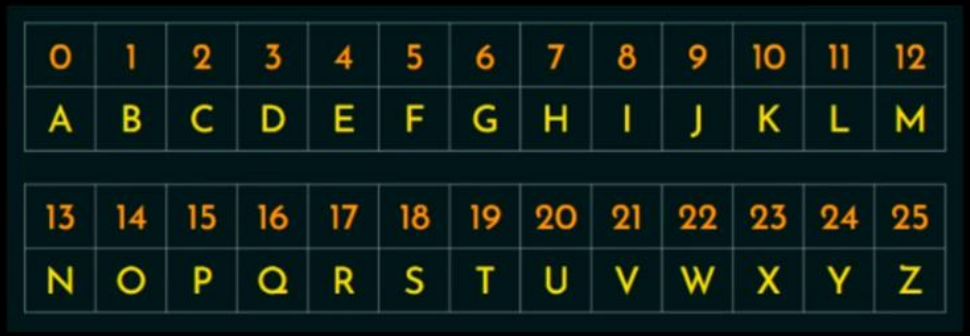
Plaintext = haroon

Key = 3

Ciphertext = (Plaintext + 3) mod 26

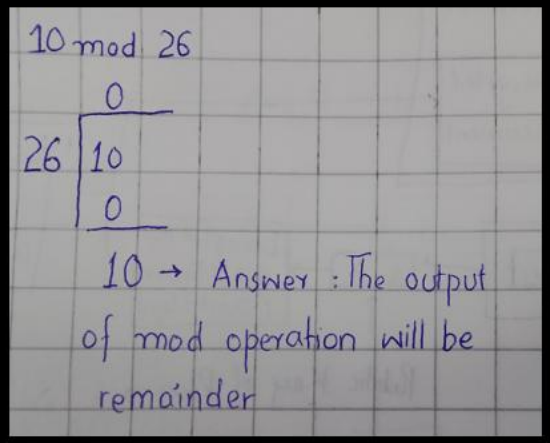
Encryption Algorithm :

C = (P + 3) mod26




| **Plaintext** | **h** | **a** | **r** | **o** | **o** | **n** |
|---|---|---|---|---|---|---|
| Value of letters | 7 | 0 | 17 | 14 | 14 | 13 |
| P + 3 | 10 | 3 | 20 | 17 | 17 | 16 |
| (P + k) mod26 | 10 | 3 | 20 | 17 | 17 | 16 |
| Ciphertext | K | D | U | R | R | Q |

The encrypted form of “haroon” using ceasar cipher is “KDURRQ”.




Any number less than 26, its mod26 is always that number.

QUESTION 2:

Decrypt "QHWZRUN VHFXULWB" using caesar cipher.

SOLUTION:

Ciphertext = QHWZRUN VHFXULWB

Key = 3

Decryption Algorithm:

P = (C - k) mod 26

| **Ciphertext** | **Q** | **H** | **W** | **Z** | **R** | **U** | **N** | **V** | **H** | **F** | **X** | **U** | **L** | **W** | **B** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Value of C | 16 | 7 | 22 | 25 | 17 | 20 | 13 | 21 | 7 | 5 | 23 | 20 | 11 | 22 | 1 |
| (C - 3) | 13 | 4 | 19 | 22 | 14 | 17 | 10 | 18 | 4 | 2 | 20 | 17 | 8 | 19 | -2 |
| (C - 3) mod26 | 13 | 4 | 19 | 22 | 14 | 17 | 10 | 18 | 4 | 2 | 20 | 17 | 8 | 19 | 24 |
| Plaintext | n | e | t | w | o | r | k | s | e | c | u | r | i | t | y |

>> (-2) mod 26 = 26 - 2 = 24.

The decrypted form of "QHWZRUN VHFXULWB" using ceasar cipher is "network security".

II. MULTIPLICATIVE CIPHER:

In multiplictive cipher we have the following plain, cipher and key domian:

$$P = \{0, 1, 2, \ldots 25\} = Z_{26}$$

$$C = \{0, 1, 2, \ldots 25\} = Z_{26}$$

$$k = Z_{26}{}^{*}$$

$$= \{0 < a < 26 \mid \gcd(a, 26) = 1\}$$

$$= \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

## ENCRYPTION AND DECRYPTION OF MULTIPLICATIVE CIPHER:

In encryption, we multiply plain text with key.

In decryption, we multiply cipher text with the multiplicative inverse of the key.

