CODE BOOK

Caesar Cipher

Type: Substitution cipher

Description: Each letter in the plaintext is shifted a fixed number of places down the alphabet.

Historical Use: Julius Caesar used it to communicate with his generals.

Encryption:

1. Choose a shift value (e.g. 3).
2. For each letter in the plaintext, shift it forward by the chosen value in the alphabet.
3. Wrap around to the beginning of the alphabet if necessary.

Decryption:

1. Use the same shift value.
2. For each letter in the ciphertext, shift it backward by the chosen value in the alphabet.
3. Wrap around to the end of the alphabet if necessary.

Example:

Shift 3: HELLO = KHOOR

Vigenere

Type: Polyalphabetic substitution cipher

Description: Each letter in the plaintext is shifted according to a keyword.

Historical Use: Both the Confederate and Union armies in the American Civil War employed variations of the Vigenere cipher for secure communication among their forces.

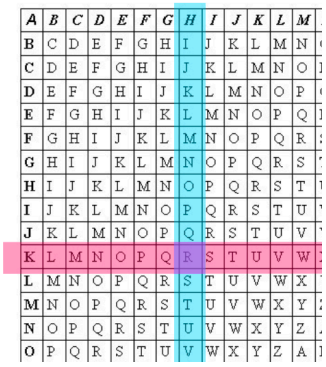
Encryption:

Find the intersection of the plaintext letter and the keyword letter in the Vigenere square. The letter at this intersection is the ciphertext letter.

Decyrption:

Find the row corresponding to the keyword letter and locate the ciphertext letter in that row. The column at this intersection is the plaintext letter.

Example:



Plaintext	Keyword	Ciphertext
H	K	R
E	E	I
L	Y	J
L	K	V
O	E	S

Plaintext: "HELLO" (H, E, L, L, O)

Keyword: "KEY" (K, E, Y, K, E)

Ciphertext: “RIJVS” (R, I, J, V, S)

Plaintext

Keyword

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

Pigpen

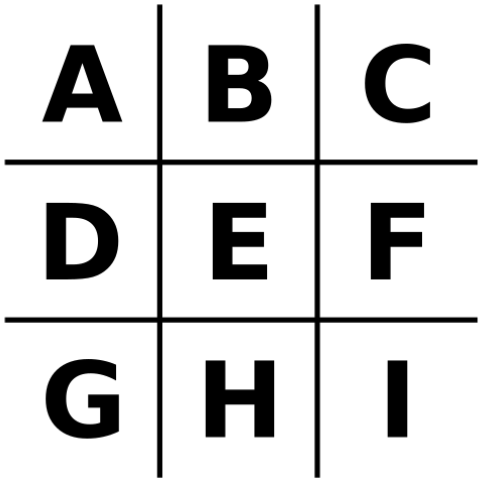
Type: Substitution cipher

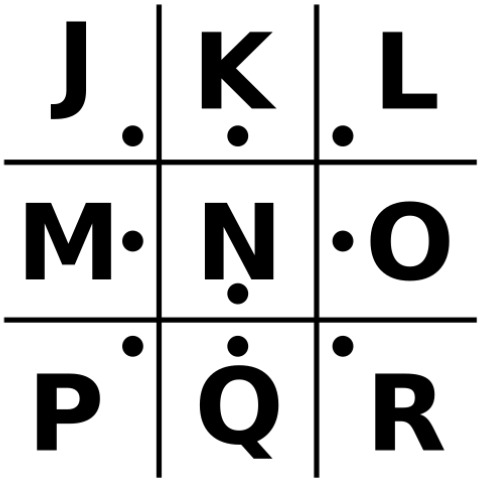
Description: Each letter is represented by a unique symbol derived from a grid or "pigpen" arrangement.

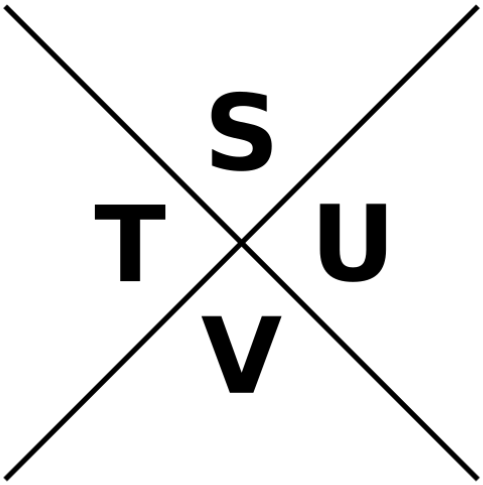
Historical Use: Used by Freemasons in the 18th century to keep their records private.

