Multiplicative Cipher: Key = k P = Plaintext C = ciphertext

Encryption: $(P \times \underline{k}) \bmod 26 = C$

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

Can we take $k = 2$?

$\underline{\mathbb{Z}_{26}}$

$2 \times \underline{k^{-1}} = 1 \pmod{26}$

Ans: No.

k can be from the set $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

$\mathbb{Z}_{26}^{*} = \{x \in \mathbb{Z}_{26} \mid \gcd(x, 26) = 1\}$

Size of the key domain is 12.

→ Brute-Force attack is very easy to implement.

→ Statistical attacks can also be implemented.

Affine Cipher: Key = (k_1, k_2)

14 August 2020 12:21

Encryption: $(P \times k_1 + k_2) \bmod 26 = C$

Decryption: $(C - k_2) \times k_1^{-1} \bmod 26 = P$

k_1^{-1} = multiplicative inverse of k_1

$-k_2$ = Additive " " k_2.

Size of key domain is $= 12 \times 26 = \underline{312}$.

Ex: Plaintext : hello   Ciphertext : $\underline{ZEBBW}$

Key = (7, 2)

plaintext	Encryption	Ciphertext
h	$(7 \times 7 + 2) \bmod 26 = 25$	Z
e	$(4 \times 7 + 2) \bmod 26 = 4$	E
l	$(11 \times 7 + 2)$ " $= 1$	B
l	" $= 1$	B
o	$(14 \times 7 + 2)$ " $= 22$	W

$(C - k_2) \times \underline{k_1^{-1}} \bmod 26$

$k_1^{-1} = 7^{-1} \bmod 26$

$\gcd(26, 7) = \gcd(7, 5)$

14 August 2020 12:32

$$26 = 7 \times 3 + 5$$
$$7 = 5 \times 1 + 2$$
$$5 = 2 \times 2 + 1$$

$$1 = 5 - 2 \times 2$$
$$= 5 - 2 \times (7 - 5 \times 1)$$
$$= 5 - 2 \times 7 + 2 \times 5$$
$$= 3 \times 5 - 2 \times 7$$
$$= 3 \times (26 - 7 \times 3) - 2 \times 7$$
$$= 3 \times 26 - 9 \times 7 - 2 \times 7$$
$$1 = 3 \times 26 - 11 \times 7$$
$$7 \times (-11) = 1 - 3 \times 26$$
$$7 \times (-11) = 1 \mod 26$$

7×15

$= 105$

$$\begin{array}{r} 26 \\ 4 \\ \hline 104 \end{array}$$

1

$$7^{-1} = -11 \mod 26$$
$$= (26 - 11) \mod 26 = 15 \mod 26$$

14 August 2020 12:36

Substitution Cipher

key = $\begin{bmatrix} a & b & c & d & e & - - - \cdots \\ K & U & H & I & T & - - \cdots \end{bmatrix}$

Size of key domain : $\underline{26!} \approx 4 \times 10^{26}$

Brute-Force attack is diff. to implement.

statistical attack can be used.

Polyalphabetic Ciphers :

plaintext — p

Ciphertext — t, k, l, ⋮ } depending upon the position of p is plaintext.

Autokey Cipher.

14 August 2020 12:42

Alice Bob

Example: Autokey Cipher

plaintext $P = P_1 P_2 P_3 \cdots$

Ciphertext $C = C_1 C_2 C_3 \cdots$

Key $K = (k_1, \underset{=k_2}{P_1}, \underset{=k_3}{P_2}, \underset{=k_4}{P_3}, \cdots)$

Size of key domain $= 26$

Encryption: $C_i = (P_i + k_i) \bmod 26$

Decryption: $P_i = (C_i - k_i) \bmod 26$

Ex: $k_1 = 8$

$P = \text{rendezvous}$

plaintext	K	Encryption	Ciphertext
17	8	25	Z
4	17	21	V
13	4	17	R
3	13	16	Q
4	3	7	H
25	4	3	D
21	25	20	U
14	21	9	J
20	14	8	I
18	20	12	M

14 August 2020 12:49

Playfair Cipher: (Invented by Charles Wheatstone)
(Playfair Square)

K =

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

Keyword : CRYPTOGRAPHY

1. Enter the keyword in the matrix row-wise, left to right and top to bottom.
2. Drop the duplicate letters.
3. Fill the remaining spaces in the matrix with the rest of the English alphabets that were not a part of our keyword. Combine I & J in the same cell.