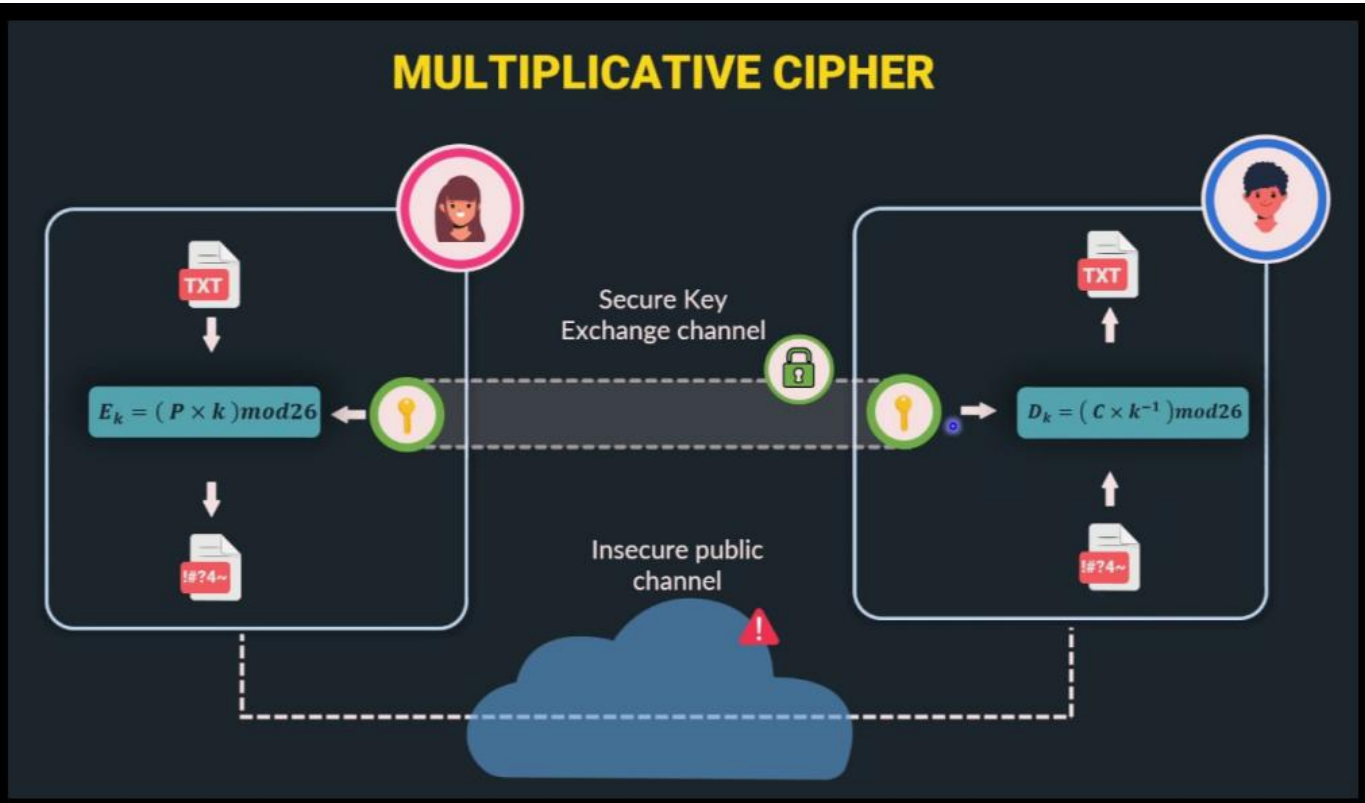
**Encryption**

$$E_k = (P \times k) mod 26$$

**Decryption**

$$D_k = (C \times k^{-1}) mod 26$$

## DIAGRAMMATIC REPRESENTATION OF MULTIPLICATIVE CIPHER:


MULTIPLICATIVE CIPHER
TXT
$E_k = (P \times k) mod 26$
!#?4~
Secure Key
Exchange channel
Insecure public
channel
TXT
$D_k = (C \times k^{-1}) mod 26$
!#?4~

QUESTION:

$Q$. Encrypt the message "*hello*" using multiplicative cipher with $key = 5$ and again retrieve the plaintext from the ciphertext

Plaintext: P = *hello*

Key: k = 5

Encryption algorithm:

$$C = (P \times k) \bmod 26$$

| $P$ | $h$ | $e$ | $l$ | $l$ | $o$ |
|---|---|---|---|---|---|
| *Value of P* | 7 | 4 | 11 | 11 | 14 |
| $P \times k$ | 35 | 20 | 55 | 55 | 70 |
| $P \times k \bmod 26$ | 9 | 20 | 3 | 3 | 18 |
| $C$ | $J$ | $U$ | $D$ | $D$ | $S$ |

$$C = JUDDS$$

| | | | | | |
|---|---|---|---|---|---|
| A | 0 | | N | 13 | |
| B | 1 | | O | 14 | |
| C | 2 | | P | 15 | |
| D | 3 | | Q | 16 | |
| E | 4 | | R | 17 | |
| F | 5 | | S | 18 | |
| G | 6 | | T | 19 | |
| H | 7 | | U | 20 | |
| I | 8 | | V | 21 | |
| J | 9 | | W | 22 | |
| K | 10 | | X | 23 | |
| L | 11 | | Y | 24 | |
| M | 12 | | Z | 25 | |

As the key is 5, so now we are going to find the multiplicative inverse of 5 mod 26

| Q | A | B | R | T1 | T2 | T |
|---|---|---|---|---|---|---|
| 5 | 26 | 5 | 1 | 0 | 1 | -5 |
| 5 | 5 | 1 | 0 | 1 | -5 | 26 |
| X | 1 | 0 | X | -5 | 26 | X |

The multiplicative inverse is -5, So -5 mod 26 = 21

Now lets decrypt it,

Ciphertext: C = $JUDDS$

M.I. of key: $k^{-1} = 21$

Decryption algorithm:

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

| $C$ | $J$ | $U$ | $D$ | $D$ | $S$ |
|---|---|---|---|---|---|
| *Value of C* | 9 | 20 | 3 | 3 | 18 |
| $C \times k^{-1}$ | 189 | 420 | 63 | 63 | 378 |
| $C \times k^{-1} mod\ 26$ | 7 | 4 | 11 | 11 | 14 |
| $P$ | $h$ | $e$ | $l$ | $l$ | $o$ |

P = hello

| | | | |
|---|---|---|---|
| A | 0 | N | 13 |
| B | 1 | O | 14 |
| C | 2 | P | 15 |
| D | 3 | Q | 16 |
| E | 4 | R | 17 |
| F | 5 | S | 18 |
| G | 6 | T | 19 |
| H | 7 | U | 20 |
| I | 8 | V | 21 |
| J | 9 | W | 22 |
| K | 10 | X | 23 |
| L | 11 | Y | 24 |
| M | 12 | Z | 25 |

## III. AFFINE CIPHER:

It is the combination of additive and multiplicative cipher.

