FNNME VRJZJ KAFNB FNZAG NCUJE BNRUX OFNJG

NNXKX FELGF BJRVF NOFUI FXAAF GTFVR FAFKU FNBJE

NADXN VMXUF

ITA-2. K2. (88) (ne, han, con) Thirty days hath September. LABRONICUS

I D S A I K Q W P L A I K A L B S C M D S P L A

K E D W Z S, U W O U A L S R S I I S C M D S . Q W

B S A I L I I L P S A ' S O A L. I O I I W U Z W

K Z I D W A S V K A I D S A U I O A L.

ITA-3. K2. (117) (sulla, f=I). La frode necessaria. MICROPOD

G Z Q K E A F S Z L T K F Q A Q S F N F Q K G K Q

T G G Z P Z Q F R A T J Z E F N S Z M T Z J S A S

Z R A P T D A F F Q K G K Z L Z S S K E O F J F Q

Q T J K R A E Z F Q Z S S Z H F J S F M T F G G K

E O F L F J Q Z G A J X T S Z J D.

SPA-1. BARKER

Z K E P C U K Y T C Y D M S R V C T P E R A

Z P Z N D Z K G C T Y R Z K R N T D G R Y C V K

K S T P Q D P E R M K T C Y G R Z Y P Q P M P E K E

E C M K S C Z S K E R G R T C M U R U C Z S R.

SPA-2. K2. (96) (deseo, f=R) Musica. D. STRASSE

T I Z Q B J N A Z K J K T F Z N B P L T B B F

K N A G B N A G K T F P J G T P A O Z F M B F

S J G H N B R T B T I K T N Z G B I Q B

B P K J I Q Z I B J M P B B J N A Q G A O J M B

M Z I Y Z N.

SPA-3. (122) (-ulado, MZ=qk) Flight? LIFER

N S P Y K I X P U A K P Z D X P S P E X K R L K O

K A X T S P Q K D X R K R R S S I N K Y K R L A R

S D K T Q L D L P X K T A S Q X S P X P R S O S P

R X J K R K T O A S T S P Q X L S D O A X I S A E

C S D L R S C P V D L N L B A X O C D K R L.

POR-2. K2 (96) (tenta; gj=NQ) Machine Age? YO TAMBIEN

E P E J T X D U R T C J Z X G C V R J D J

X I N R S O C H C D T C V R P U C D V R J

Z J U D C T J H J D G X U M P C H J A X H X

O X T J T V R J A J U A C M C B J S X.

*O. *T R T M X I H *Q X U J D

POR-3. K1. (nossos va-) Letter to horseman? ZYZZ

U C U C G V C J F D E F W E O C B G C V S I H C L

I T I W F Y C V F U H F W F T L F R F B C H W F C

E S H I L F G I C D E G T I J H C V G R P C V C J

F V D E F W F H C V L F V F H J I S K I X J I Z U

I G V T I V V I V B C D E F G H I V V C I F Y K F

R F T W F V.

SOLUTIONS TO LECTURE 6 PROBLEMS

Thanks to GRAPE JUICE for the straightforward SOLS.

LAT-1 K2. (sallust) Wars and Victors? SCARLET (105/17)

```
FCDR JRBBQC OQCN TZUNBR, URPRMQC ZRHRMMQCR GRONDRMR.
NDUNKRMR UQNSNO, RPNZC NHDZSF BNURMR, GRKFDN, UQCS  NUPFMRO
SRBNDP. *OZBBQOP                          [cum,  bdghj=JGHIE]
```

Omne bellum sumi facile, ceterum aegerrume desinere. Incipere cuivis, etiam ignavo licere, deponi, cum victores velint. - Sallust

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

K2 = JUGRTHINE

After placing the very generous tips, the solution was a simple matter of filling in the key alphabet. Solution time about 5 minutes.

NOR-1. Cosmology. (verden) (*qwx) NIL VIRONUS (109/22)

```
IKPNH ERAMC KDAOA GPKMK NNKMK MEKOK MZLAG
GKQPH EVKMM KGKOK GPDAO VFIIK GHKRF DOIFV
FGNCF JPKRK MIKGN FEKGG KNCKP FDYKM PKAGN PKAG.
```

K2 = FYSIKK LOVA

Det som virkelig interesserer meg er ae inne ut om herren egentlig hadde noe vagg da han skapte verden sa mennesket. Albert Einstein

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

Letting e=K, there was only one position for VERDEN. This gave the interesting pattern ERE??ERE at letter 18. Trying the pattern ABaCcaba in my Norwegian word list gave the word INTERESSERER. This in turn gave ERTEINSTEIN at the end of the gram, which implied Albert Einstein. From that point on the solution was a matter of filling in the key alphabet. Solution time about 1 hour.