14 August 2020 12:56

Encryption! 1. Break the plaintext into groups of two alphabets.

2. If both alphabets are same (or only one is left), add x after the first alphabet.

3. If both alphabets are in the same row, replace them with the alphabets to immediate right

4. If both alph. are in the same column, replace them with the alphabets immediate below.

5 If the alphabets are not in the same row or column, replace them with alphabets in the same row respectively, but at the other pair of corners of the rectangle defined by the original pair.

Keyword: CRYPTOGRAPHY

K =

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

plaintext: meet me on the bridge.

me et me on th eb ri dg ex

Ciphertext: VM KR VM AL PB KG PE EO IV.

Size of key domain = $25!$

14 August 2020 13:13

Vignere Cipher: (Designed by Blaise de Vignere)

Initial Secret Key $(k_1, k_2, k_3, ---, k_m)$

plaintext $\bar{P} = P_1 P_2 P_3 ---$

Ciphertext $C = C_1 C_2 C_3 ---$

Key : $\underline{K} = [(k_1\ \underset{=k_{m+1}}{k_1}\ k_2\ k_3 ---, k_m)(\underset{=k_{m+1}}{k_1}\ \underset{=k_{m+2}}{k_2}\ k_3 ---, k_m)(\underset{=k_{2m+1}}{k_1} ---]$

Encryption : $C_i = (P_i + k_i) \bmod 26$

Decryption : $P_i = (C_i - k_i) \bmod 26$

14 August 2020 13:18

Hill Cipher: (Invented by Lester S. Hill in 1929)

1. plaintext is divided into equal size blocks.
2. key is a square matrix of size m where m is the size of the block.

$$k = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ \vdots & & & \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

plaintext $p = (P_1^1\, P_2^1\, P_3^1 \cdots P_m^1)(P_1^2\, P_2^2\, P_3^2 \cdots P_m^2) \cdots$

Ciphertext $C = (C_1^1\, C_2^1\, C_3^1 \cdots C_m^1)(C_1^2\, C_2^2\, C_3^2 \cdots C_m^2) \cdots$

Encryption: $C_B = P_B K \bmod 26$

$$\begin{bmatrix} C_1^i \\ C_2^i \\ \vdots \\ C_m^i \end{bmatrix}^T = [P_1^i\; P_2^i \cdots P_m^i] \begin{bmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & & \\ k_{m1} & \cdots & k_{mm} \end{bmatrix}$$

$$\begin{bmatrix} c_2 \\ \vdots \\ c_m \end{bmatrix} = \begin{bmatrix} r_1 & r_2 & \cdots & r_m \end{bmatrix} \begin{bmatrix} \vdots & & \\ k_{m1} & \cdots & k_{mm} \end{bmatrix}$$

14 August 2020 13:23

Decryption: $P = CK^{-1} \bmod 26$

$$\begin{bmatrix} p_1 \\ \vdots \\ p_m \end{bmatrix} = \begin{bmatrix} c_1 \\ \vdots \\ c_m \end{bmatrix} \begin{bmatrix} K^{-1} \end{bmatrix} \bmod 26$$

* K should be such that K^{-1} exits.
* Brute-Force is very difficult to apply.
* It do not preserve the statistics of the plaintext.

14 August 2020 13:28

One-Time Pad:

Shannon show that the Perfect secrecy can be achieved if each plaintext letter is encrypted with a key randomly chosen from the key domain.

One time pad uses this idea.

But practically This is very difficult to implement.