Classical Cryptology

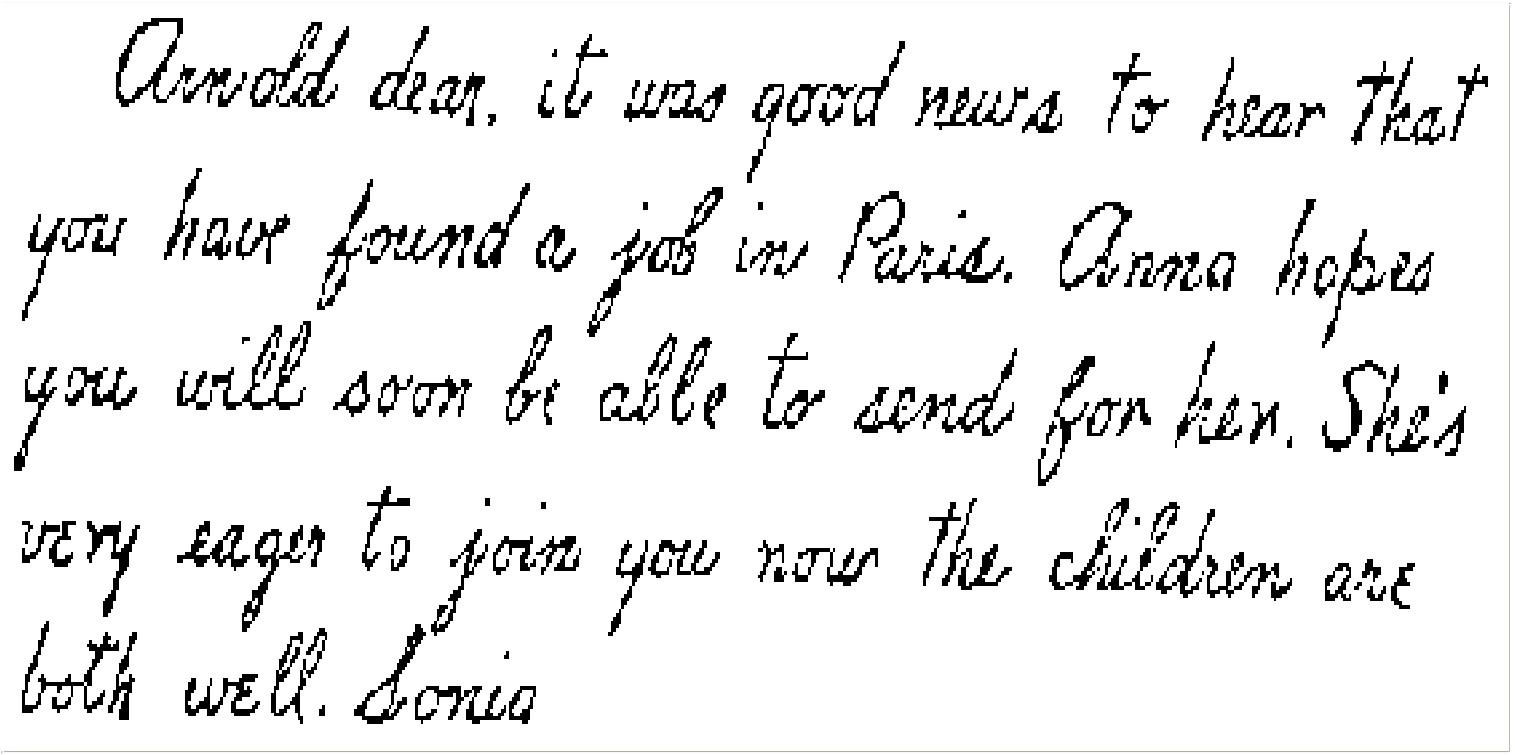
Concealment Cipher

Worthie Sir John:- Hope, that is ye beste comfort of ye afflicted, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking me. 'Tis not much that I can do: but what I can do, bee ye verie sure I wille. I knowe that, if dethe comes, if ordinary men fear it, it frights not you, accounting it for a high honor, to have such a rewarde of your loyalty. Pray yet that you may be spared this soe bitter, cup. I fear not that you will grudge any sufferings; only if bie submission you can turn them away, 'tis the part of a wise man. Tell me, an if you can, to do for you anythinge that you wolde have done. The general goes back on Wednesday. Restinge your servant to command. - R.T.

