# SUBSTITUTION

## ① Caesar cipher

↳ (K = 3)

$C = E(3, P)$

$C = (P+3) \bmod 26$

Cipher text

$P = D(3, C)$

$P = (C-3) \bmod 26$

Plain text (decrypted)

## General Caesar cipher

$C = E(K, P)$

$\Rightarrow C = (P+K) \bmod 26$

$P = D(K, C)$

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

E: encryption algorithm

D: decryption algorithm

K: secret key [shift]

P: plain text

C: cipher text

Transformation

| | 0 | 1 | 2 | 3 | |
|---|---|---|---|---|---|
| Plain text | A | B | C | D | ... |
| cipher text [K = 3] | D | E | F | G | ... |

Example :

P = PASSWORD

Shift = 3

Cipher text = (P+3) (A+3) (S+3) ...

∴ Answer = SDVVZRUG

## Monoalphabetic cipher

[I don't think that will be asked to solve these, but anyway]

① The most common letters in English (in decreasing order)

1) E 2) T 3) A 4) O 5) I 6) N

7) S 8) H 9) R .....

② More than half of the words end with E, T, D, S

③ Digraph : TH, HE, AN, IN, ER, ON ...

④ Double letters : SS, EE, TT, FF, LL, MM, OO ...

⑤ Trigraphs : THE, AND, THA, ENT

∴ Eg : Plain text = PPXMOPPOQPEPSZWSZOZQSOVZZ

Here, most frequent letter : 1) P
2) Z
3) S

Compare with the most frequent letters in English language

P ⇒ E

Z ⇒ T

S ⇒ A

∴ Step1 : Manage = EEXMOEEOQEEEA T WAT

UTUTQAOVTT

Trigraph + T

Most frequent trigraph THE, THA etc

Here Ans = THAT

And so on

(3) PLAYFAIR CIPHER

Encryption

Step 1: Construct 5 x 5 matrix.

[Create the key first [remove duplicates] - write each letter only once]

~~Plain text~~

Note: Include I/J as a single unit

{If I is written in key already, don't write J with other letters.}

(OR)

Exclude Q

Step 2: Plain text - make digraphs & make pairs

Eg: P = WORLD

∴ P = WO RL DX

If a letter is missing, add 'X'

Step 3: Rules

Rule 1: If 2 letters are repeating, separate them by adding 'X' in between them.

Eg: BALLOON

∴ P = BA LX LO ON [Two same letters should not be together]

Rule 2: If plain text letters are in the same row, replace each element with the element at its right; the last element follows circularly and goes to the first.

**Rule 3**: If plain text pair is in the same column, replace each with the element beneath it (below it). The last element circularly follows the first one.

**Rule 4**: If plain text letters are in different row and column, then replace each letter with:

a) Element in the same row as it is and column of the other element.

(OR)

b) Letter in its own column but row of the other letter.

---

Eg: P = WORLD
Key = SECURE

**Step 1**: Playfair matrix [5 × 5]

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

→ E occurs 2 times in secure write only once.

→ write remaining letters in order, exclude the ones already there.

→ I/J - write together

(61)

exclude Q

**Step 2**: P = WO RL DX

**Step 3**: Cipher text C = ?

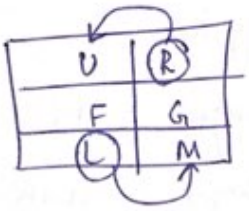
i) Consider WO

WO is in the same column as the matrix. [Apply rule 3]

∴ Replace W by E
Replace O by W ∴ WO = EW

ii) Consider RL

→ Apply rule 4




∴ RL = UM

iii) Consider DX - same column

→ Apply rule 3


∴ DX = KC

Answer:

∴ Cipher text = EW UM KC

Playfair Cipher

## Decryption

→ opposite of encryption.

→ Rules: right changes to left
below changes to above.

→ Finally remove 'X'

Eg: Ciphertext / Encrypted text = GATLMZCLRQTX

Key : MONARCHY

∴ Step 1: Playfair matrix

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

Step 2: Diagraphs : GA TL MZ CL RQ TX

(i) GA → different columns
Apply rule 4

∴ GA = I (or J) N

Let's consider I, if the word makes sense later

∴ GA = IN

(ii) TL : same row [Rule 2]

∴ TL = ST

} Decryption: so, left

(iii) MZ
Rule 4 ∴ MZ = RU

(iv) CL → same column (Rule 3)

CL = ME

(v) RQ → different row & column (Rule 4)

RQ = NT

(vi) TX → Rule 4

TX = SZ

Step 3 : Remove letter corresponding to 'X', ~~bec~~ if no sense is made with its presence.