Here we use a pair of keys (k1, k2)

In affine cipher we have the following plain, cipher and keys domian:

$$P = \{0, 1, 2, \ldots 25\} = Z_{26}$$

$$C = \{0, 1, 2, \ldots 25\} = Z_{26}$$

$$k_1 = \{0 < a < 26 \mid \gcd(a, 26) = 1\} = Z_{26}^*$$

$$k_2 = \{0, 1, 2, \ldots 25\} = Z_{26}$$

ENCRYPTION AND DECRYPTION OF AFFINE CIPHER:

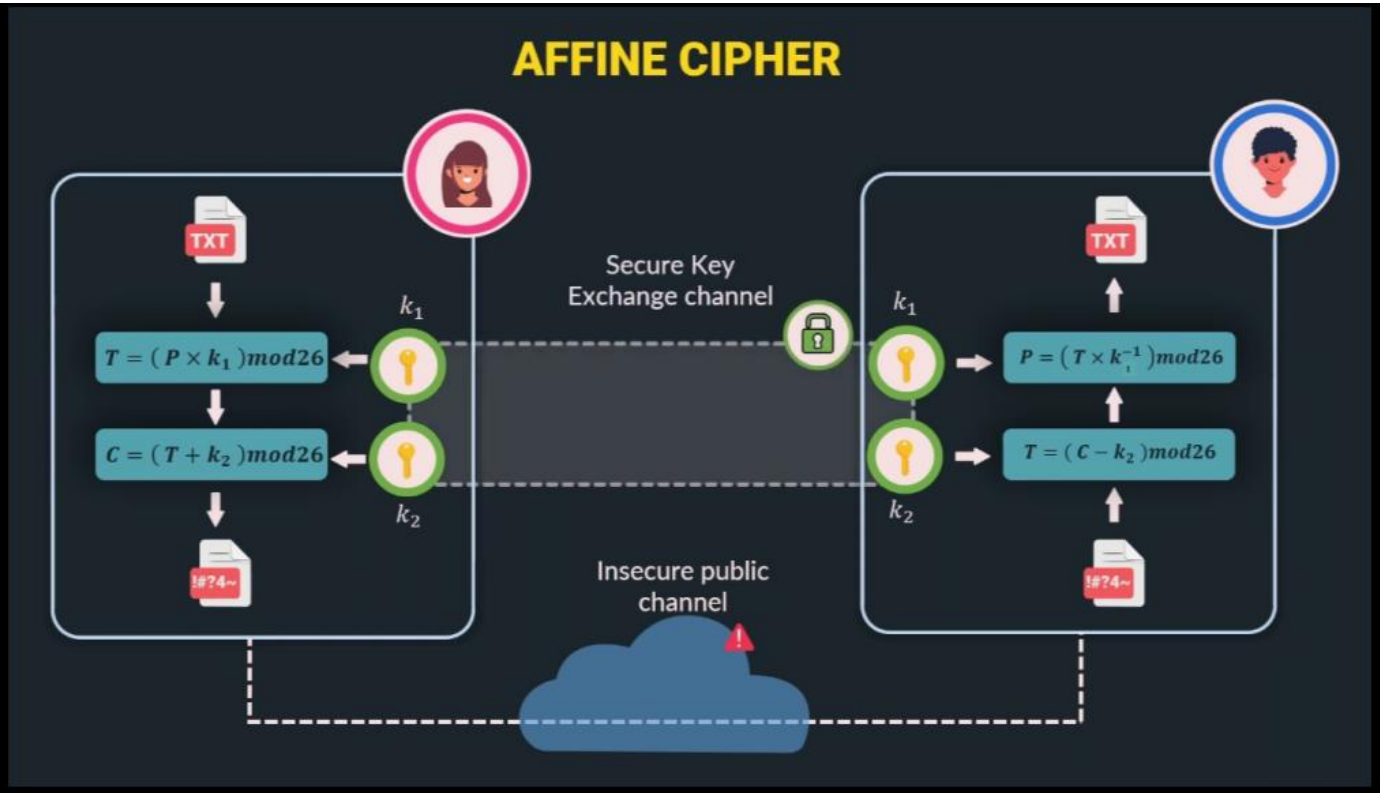
Encryption

$$E_k = (P \times k_1 + k_2) mod 26$$

Decryption

$$D_k = \left( (C - k_2) \times {k_1}^{-1} \right) mod 26$$

DIAGRAMMATIC REPRESENTATION OF AFFINE CIPHER:


AFFINE CIPHER
TXT
$k_1$
$T = (P \times k_1) mod 26$
$C = (T + k_2) mod 26$
$k_2$
!#?4~
Secure Key
Exchange channel
Insecure public
channel
$k_1$
$k_2$
$P = (T \times k_1^{-1}) mod 26$
$T = (C - k_2) mod 26$
TXT
!#?4~

QUESTION:

$Q$. Encrypt the message "*hello*" using affine cipher with *key pair*(7,2) and again retrieve the plaintext from the ciphertext

Plaintext: P = *hello*

Keys: $k_1 = 7$ $k_2 = 2$

Encryption algorithm:

