Bacon's Bilateral Cipher (1561 – 1624)

Francis Bacon presented this example of a type of **steganography** (i.e., hiding the existence of the message).

Correspondents agree on an encoding of the alphabet.

The plaintext is hidden in an innocuous message by the selection of a font using the letter `a` for, say, plain-face, and `b` for bold-face.

See Figure 1.5 on page 13.

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

Example: If the plaintext is RHODES and the innocuous text is

ITS A BEAUTIFUL DAY IN THE
NEIGHBORHOOD

then the message is hidden as

R	H	O	D	E	S
baaaa	aabbb	abbab	aaabb	aabaa	baaab
ITSAB	EA**UTI**	F**UL**D**A**	YIN**TH**	EN**E**IG	**H**BOR**H**

When the proper spacing is put back in:

ITS A BEA**UTI**F**UL** D**A**Y IN **TH**E
N**E**IG**H**BOR**H**OOD

Jefferson’s Wheel Cipher (c. 1790)

Two correspondents possess sets of cipher wheels with alphabets such as those shown here in “unwrapped” form.

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

To encipher: 10-letter groups of plaintext are aligned horizontally and ciphertext is read from any desired row.

Example: `MONTICELLO` enciphers as `DWXBQMFGWD`.

Example: `VIDIMEFOZ` deciphers as `JOHN ADAMS`.

This is an example of a **polyalphabetic** cipher.

(See Figure 1.7 on page 15.)

Wheatstone-Playfair Cipher (1854)

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

with sides and top “glued together” as

Fig. 1.8 goes here

To encipher: Plaintext letter pairs determine corners of rectangles.

- If in same row, ciphertext is respective pair to right.
- If in same column, ciphertext is respective pair down.
- If in different row and column, ciphertext is pair in opposite corners.

To decipher: Reverse encipher.

Example: The plaintext WE ARE NOT AMUSED becomes

WE	AR	EN	OT	AM	US	ED
BH	PC	HA	GY	MN	TD	DC

Example: The ciphertext MQ OC EP FK becomes

PLAYFAIR

The Wheatstone-Playfair cipher is an example of a **polygraphic** or **block** cipher.

ADFGVX (1918)

Correspondents know the encoding table for letters and the keyword.

To encipher: Plaintext is coded using the letters A, D, F, G, V, X via the following chart. The resulting pre-ciphertext is then enciphered by a keyword columnar transposition.

	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	Ø	T	9

To decipher: Reverse the transposition and then decode using the chart.

Example: Encipher WE WILL WIN using the keyword ARMS.

plain:	W	E	W	I	L	L	W	I	N
pre-cipher:	DF	GX	DF	FD	AD	AD	DF	FD	XD

A	R	M	S
1	3	2	4
D	F	G	X
D	F	F	D
A	D	A	D
D	F	F	D
X	D		

Final ciphertext:

D D A D X G F A F F F D F D X D D D

ADFGVX Cipher

On the year that marked the beginning of World War I, England advanced ahead of Germany when the British cable ship Teleconia hauled up Germany's underwater cables used for overseas communications. That left the Germans with no choice but communication through international cables and radio transmission. In order to protect themselves from their enemies, Germany encrypted all of their communication. In response, England established a specialized organization that was dedicated to deciphering these messages.

(`http://global.mitsubishielectric.com/misty/tour/stage3/`)

ADFGVX Cipher

In cryptography, the ADFGVX cipher was a field cipher used by the German Army during World War I. ADFGVX was in fact an extension of an earlier cipher called ADFGX. Invented by Colonel Fritz Nebel and introduced in March 1918, the cipher was a fractionating transposition cipher which combined a modified Polybius square with a single columnar transposition. The cipher is named after the six possible letters used in the ciphertext: A, D, F, G, V and X. These letters were chosen deliberately because they sound very different to each other when transmitted via morse code. The intention was to reduce the possibility of operator error.

(from Wikipedia)

The ADFGX Cipher in World War I

The ADFGX cipher, developed by German army radio officer Fritz Nebel (1891–1967), made its appearance on March 5, 1918, when the Germans used it in a wireless transmission on the western front. Instead of the numerals 1 through 5 along a side of the Polybius square, Nebel's cipher applied the letters A, D, F, G, and X, which he chose because their equivalents in Morse code were so dissimilar that confusion was unlikely. (For example, A is one dot and two dashes, while D is one dash and two dots.) Three months later, on June 1, the German army added the letter V to make a sixth row and column. The 6 x 6 grid of the ADFGVX cipher allowed the inclusion of the 10 numerals from 0 to 9, like its predecessor.

The brilliance of the ADFGX cipher lay in the fact that, unlike ordinary codes, the frequency of letters such as E was not easy to recognize. Furthermore, the code could become even more challenging by applying a system of transposition. Suppose a message is written out in ADFGVX format–that is, as a series of two-letter combinations using just those six letters. That string of letters is then placed in a matrix under the letters of a chosen keyword, such as KAISER, which an army in wartime would typically change every day, Then the letters of the keyword are placed in alphabetical order–in this case, spelling AEIKRS, with the corresponding columns moved as well. After being transposed in this manner, the message is transcribed by reading down along each column, making it impossible for anyone who does not know the keyword to translate the message.

A modern computer would be capable of unscrambling such a transmission, even in a situation involving an unknown keyword, but the Allies in World War I were initially unable to break Nebel's code. However, French artillery captain Georges-Jean Painvin (1886–1980) did succeed in deciphering the code. Though his work was good only for a single day, it enabled the allied armies to counter the German offensive of June 9, 1918.

(www.espionageinfo.com/A-An/ADFGX-Cipher.html)