

بقانون واحد

Autokey Cipher

Caesar Cipher

One-Time Pad بدون تكرار

Vigenère Cipher تكرار الحرف

النص المشفر:

"EQNVZ"

المفتاح:

"XMCKL"

"HELLO"

"KEYKE"

Encryption

$$C = (P + K) \mod 26$$

Decryption

$$P = (C - K) \mod 26$$

Affine Cipher

Encryption

$$C = (P \cdot K_1 + K_2) \mod 26$$

Decryption

$$P = (C - K_2) \cdot K_1^{-1} \mod 26$$

Encryption Matrix Hill Cipher

$$C = K \cdot P \mod 26$$

$$C = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \mod 26$$

Multiplicative Cipher

Encryption

$$C = (P \cdot K) \mod 26$$

Decryption

$$P = (C \cdot K^{-1}) \mod 26$$