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

| $P$ | $h$ | $e$ | $l$ | $l$ | $o$ |
|---|---|---|---|---|---|
| *Value of P* | 7 | 4 | 11 | 11 | 14 |
| $P \times k_1$ | 49 | 28 | 77 | 77 | 98 |
| $P \times k_1 + k_2$ | 51 | 30 | 79 | 79 | 100 |
| $(P \times k_1 + k_2) \bmod 26$ | 25 | 4 | 1 | 1 | 22 |
| $C$ | $Z$ | $E$ | $B$ | $B$ | $W$ |

$$C = ZEBBW$$

| | | | |
|---|---|---|---|
| A | 0 | N | 13 |
| B | 1 | O | 14 |
| C | 2 | P | 15 |
| D | 3 | Q | 16 |
| E | 4 | R | 17 |
| F | 5 | S | 18 |
| G | 6 | T | 19 |
| H | 7 | U | 20 |
| I | 8 | V | 21 |
| J | 9 | W | 22 |
| K | 10 | X | 23 |
| L | 11 | Y | 24 |
| M | 12 | Z | 25 |

The multiplicative inverse of k,

7 mod 26

| Q | A | R | R | T1 | T2 | T |
|---|---|---|---|---|---|---|
| 3 | 26 | 7 | 5 | 0 | 1 | -3 |
| 1 | 7 | 5 | 2 | 1 | -3 | 4 |
| 2 | 5 | 2 | 1 | -3 | 4 | -11 |
| 2 | 2 | 1 | 0 | 4 | -11 | 26 |
| X | 1 | 0 | X | -11 | 26 | X |

The multiplicative inverse of 7 mod 26 is -11 or 15.

Lets decrypt it now,

Ciphertext: C = $ZEBBW$

$k_1^{-1} = 15 \qquad k_2 = 2$

Decryption algorithm:

$$P = \left( (C - k_2) \times k_1^{-1} \right) mod 26$$

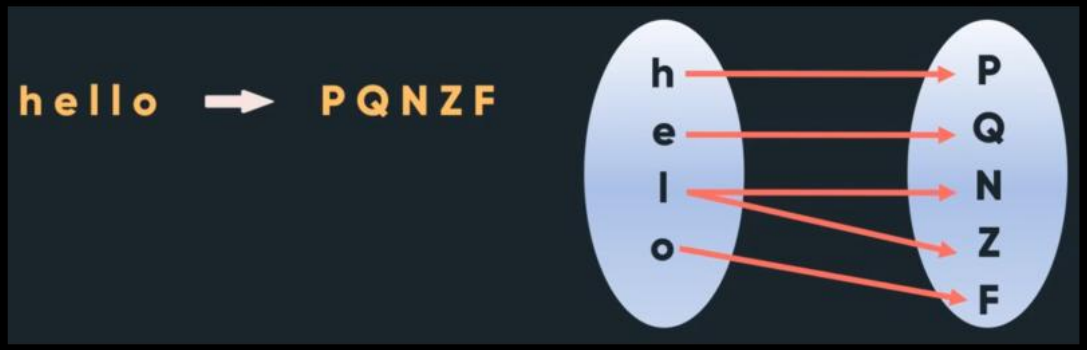
| $C$ | $Z$ | $E$ | $B$ | $B$ | $W$ |
|---|---|---|---|---|---|
| $Value\ of\ C$ | 25 | 4 | 1 | 1 | 22 |
| $C - k_2$ | 23 | 2 | $-1$ | $-1$ | 20 |
| $(C - k_2) \times k_1^{-1}$ | 345 | 30 | $-15$ | $-15$ | 300 |
| $(C - k_2) \times k_1^{-1}$ mod26 | 7 | 4 | 11 | 11 | 14 |
| $P$ | $h$ | $e$ | $l$ | $l$ | $o$ |

$P = hello$

| | | | |
|---|---|---|---|
| A | 0 | N | 13 |
| B | 1 | O | 14 |
| C | 2 | P | 15 |
| D | 3 | Q | 16 |
| E | 4 | R | 17 |
| F | 5 | S | 18 |
| G | 6 | T | 19 |
| H | 7 | U | 20 |
| I | 8 | V | 21 |
| J | 9 | W | 22 |
| K | 10 | X | 23 |
| L | 11 | Y | 24 |
| M | 12 | Z | 25 |

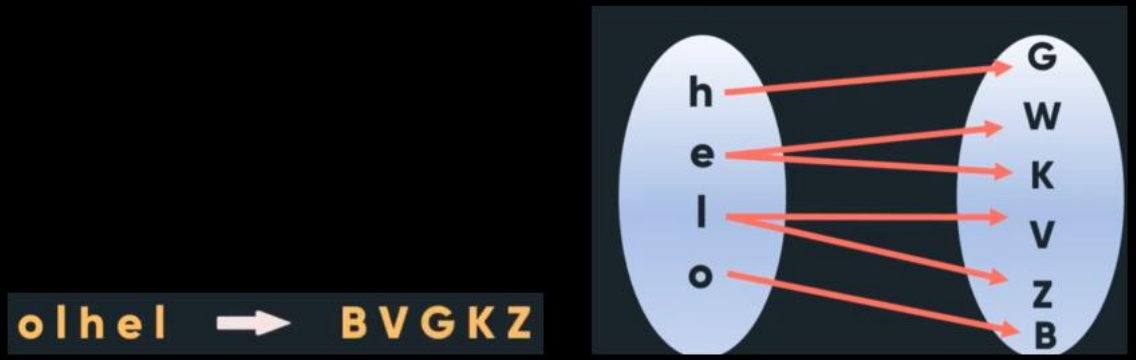
b. POLYALPHABETIC CIPHERS:

In polyalphabetic ciphers, each occurence of a character in the plain text may have different substitute in the cipher text and is dependent on its position in the plain text.




Relationship between character in the plain text to a character in the cipher text is one to many.