Concealment Cipher

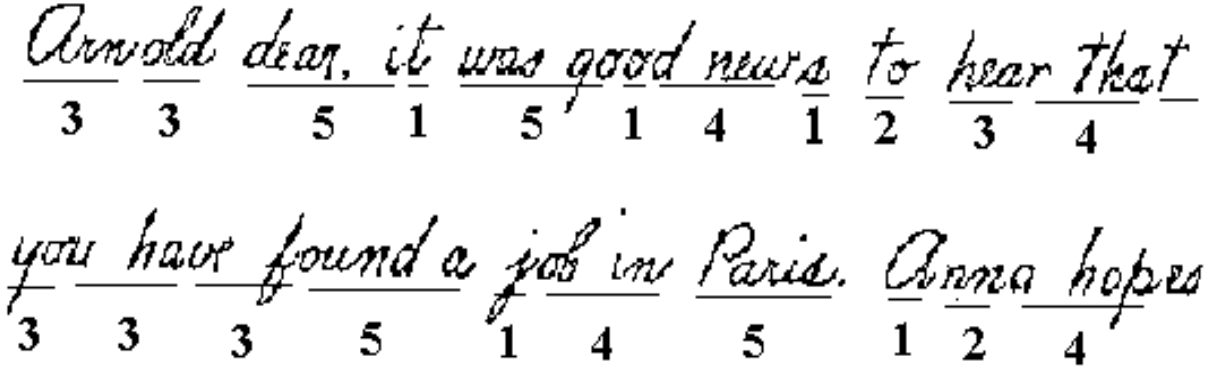
Worthie Sir John:- Hope, that is ye beste comfort of ye afflicted, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking me. 'Tis not much that I can do: but what I can do, bee ye verie sure I wille. I knowe that, if dethe comes, if ordinary men fear it, it frights not you, accounting it for a high honor, to have such a rewarde of your loyalty. Pray yet that you may be spared this soe bitter, cup. I fear not that you will grudge any sufferings; only if bie submission you can turn them away, 'tis the part of a wise man. Tell me, an if you can, to do for you anythinge that you wolde have done. The general goes back on Wednesday. Restinge your servant to command. - R.T.

Russian Nihilist


Arnold dear, it was good news to hear that
you have found a job in Paris. Anna hopes
you will soon be able to send for her. She's
very eager to join you now the children are
both well. Sonia

Russian Nihlist

By counting the number of letters between those letters whose "tails" point upwards, we get the following sequence of numbers.



33 51 51 41 23 43 33 51 45 12 43 24 11 34 34 11 34 34 42 33 11 44 42 43 33

Now use the following table to decrypt this message:

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

To get: NEEDMONEYFORASSASSINATION

Bacon's Bi-literal Cipher

An*oth*e*r* examp*l*e of t*h*is typ*e* *i*s *t*he *Fran*cis Bac*on* Bi-l*it*era*l* cipher w*h*e*r*e tw*o* *s*lightly different typefaces are used to conceal a binary code of length 5. At the end of the 19th century, a Mrs. Gallup studied the first edition of one of Bacon's early works, and on the title-page, hidden under two sets of italics, she discovered the name of William Rowley - Bacon's chief secretary.

Bacon's Bi-literal Cipher

An*oth*e*r* examp*l*e of t*h*is type *i*s *t*he *Fran*cis Ba*con*

aabbb abaaa aabaa aabaa aaabb ababb abbaa aaabb

H I D D E N M E

Bi-l*it*era*l* cipher w*her*e tw*o s*lightly

baaab baaab aaaaa aabab aaabb.....

S S A G E

A - *aaaaa*
B - *aaaab*
C - *aaaba*
D - *aabaa*
E - *aaabb*
F - *aabba*
G - *aabab*
H - *aabbb*

IJ - *abaaa*
K - *abaab*
L - *ababa*
M- *abbaa*
N - *ababb*
O - *abbba*
P - *abbab*
Q - *abbbb*

R - *baaaa*
S - *baaab*
T - *baaba*
UV - *babaa*
W- *baabb*
X- *babba*
Y- *babab*
Z -*babbb*