Replace each letter in the plaintext with its corresponding symbol from the grids.

HELLO = 







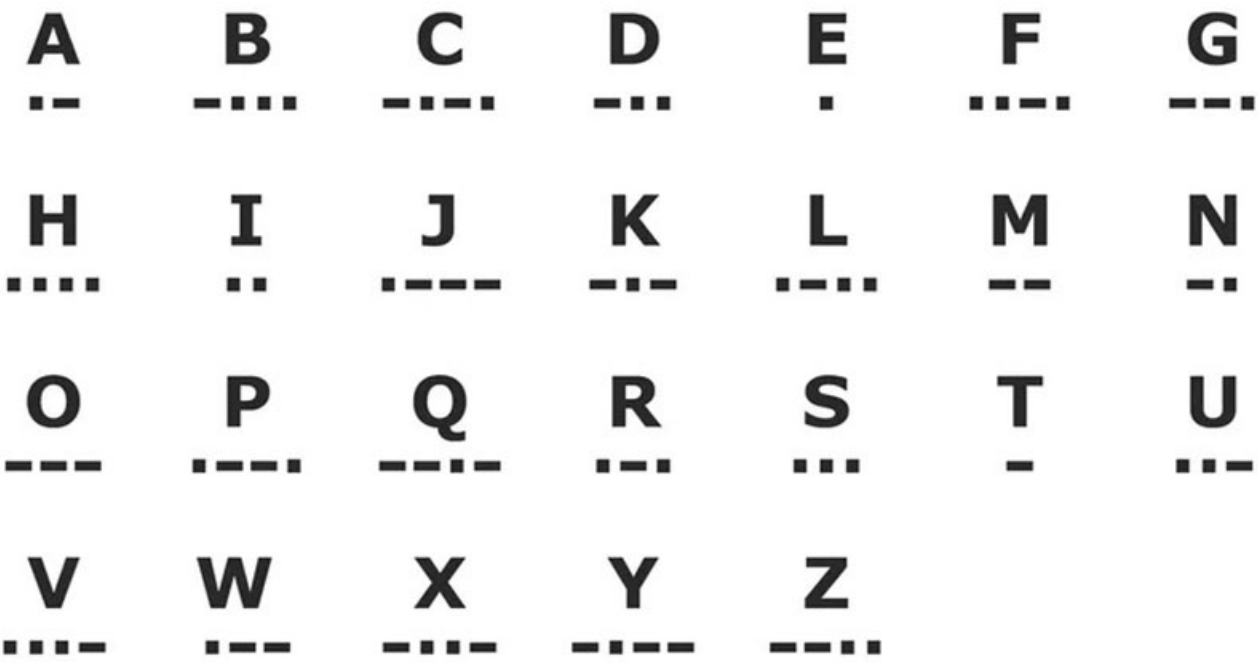
Morse Code

Type: Encoded transmission cipher

Description: Represents each letter and numeral as a sequence of dots and dashes.

Historical Use: Extensively used for telegraphic communication in the 19th and 20th centuries, notably by Samuel Morse.

Convert each letter of the plaintext into its corresponding sequence of dots and dashes.