Now if the plain text is shuffled:




We can see that mapping is one to many like l is mapped to V and Z unlike monoalphabetic cipher in which l was mapped to O

everywhere. Similarly e can be mapped to W and if used second time then might be mapped to K and some other letter if used 3rd time in the plain text. That is the reason why we need polyalphabetic cipher that the frequency of the letters in the cipher text are changed so these cipher are not prone to statistical attacks.

## TYPES OF POLYALPHABETIC CIPHERS:

Polyalphbetic ciphers are of the following types,

### a. AUTOKEY CIPHER:

- In a polyalphabetic cipher we represent plain text, cipher text and key as a stream of characters rather than a single unit. So here we represent plain text as p1 p2 p3 where Pi is the ith character of the plain text. Here the domain of the plain text is Z26.
- Similar to the plain text we represent ciphertext as a stream of characters represented by c1 c2 c3 and so on where Ci is the ith character of the cipher text. Here also the domain of ciphertext is Z26.
- In the key first character is k1 and k1 is a secretly agreed predetermined value which is agreed by both alice and bob before encryption and decryption.
- So alice and bob fixes on a value k1 which is known to both of them so the key stream starts with this k1 value the next value is p1 that is the first character of the plain text followed by p2 which is the second character of the plain text p3 and so on.
- So we can see in the key stream we start with k1 which is secretly determined by both alice and bob and then we append the plain text to this k1 so the key stream is automatically generated once we know the value of k1 and the plain text.
- Since it is a combination of k1 followed by the plaintext characters thus giving it its name auto key cipher that is the key is automatically generated once the value of k1 and the plain text is known to us.
- Here also the domain of key is Z26.

$$P = p_1 p_2 p_3 \ldots \in Z_{26}$$

$$C = c_1 c_2 c_3 \ldots \in Z_{26}$$

$$k = k_1\ p_1\ p_2\ p_3 \ldots \in Z_{26}$$

$k_1$ is a secretly agreed predetermined value

The encryption algorithm of auto key cipher is Ci equal to Pi plus ki mod 26. So here we can see for generating the ith character of the cipher text we require the ith character of the plain text and the ith character of the key stream. So for generating c1 we do p1 plus k1 mod 26. Similarly for generating c2 we do p2 plus p1 mod 26 and so on. The decryption algorithm is Pi equal to Ci minus ki mod 26, similar to the encryption algorithm for generating the ith character of the plain text we require both the ith character of the cipher text and the ith character of the key stream. So for p1 to generate we require c1 minus k1 mod 26 and for p2 we do c2 minus p1 mod 26 and so on.

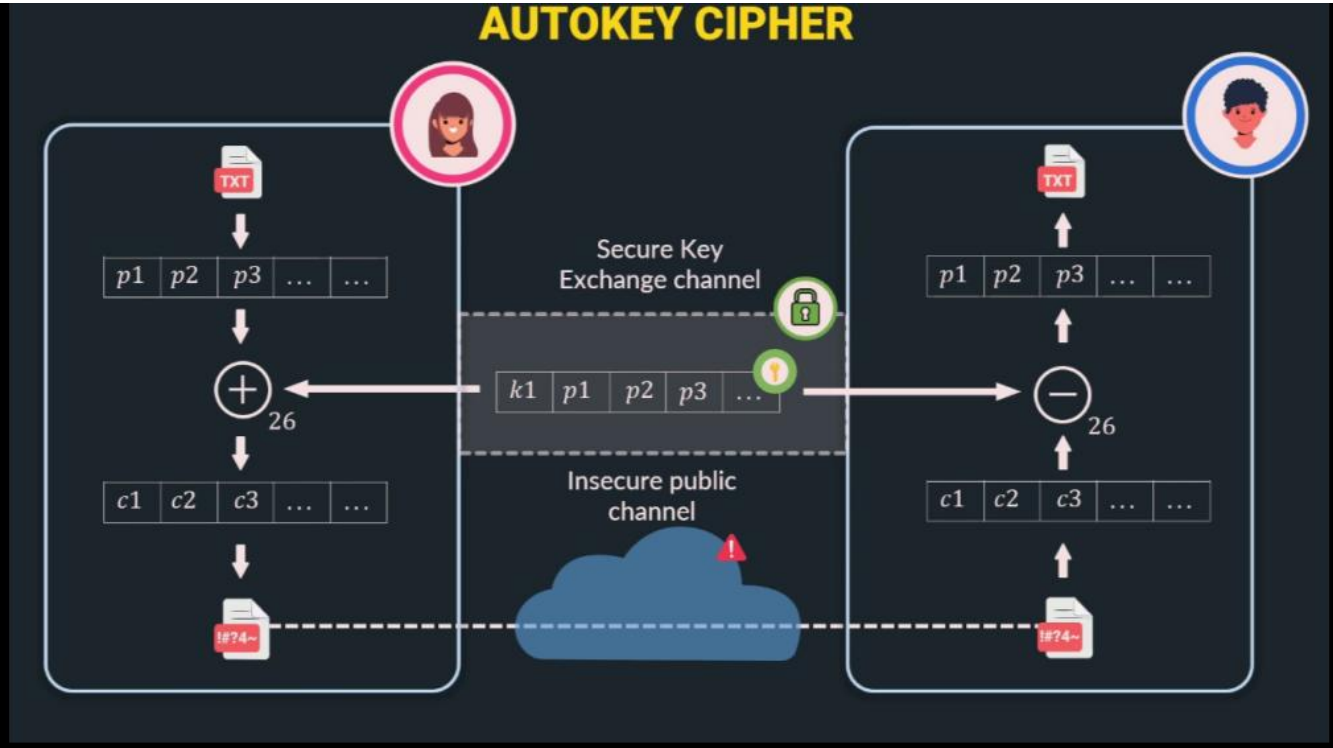
Encryption

$$C_i = (P_i + k_i)\ mod 26$$

Decryption

$$P_i = (C_i - k_i)\ mod 26$$

DIAGRAMATIC REPRESENTATION OF AUTOKEY CIPHER:




1. So alice takes a plain text and represents it as a stream of characters represented by p1 p2 p3 and so on, now for encrypting she will require the key stream so she will generate the key stream.
2. So the first character of the key stream is k1 which is predetermined by both alice and bob and shared between each other the next value of the key is p1 which is the first character of the plain text followed by p2 p3 and so on, so now we have the key stream.
3. Here now alice takes the plain text stream and the key stream and provides it to addition operation which is limited by mod 26 so your 26 represents that the output should be within Z26.
4. So what does the addition do it takes the first character of the plaintext that is p1 adds with the first character of the key that is

given and then applies the mod 26 operator so it is p1 plus k1 mod 26. Similarly for the second character that is p2 plus p1 mod 26 and so on.

5. In this way it generates the ciphertext stream which is represented by c1 c2 c3 and so on, where c1 is equal to p1 plus k1 mod 26 c2 is equal to p2 plus p1 mod 26 and same operation goes for all other characters.
6. This cipher text is sent to bob by an insecure public channel now bob has the cipher text, now for decrypting, bob represents the cipher text as a stream of characters represented by c1 c2 c3 and so on.
7. Now bob takes the ciphertext stream and the key stream and gives it to a negation operation which is limited by mod 26 operator which takes c1, it subtracts k1 and applies mod 26 that is c1 minus k1 mod 26, similarly c2 minus p1 mod 26 and so on.
8. In this way it generates a plain text stream which is represented by p1 p2 p3 and so on.
9. Here the key stream is shared using an secure key exchange channel.

## CRYPTANALYSIS OF AUTO KEY CIPHER:

Auto key cipher hides the single letter frequency statistics from the cipher text. For example, let's do the frequency analysis of the plain text and cipher text in the below example of the plain text text ecrypted with autokey cipher and k1 as 12.


- So here the frequency of the letter a is 2 t is also 2 c is 1 and k is 1. now let's do the same for the cipher text so here the frequency of letter M is 3 T is 2 and C is 1.
- So there is no relationship between the frequency of the characters of the plain text and the frequency of the characters in the cipher text which implies that it hides the frequency statistics from the ciphertext so it is not prone to a statistical attack.
- However the key k1 can take only 25 values that is from 1 to 25 since the domain of key is Z26 so your k1 can take only values from 1 to 25 that are only 25 values can be taken by k1 which is a small key domain and hence it is vulnerable to brute force attack.
- Hence it is in need of a cipher which has a larger key domain.

QUESTION:

Encryption,

$Q$. Encrypt the message "*attack*" using autokey cipher with $k1 = 12$ and again retrieve the plaintext from the ciphertext

P = *hello*

$k_1 = 12$

Encryption algorithm:

$$C_i = (P_i + k_i)\ mod 26$$

| $P_i$ | $a$ | $t$ | $t$ | $a$ | $c$ | $k$ |
|---|---|---|---|---|---|---|
| $Value\ of P_i$ | 0 | 19 | 19 | 0 | 2 | 10 |
| $K_i$ | 12 | 0 | 19 | 19 | 0 | 2 |
| $(P_i + k_i)\ mod 26$ | 12 | 19 | 12 | 19 | 2 | 12 |
| $C_i$ | $M$ | $T$ | $M$ | $T$ | $C$ | $M$ |

$$C = MTMTCM$$

| | | | |
|---|---|---|---|
| A | 0 | N | 13 |
| B | 1 | O | 14 |
| C | 2 | P | 15 |
| D | 3 | Q | 16 |
| E | 4 | R | 17 |
| F | 5 | S | 18 |
| G | 6 | T | 19 |
| H | 7 | U | 20 |
| I | 8 | V | 21 |
| J | 9 | W | 22 |
| K | 10 | X | 23 |
| L | 11 | Y | 24 |
| M | 12 | Z | 25 |

Decryption,

Ciphertext: C = $MTMTCM$

K = $(12, 0, 19, 19, 0, 2)$

Decryption algorithm:

$$P_i = (C_i - k_i)\ mod 26$$

| $C_i$ | $M$ | $T$ | $M$ | $T$ | $C$ | $M$ |
|---|---|---|---|---|---|---|
| $Value\ of\ C_i$ | 12 | 19 | 12 | 19 | 2 | 12 |
| $K_i$ | 12 | 0 | 19 | 19 | 0 | 2 |
| $(C_i - k_i)\ mod 26$ | 0 | 19 | 19 | 0 | 2 | 10 |
| $P_i$ | $a$ | $t$ | $t$ | $a$ | $c$ | $k$ |

$$P = attack$$

| | | | |
|---|---|---|---|
| A | 0 | N | 13 |
| B | 1 | O | 14 |
| C | 2 | P | 15 |
| D | 3 | Q | 16 |
| E | 4 | R | 17 |
| F | 5 | S | 18 |
| G | 6 | T | 19 |
| H | 7 | U | 20 |
| I | 8 | V | 21 |
| J | 9 | W | 22 |
| K | 10 | X | 23 |
| L | 11 | Y | 24 |
| M | 12 | Z | 25 |

b. VIGENERE CIPHER:

Here the keyword is the repitition of a secret keyword of length m where 1<=m<=26. The key stream can be created without knowing what is the plain text.

$$P = p_1 p_2 p_3 \ldots \in Z_{26}$$

$$C = c_1 c_2 c_3 \ldots \in Z_{26}$$

$$K = k_1\ k_2 \ldots k_m\ k_1 k_2 \ldots \in Z_{26}$$

*where,*

$k_i$ *is the* $i^{th}$ *character of a secretly agreed keyword*$(k)$*of length* $m$