Transposition Ciphers

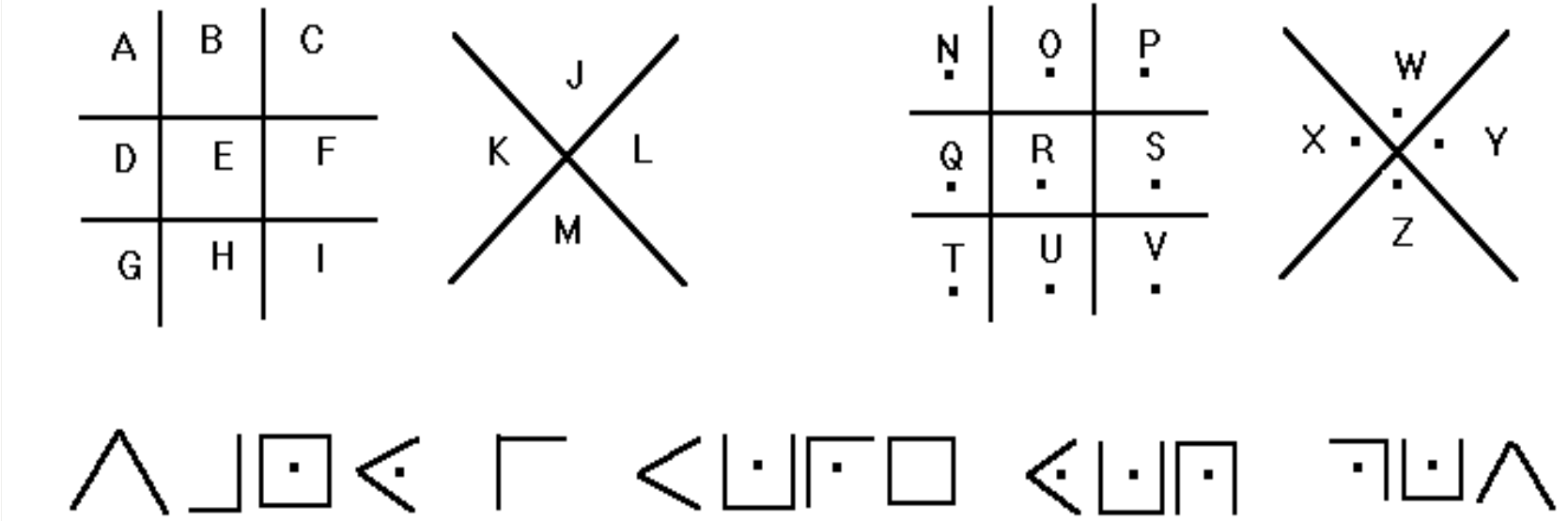
THIS IS A PHONY MESSAGE BUT IT SERVES ITS PURPOSE, (40 letters). We write the letters in an 8×5 array (one choice amongst many possible sizes) to get:

T H I S I
S A P H O
N Y M E S
S A G E B
U T I T S
E R V E S
I T S P U
R P O S E

By columns: TSNSU EIRHA YATRT PIPMG IVSOS HEETE PSIOS BSSUE

By diagonals: TSHNA ISYPS UAMHI ETGEO IRIES RTVTB PSESO PSSUE

Substitution (Freemason) Cipher



M A R Y I L O V E Y O U T O M

Substitution Ciphers

Caesar's (Shift) Cipher

Graph Theory rots $\rightarrow$ JUDSK WKHRUB URWV

General Shift Cipher:

$$\mathbf{x \rightarrow x + a \pmod{26} \qquad 0 \leq a \leq 25}$$

Affine Cipher:

$$\mathbf{x \rightarrow ax + b \pmod{26} \qquad (a,26) = 1}$$

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Substitution Ciphers

Monoalphabetic:

Any permutation of the letters can be used for the substitution. The "trick" is trying to remember the permutation.

Using a keyword or phrase:

Keyphrase: Dave Brown eats it

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
d	a	v	e	b	r	o	w	n	t	s	i	c	f	g	h	j	k	l	m	p	q	u	x	y	z

Substitution Ciphers

Polygraph (Playfair):

Arrange alphabet in a 5×5 grid and replace pairs by:

1) in same row, use letters to the right.
2) in same column, use letters below.
3) else, use letters in same row in opposite corners.

Message: Just kidding dave

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

JU ST KI DX DI NG DA VE

dj tu jm ub je oh eb dh

Enciphered: djtuj mubje ohebd h

Substitution Ciphers

Polyalphabetic (Vigenère - 1586)

In this type of substitution cipher, a letter is not
fl inki sinf or itnowflinkis infori t nowfli nk isi
NY BUSA LGCJ CW ANOGPNEDGSWF KVUVVZ T YSPYPZ VC VGB

always replaced by the same letter. This procedure
nforit nowflink is inf orit nowfli nkis inforitno
NQKRGL ESLQLKRN JQ BUJ GRUX YSPYPZ GRQK XETQVLNES

distorts the statistical frequencies of the original
wflinkis inf oritnowflin kisinforitn ow fli nkisinfo
ZNDBBBBK BUJ GKIMVGPNNIY PZWYHJBTQXF FB YSM BBQYQAFZ

message. A keyword or phrase is used, and duplicate
ritnowf l inkisin fo ritnow fl inki nfo ritnowfli
DMLFOCJ L SRJEGZQ TF GPKNGA ND CFOL NSR UCIYWYFEM

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25