Classical Cryptographic Ciphers: A Brief Overview

1 Caesar's Cipher

The Caesar cipher is one of the earliest substitution ciphers, named after Julius Caesar who used it for military communications. It shifts each letter in the plaintext by a fixed number of positions in the alphabet [web:1][web:2].

Encryption: $C = (P + k) \mod 26$

Decryption: $P = (C - k) \mod 26$

Example: With a shift of 3, the plaintext "HELLO" becomes "KHOOR":

- H $\rightarrow$ K, E $\rightarrow$ H, L $\rightarrow$ O, L $\rightarrow$ O, O $\rightarrow$ R

2 Multiplicative Cipher

The multiplicative cipher multiplies each letter by a key value. The key must be coprime to 26 to ensure decryption is possible.

Encryption: $C = (P \times k) \mod 26$

Decryption: $P = (C \times k^{-1}) \mod 26$

Example: With key $k = 5$, plaintext "CAT" becomes "KTJ":

- C(2): $2 \times 5 = 10 \mod 26 = \text{K}$
- A(0): $0 \times 5 = 0 \mod 26 = \text{A}$
- T(19): $19 \times 5 = 95 \mod 26 = 17 = \text{R}$

3 Pigpen Cipher

The Pigpen cipher is a geometric substitution cipher that replaces letters with symbols based on grids and X-shapes. Each letter corresponds to the shape of its surrounding grid.

Example: The word "HELLO" is encoded using grid positions where each letter is replaced by the shape of its cell (with or without dots for the second grid).

4 Hill Cipher

The Hill cipher is a polygraphic substitution cipher based on linear algebra. It uses matrix multiplication to encrypt blocks of letters [web:6][web:10].

Encryption: $\mathbf{C} = \mathbf{KP} \mod 26$

Example: For a 2×2 key matrix $\mathbf{K} = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$, encrypt "HE":

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 33 \\ 34 \end{pmatrix} \mod 26 = \begin{pmatrix} 7 \\ 8 \end{pmatrix} \rightarrow \text{"HI"}$$

5 ADFGVX Cipher: Detailed Example

The ADFGVX cipher combines a 6×6 Polybius square (using the characters A, D, F, G, V, X as row/column labels) for substitution and a columnar transposition for additional scrambling. This example uses the plaintext "ATTACK".

Step 1: Construct the Polybius Square

Let the Polybius square be filled with the alphabet and digits 0–9, keyed by the word "CIPHER" followed by the rest (without repeating chars):

	A	D	F	G	V	X
A	C	I	P	H	E	R
D	A	B	D	F	G	J
F	K	L	M	N	O	Q
G	S	T	U	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

Each plaintext letter is encoded by the row and column header. For example, 'A' is at row D, column A.

Step 2: Substitute Each Letter

Substitute each letter of "ATTACK":

- A: Row D, Col A — DA
- T: Row G, Col D — GD
- T: Row G, Col D — GD
- A: Row D, Col A — DA
- C: Row A, Col A — AA
- K: Row F, Col A — FA

The fractionated message (substitution result):

$$DA\ GD\ GD\ DA\ AA\ FA$$

Step 3: Columnar Transposition

Write the message out under a keyword. Let the keyword be "LONG":

L O N G

Write the letters in rows:

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

Now, order columns alphabetically by the keyword: G, L, N, O.

- G: [D, A, A]

- L: [D, G, A]
- N: [G, D, F]
- O: [A, D, A]

Ciphertext is read column-by-column in the order G, L, N, O:

$$\text{G} : D, A, A;\ \text{L} : D, G, A;\ \text{N} : G, D, F;\ \text{O} : A, D, A$$

So the ciphertext is:

DAADGA GDF ADA

Grouped: "DAADGAGDFADA"

6 Playfair Cipher

The Playfair cipher encrypts digraphs (pairs of letters) using a 5×5 key matrix. It provides better security than monoalphabetic substitution by hiding single-letter frequencies [web:10][web:12].

Rules:

- Same row: shift right
- Same column: shift down
- Rectangle: swap columns

Example: Using key "MONARCHY", encrypt "HELLO":

- Prepare digraphs: HE LL O (add X) → HE LX LO
- Using the key matrix: HE → DM, LX → YR, LO → FS
- Ciphertext: "DMYRFS"

7 Rail Fence Cipher

The Rail Fence cipher is a transposition cipher that writes the plaintext in a zigzag pattern across multiple rails, then reads off each rail sequentially [web:16].

Example: Encrypt "HELLO WORLD" with 3 rails:

```
H . . . O . . . L .
. E . L . W . R . D
. . L . . . O . . .
```

Reading row by row: "HOLLEWRDLO"

8 Columnar Transposition Cipher

In the Columnar Transposition cipher, plaintext is written in rows, but the ciphertext is read column by column in an order determined by a keyword [web:6].

Example: Using keyword "KEY" (order: 2, 1, 3), encrypt "HELLO WORLD":

```
K E Y
2 1 3
------
H E L
L O W
O R L
D
```

Reading columns in order 1, 2, 3: “EORHLODLWL”

9 Vernam Cipher (One-Time Pad)

The Vernam cipher, also known as the one-time pad, is theoretically unbreakable if the key is truly random, as long as the message, used only once, and kept secret [web:12].

Encryption: $C = P \oplus K$ (XOR operation)

Decryption: $P = C \oplus K$

Example: Plaintext “HELLO” with random key “XMCKL”:

- H(7) $\oplus$ X(23) = 16 = Q
- E(4) $\oplus$ M(12) = 8 = I
- Result: “QIEMZ”

10 Vigenère Cipher

The Vigenère cipher is a polyalphabetic substitution cipher that uses a keyword to apply multiple Caesar shifts. It uses a repeating keyword to determine the shift for each letter [web:8][web:12][web:14].

Encryption: $C_i = (P_i + K_i) \mod 26$

Example: Using keyword “KEY”, encrypt “HELLO”:

- H + K(10) = R
- E + E(4) = I
- L + Y(24) = J
- L + K(10) = V
- O + E(4) = S
- Ciphertext: “RIJVS”