∴ P = INSTRUMENTSZ

Remove 'Z' (corresponding to X)

∴ Plain text = INSTRUMENTS

④ **Hill cipher**

| A | B | C | D | ..... | Y | Z |
|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | | 24 | 25 |

Cipher text $C = KP \bmod 26$

For $(m=3)$ i.e.,

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26$$
$$C_3 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26$$

If key is a $k \times k$ matrix, plain text is arranged in $[k \times 1]$ matrices.

For example, If key = HILL

$$K = \begin{bmatrix} H & I \\ L & L \end{bmatrix} \rightarrow 2 \times 2$$

Plain text = SHORT EXAMPLE

∴ Plain text $P = \begin{bmatrix} S \\ H \end{bmatrix} \begin{bmatrix} O \\ R \end{bmatrix} \begin{bmatrix} T \\ E \end{bmatrix} \begin{bmatrix} X \\ A \end{bmatrix} \begin{bmatrix} M \\ P \end{bmatrix} \begin{bmatrix} L \\ E \end{bmatrix}$

$C = KP \bmod 26$

∴ P/I/7 /1

**Note:** 1) Add X if a letter is missing.

2) For 3×3 matrix, divide plain text into sets of 3 letters [3×1] matrices

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

| R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

$$\therefore \quad K = \begin{bmatrix} H & I \\ L & L \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

$$P = \begin{bmatrix} 18 \\ 7 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \end{bmatrix} \begin{bmatrix} 19 \\ 4 \end{bmatrix} \begin{bmatrix} 23 \\ 0 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix} \begin{bmatrix} 11 \\ 4 \end{bmatrix}$$

$$\boxed{C = KP \bmod 26}$$

$$\therefore \quad C_1 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 18 \\ 7 \end{bmatrix} \bmod 26$$

$$C_1 = \begin{bmatrix} 182 \\ 275 \end{bmatrix} \bmod 26$$

$$\therefore \quad C_1 = \begin{bmatrix} 0 \\ 15 \end{bmatrix}$$

$$\therefore \boxed{C_1 = \begin{bmatrix} A \\ P \end{bmatrix}}$$

1) 275 ÷ 26 = 10.5769

2) 10.5769 − 10 = 0.5769

3) 0.5769 × 26 = 15

$\therefore$ 275 % 26 = 15

Remove integer part of quotient and multiply what's left with 26.

Similarly,

$$C_2 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \end{bmatrix} \bmod 26$$

$$C_2 = \begin{bmatrix} 234 \\ 341 \end{bmatrix} \bmod 26$$

$$\boxed{C_2 = \begin{bmatrix} 0 \\ 3 \end{bmatrix} = \begin{bmatrix} A \\ D \end{bmatrix}}$$

$$C_3 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 19 \\ 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 9 \\ 19 \end{bmatrix}$$

$$= \begin{bmatrix} J \\ T \end{bmatrix}$$

$$C_4 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 23 \\ 0 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 5 \\ 19 \end{bmatrix}$$

$$= \begin{bmatrix} F \\ T \end{bmatrix}$$

$$C_5 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix} \text{ mod } 26$$

$$C_5 = \begin{bmatrix} 22 \\ 11 \end{bmatrix}$$

$$\boxed{C_5 = \begin{bmatrix} W \\ L \end{bmatrix}}$$

$$C_6 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 41 \\ 4 \end{bmatrix}$$

$$C_6 = \begin{bmatrix} 5 \\ 9 \end{bmatrix}$$

$$\boxed{C_6 = \begin{bmatrix} F \\ J \end{bmatrix}}$$

$$\therefore \boxed{\text{Cipher text} = APADJTFTWLFJ}$$

# HILL CIPHER

## Decryption

$P = K^{-1} C \bmod 26$

3×3 matrix

1) Find inverse
2) Substitute values for each alphabet, divide into groups of 3
3) Substitute in $P = K^{-1} C \bmod 26$

Adjoint of a 3×3 matrix

$$A = \begin{bmatrix} 1 & 2 & -2 \\ -1 & 3 & 0 \\ 0 & -2 & 1 \end{bmatrix}$$

$$A^{-1} = \frac{1}{|A|} \text{adj}(A)$$

$\therefore |A| = 1(3+0) - 2(-1) - 2(2)$

$|A| = 3 + 2 - 4$

$|A| = 1$

$|A| = 1 \neq 0$

$\therefore A^{-1}$ exists

Adj of A =

| | $C_1$ | $C_2$ | | | |
|---|---|---|---|---|---|
| | 1 | 2 | -2 | 1 | 2 |
| $R_1$ | -1 | 3 | 0 | -1 | 3 |
| $R_2$ | 0 | -2 | 1 | 0 | -2 |
| | 1 | 2 | -2 | 1 | 2 |
| | -1 | 3 | 0 | -1 | 3 |