REFERENCES / RESOURCES [updated 3 February 1996]

[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.

[BAZE] Bazeries, M. le Capitaine, " Cryptograph a 20 rondelles-alphabets," Compte rendu de la 20e session de l' Association Francaise pour l'Advancement des Scienses, Paris: Au secretariat de l' Association, 1892.

[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.

[BOWE] Bowers, William Maxwell, "The Bifid Cipher, Practical Cryptanalysis, II, ACA, 1960.

[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.

[BROG] Broglie, Duc de, Le Secret du roi: Correspondance secrete de Louis XV avec ses agents diplomatiques 1752-1774, 3rd ed. Paris, Calmann Levy, 1879.

[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).

[DELA] Delastelle, F., Cryptographie nouvelle, Maire of Saint-Malo, P. Dubreuil, Paris, 1893.

[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.

[HAWC] Hawcock, David and MacAllister, Patrick, "Puzzle Power! Multidimensional Codes, Illusions, Numbers, and Brainteasers," Little, Brown and Co., New York, 1994.

[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.

[ITAL] Italian - English Dictionary, compiled by Vittore E. Bocchetta, Fawcett Premier, New York, 1965.

[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.

[KERC] Kerckhoffs, "la Cryptographie Militaire, " Journel des Sciences militaires, 9th series, IX, (January and February, 1883, Libraire Militaire de L. Baudoin &Co., Paris. English trans. by Warren T, McCready of the University of Toronto, 1964

[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.

[LEAU] Leaute, H., "Sur les Mecanismes Cryptographiques de M. de Viaris," Le Genie Civil, XIII, Sept 1, 1888.

[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.

[MAGN] Magne, Emile, Le plaisant Abbe de Boisrobert, Paris, Mecure de France, 1909.

[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.

[MAVE] Mavenel, Denis L., Lettres, Instructions Diplomatiques et Papiers d' Etat du Cardinal Richelieu, Historie Politique, Paris 1853-1877 Collection.

[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., "2erman 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.

[NICK] Nickels, Hamilton, "Codemaster: Secrets of Making and Breaking Codes," Paladin Press, Boulder, CO., 1990.

[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.

[PERR] Perrault, Charles, Tallement des Reaux, Les Historiettes, Bibliotheque del La Pleiade, Paris 1960, pp 256-258.

[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.

[PORT] Barker, Wayne G. "Cryptograms in Portuguese," Aegean Park Press, Laguna Hills, CA., 1986.

[POR1] Aliandro, Hygino, "The Portuguese-English Dictionary," Pocket Books, New York, N.Y., 1960.

[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)

[SMIH] Smith, David E., "John Wallis as Cryptographer", Bulletin of American Mathematical Society, XXIV, 1917.

[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.

[SPAN] Barker, Wayne G. "Cryptograms in Spanish," Aegean Park Press, Laguna Hills, CA., 1986.

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

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

[STIX] Stix, F., Zur Geschicte und Organisation der Wiener Geheimen Ziffernkanzlei, Mitteilungen des Osterreichischen Instituts fir Geschichtsforschung, LI 1937.

[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.

[USAA] U. S. Army, Office of Chief Signal Officer, "Instructions for Using the Cipher Device Type M-94, February, 1922," USGPO, Washington, 1922.

[VAIL] Vaille, Euggene, Le Cabinet Noir, Paris Presses Universitaires de Frances, 1950.

[VALE] Valerio, "De La Cryptographie," Journal des Scienses militares, 9th series, Dec 1892 - May 1895, Paris.

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

[VIAR] de Viaris in Genie Civil: "Cryptographie", Publications du Journal Le Genie Civil, 1888.

[VIA1] de Viaris, "L'art de chiffre et dechiffre les depeches secretes," Gauthier-Villars, Paris, 1893.

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

[WALL] Wallis, John, "A Collection of Letters and other Papers in Cipher" , Oxford University, Bodleian Library, 1653.

[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)