Atbash

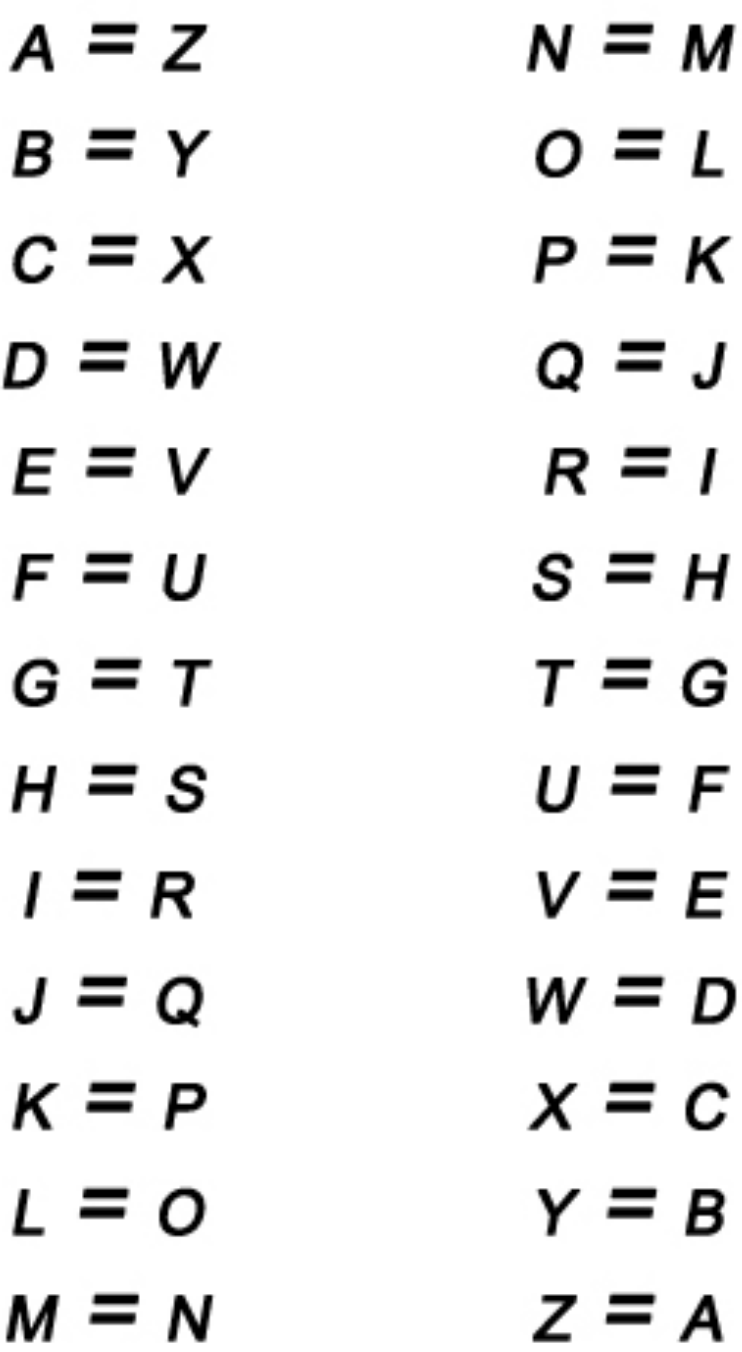
Type: Substitution cipher

Description: A simple substitution cipher where each letter of the alphabet is mapped to its reverse

Historical Use: Used in the Hebrew script for the book of Jeremiah and also by Jewish scholars.

Replace each letter in the plaintext with its corresponding letter in the reverse alphabet.

HELLO = ZVOOL



RailFence

Type: Transposition cipher

Description: The plaintext is written in a zigzag pattern on an imaginary fence, then read off line by line.

Historical Use: Used by soldiers during the American Civil War to encode messages.

Encrypt:

- Choose the number of rails, draw them out.
- Write in zigzag pattern, with the plaintext diagonally down and up across the rails.
- Read along the rails for the cipher text.

Decrypt:

- Draw rails and mark where letters should go.
- Write the ciphertext along the rails at each letter marking.
- Read along the zigzag pattern for the plaintext.

Plaintext T H I S I S A S E C R E T M E S S A G E

Rail Fence Encoding *key = 4*

T						A						T					G	
	H				S		S				E		M				A		E
		I		I				E		R				E		S			
			S						C						S				

Ciphertext T A T G H S S E M A E I I E R E S S C S

Baconian Bilateral Cipher

Type: Substitution cipher

Description: Uses sequences of 'A's and 'B's to represent each letter of the alphabet, encoding them into binary-like five-bit sequences.

Historical Use: Created by Francis Bacon in the early 17th century. It was used to encode secret messages in a way that could be hidden in plain text.

Translate each letter into its a five-letter sequence of 'A's and 'B's.

HELLO = AABBB AABAA ABABA ABABA ABBAB

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

Polybius

Type: Substitution cipher

Description: Uses a 5x5 grid to encode letters. Each letter is represented by its coordinates in the grid. For the English alphabet, I and J share a cell.

Historical Use: Invented by the Ancient Greek historian Polybius. Used for telegraphy and field ciphers.

Replace each letter with its coordinates (row, column).

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