Process column wise, write Row wise

Answer

$$\text{Adj}(A) = \begin{bmatrix} 3 & 2 & 6 \\ 1 & 1 & 2 \\ 2 & 2 & 5 \end{bmatrix}$$

$$A^{-1} = \frac{1}{1} \begin{bmatrix} 3 & 2 & 6 \\ 1 & 1 & 2 \\ 2 & 2 & 5 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 3 & 2 & 6 \\ 1 & 1 & 2 \\ 2 & 2 & 5 \end{bmatrix}$$

# 2x2 matrix - Hill cipher decryption

Question : C = FK MF IO

$$K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$$

$$P = K^{-1} C \bmod 26$$

$$K^{-1} = \frac{1}{|K|} Adj(K)$$

$|K| = 12 - 9 = 3$

$d$ = Determinant = 3

$d d^{-1} \equiv 1 \bmod 26$

$\therefore \frac{1}{|K|} = |K|^{-1} = d^{-1}$

$\therefore 3 \times d^{-1} \equiv 1 \bmod 26$

$3 \times d^{-1} = 1 \bmod 26$

$d^{-1} = 9$

$3 \times d^{-1} \bmod 26 = 1$

$\therefore 3(d^{-1}) \bmod 26 = 1$

$27 \bmod 26 = 1$

$\therefore d^{-1} = 9$

$\therefore |K|^{-1} = 9$

Eg: $5(d^{-1}) \equiv 1 \bmod 26$

$5(d^{-1}) \bmod 26 = 1$

$\therefore d \times 5 + 1 = d^{-1}$

$$Adj(K) = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$$

Add 26 to remove negative values

$$Adj(K) = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

$$\therefore K^{-1} = 9 \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} \bmod 26$$

$$K^{-1} = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

$\therefore$ Decypt

$$P_1 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} F \\ K \end{bmatrix} \bmod 26$$

$$P_1 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \bmod 26$$

$$P_1 = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$$

$$P_1 = \begin{bmatrix} A \\ T \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} M \\ F \end{bmatrix} \text{ mod } 26$$

$$P_2 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \text{ mod } 26$$

$$P_2 = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} T \\ A \end{bmatrix}$$

Similarly,

$$P_3 = \begin{bmatrix} C \\ K \end{bmatrix}$$

∴ Plain text = ATTACK

## Polyalphabetic ciphers

→ Using different monoalphabetic substitutions as we proceed with the plain text.

i) A set of related monoalphabetic substitution is used.

ii) A key determines which particular rule is used for a given transformation.

### Vigenere cipher

→ A set of monoalphabetic substitutions consists of 26 Caesar ciphers with shifts of 0 through 25.

Encryption : $C_i = (P_i + k_{i \bmod m}) \bmod 26$

Decryption : $P_i = (C_i - k_{i \bmod m}) \bmod 26$

→ Advantage : Frequency information is obscured.

Key : deceptive

Plaintext : we are discovered save yourself

Repeat key such that the no. of key & plaintext becomes equal.

Plain text : WE ARE DISCOVERED SAVE YOURSELF

∴ Key = DECEPTIVEDECEPTIVEDECEPTIVE

Answer : cipher text = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

| | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key : | 3 | 4 | 2 | 4 | 15 | 19 | 8 | 21 | 4 | 3 | 4 | 2 | 4 | 15 | 19 | 8 | 21 | 4 | | | | |
| Plain text : | 22 | 4 | 0 | 17 | 4 | 3 | 8 | 18 | 2 | 14 | 21 | 4 | 17 | 4 | 3 | 18 | 0 | 21 | | | | |
| Cipher text : | 25 | 8 | 2 | 21 | 19 | 22 | 16 | 13 | 6 | 17 | 25 | 6 | 21 | 19 | 22 | 0 | 21 | 25 | | | | |
| | Z | I | C | V | T | W | Q | N | G | R | Z | G | V | T | W | A | V | Z | | | | |

$(P+K) \bmod 26$

| | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K: | 3 | 4 | 2 | 4 | 15 | 19 | 8 | 21 | 4 | 3 | 4 | 2 | 4 | 15 | 19 | 8 | 21 | 4 | | | | |
| P: | 4 | 24 | 14 | 20 | 17 | 18 | 4 | 11 | 5 | 22 | 4 | 0 | 17 | 4 | 3 | 8 | 18 | 2 | | | | |
| C: | 7 | 2 | 16 | 24 | 6 | 11 | 12 | 6 | 9 | 25 | 8 | 2 | 21 | 19 | 22 | 16 | 13 | 6 | | | | |
| | H | C | Q | Y | G | L | M | G | J | Z | I | C | V | T | W | Q | N | G | | | | |

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

## Vernam cipher

→ Key is as long as the plaintext but has no statistical relationship to it.