## ENCRYPTION AND DECRYPTION OF VIGENERE CIPHER:

**Encryption**

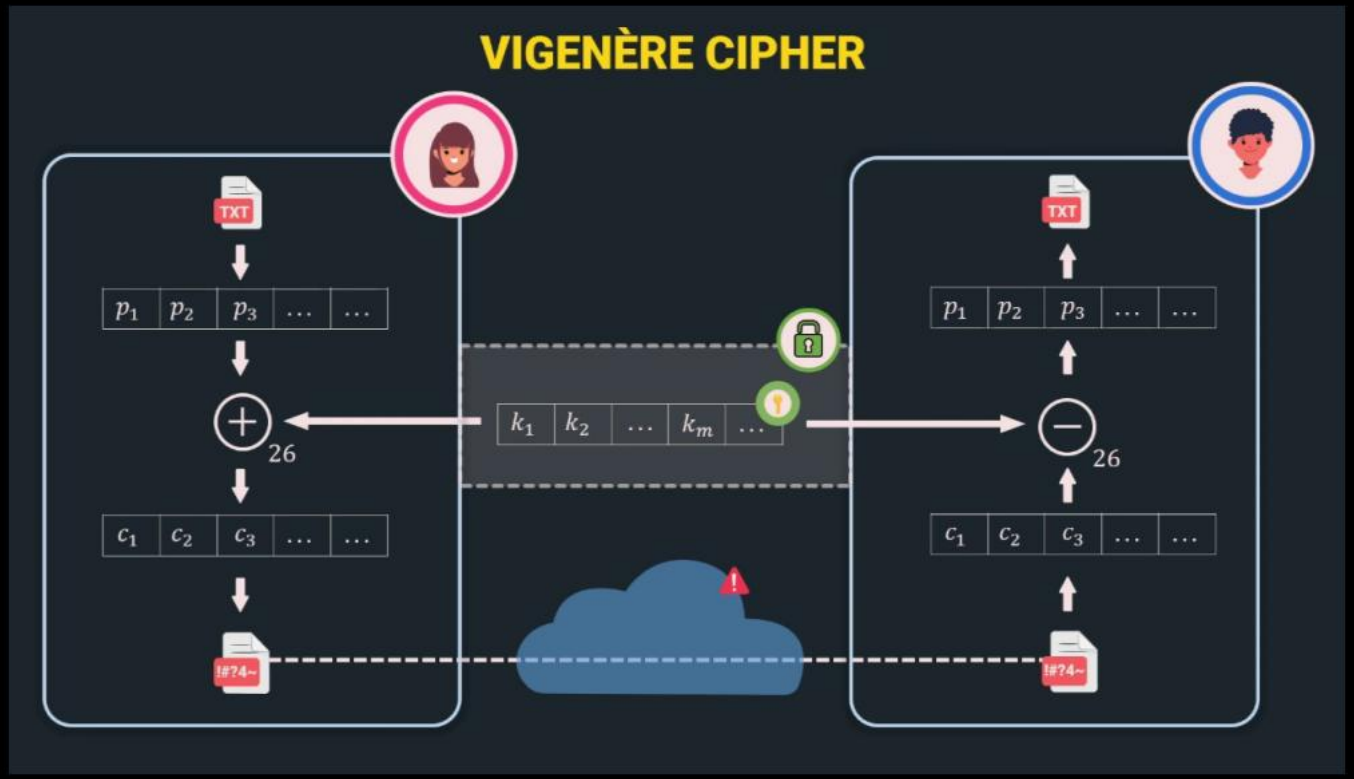
$$C_i = (P_i + k_i)\ mod 26$$

**Decryption**

$$P_i = (C_i - k_i)\ mod 26$$

Additive/Shift cipher is a special case of Vigenere cipher where m = 1.

## DIAGRAMMATIC REPRESENTATION OF VIGENERE CIPHER:


VIGENÈRE CIPHER
TXT
$p_1$ $p_2$ $p_3$ … …
26
$c_1$ $c_2$ $c_3$ … …
!#?4~
$k_1$ $k_2$ … $k_m$ …
TXT
$p_1$ $p_2$ $p_3$ … …
26
$c_1$ $c_2$ $c_3$ … …
!#?4~

QUESTION:

*Q*. Encrypt the message *"hello world"* using Vigenère cipher with *keyword* = *"cat"* and again retrieve the plaintext from the ciphertext

P = *hello world*

keyword = cat

Step 1: Generate initial key-stream

| c | a | t |
|---|---|---|
| 2 | 0 | 19 |

k = (2, 0, 19)

| | | | |
|---|---|---|---|
| A | 0 | N | 13 |
| B | 1 | O | 14 |
| C | 2 | P | 15 |
| D | 3 | Q | 16 |
| E | 4 | R | 17 |
| F | 5 | S | 18 |
| G | 6 | T | 19 |
| H | 7 | U | 20 |
| I | 8 | V | 21 |
| J | 9 | W | 22 |
| K | 10 | X | 23 |
| L | 11 | Y | 24 |
| M | 12 | Z | 25 |

Step 2: Encryption

P = *hello world*

k = (2, 0, 19)