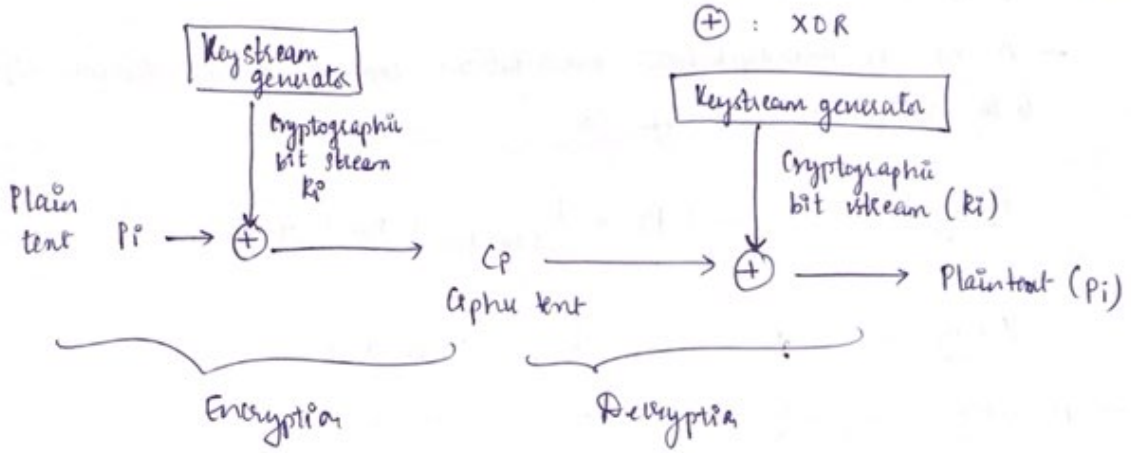
$$C_i = P_i \oplus k_i$$

$P_i$ : $i^{th}$ binary digit of plaintext

$k_i$ = $i^{th}$ binary digit of key

$C_i$ = " " " " ciphertext

$\oplus$ : XOR




Vernam cipher.

$$P_i = C_i \oplus k_i$$

→ Disadvantage : Repeating key.

## One time pad

→ Improvement of Vernam cipher.

→ Using a random key to remove repetation. - Increases security.

→ Unbreakable.

→ New key (equal to message length) for every new message.

→ Perfect secrecy.

Disadvantage

1) Problem of making large quantities of random keys.

2) " " key distribution & protection.

Example 1)

**Encryption**

P = H E L L O

7 4 11 11 14

Key = D G H B C

3 6 7 1 2

Add

10 10 18 12 16

Cipher text = 10 10 18 12 16

K K S M Q

If addition gives a number < 26, don't change

Else, subtract 26 from it.

Example 2) Plain text = RAMS WARUPK

Key = RAN CHO BABA

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ∴ Plain text (P) = | 17 | 0 | 12 | 18 | 22 | 0 | 18 | 20 | 15 | 10 |
| Key (K) | 17 | 0 | 13 | 2 | 7 | 14 | 1 | 0 | 1 | 0 |
| P+K | 34 | 0 | 25 | 20 | 29 | 14 | 19 | 20 | 16 | 10 |
| | 8 | 0 | 25 | 20 | 3 | 14 | 19 | 20 | 16 | 10 |

34-26

29-26

∴ Cipher text : IAZUDOTUQK

## One-time pad decryption

Cipher : IAZUDOTUQK (same key)

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ∴ Cipher (c) | - | 8 | 0 | 25 | 20 | 3 | 14 | 18 | 20 | 16 | 10 |
| Key (k) | - | 17 | 0 | 13 | 2 | 7 | 14 | 1 | 0 | 1 | 0 |
| Subtract c-k | : | -9 | 0 | 12 | 18 | -4 | 0 | 17 | 20 | 15 | 10 |
| If c-k<0, add 26 Else, same | | 17 | 0 | 12 | 18 | 22 | 0 | 17 | 20 | 15 | 10 |

Plain text : RAMSWARUPK