Encryption algorithm:

$$C_i = (P_i + k_i)\ mod 26$$


| | | | |
|---|---|---|---|
| A | 0 | N | 13 |
| B | 1 | O | 14 |
| C | 2 | P | 15 |
| D | 3 | Q | 16 |
| E | 4 | R | 17 |
| F | 5 | S | 18 |

| $P_i$ | h | e | l | l | o | w | o | r | l | d |
|---|---|---|---|---|---|---|---|---|---|---|
| $P_i$'s values | 7 | 4 | 11 | 11 | 14 | 22 | 14 | 17 | 11 | 3 |
| $K_i$ | 2 | 0 | 19 | 2 | 0 | 19 | 2 | 0 | 19 | 2 |
| $(P_i + K_i)$ mod26 | 9 | 4 | 4 | 13 | 14 | 15 | 16 | 17 | 4 | 5 |
| $C_i$ | J | E | E | N | O | P | Q | R | E | F |

C = JEENOPQREF

| | | | |
|---|---|---|---|
| G | 6 | T | 19 |
| H | 7 | U | 20 |
| I | 8 | V | 21 |
| J | 9 | W | 22 |
| K | 10 | X | 23 |
| L | 11 | Y | 24 |
| M | 12 | Z | 25 |

C = JEENOPQREF

k = (2, 0, 19)

Decryption algorithm:

$$P_i = (C_i - k_i)\ mod 26$$

| $C_i$ | J | E | E | N | O | P | Q | R | E | F |
|---|---|---|---|---|---|---|---|---|---|---|
| $C_i$'s values | 9 | 4 | 4 | 13 | 14 | 15 | 16 | 17 | 4 | 5 |
| $K_i$ | 2 | 0 | 19 | 2 | 0 | 19 | 2 | 0 | 19 | 2 |
| $(C_i - K_i)$ mod26 | 7 | 4 | 11 | 11 | 14 | 22 | 14 | 17 | 11 | 3 |
| $P_i$ | h | e | l | l | o | w | o | r | l | d |

P = hello world

| | | | |
|---|---|---|---|
| B | 1 | O | 14 |
| C | 2 | P | 15 |
| D | 3 | Q | 16 |
| E | 4 | R | 17 |
| F | 5 | S | 18 |
| G | 6 | T | 19 |
| H | 7 | U | 20 |
| I | 8 | V | 21 |
| J | 9 | W | 22 |
| K | 10 | X | 23 |
| L | 11 | Y | 24 |
| M | 12 | Z | 25 |

CRYPTANALYSIS OF VIGENERE CIPHER:

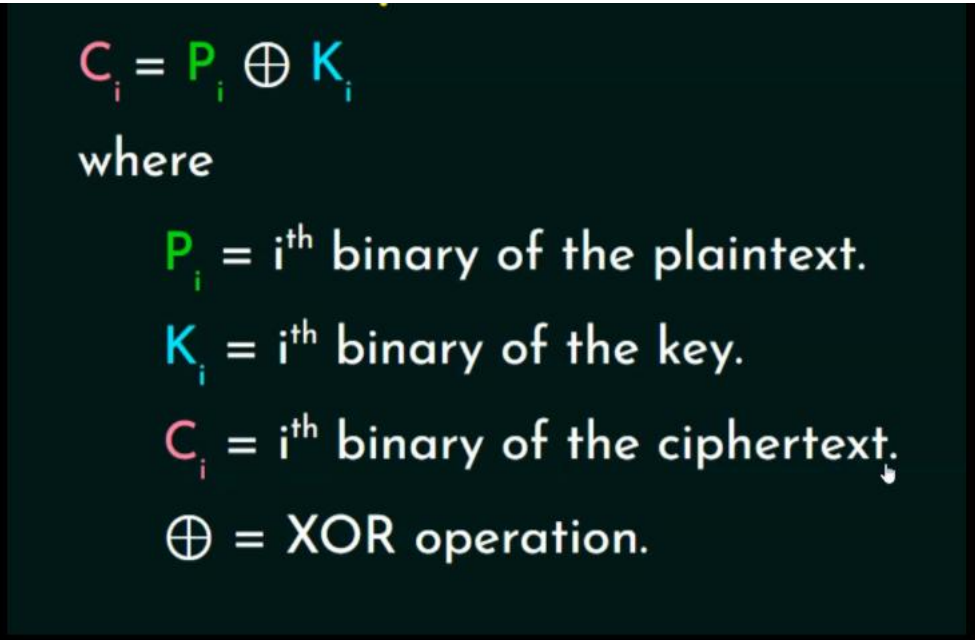
The whole ciphertext does not preserve the single letter frequency but dividing the ciphertext into pieces of length of the keyword can make the crytanalysis easier. We can perform it using kasiski test.

KASISKI TEST:

1. Cryptanalyst searches for repeated text segments of at least 3 characters.
2. Suppose (d1, d2, d3,...dn) represents the distances between the repeating segments.
3. Length of the keyword (m) = gcd (d1, d2, d3,...dn)
4. So the cryptanalyst divides the ciphertext into pieces of lenght (m)
5. Then cryptanalyst applies statistical attack to each piece till a sensible plain text is obtained.

c. VERNAM CIPHER:

- ☐ Vernam cipher was proposed by Gilbert Vernam in 1918.
- ☐ In vernam cipher domain of the plain text is 0 to 25, domian of the cipher text is also 0 to 25 and the key also.
- ☐ Here the key, plain text and cipher text are first converted to binary bits before performing some operations on it.
- ☐ Here the key is repeated untill the lenght of the key = length of the plain text.
- ☐ This cipher works on binary bits rather than letters.
- ☐ The initial vernam cipher proposed by gilbert vernam uses repeating keywords (key).
- ☐ The system worked with a very long but repeating keyword.
- ☐ This technique can be brocken with sufficient cipher text, the use of known or probable plain text sequences, or both because the keyword is repeating so it may reveal some statistical relationship.
- ☐ The system can be expressed as follows.



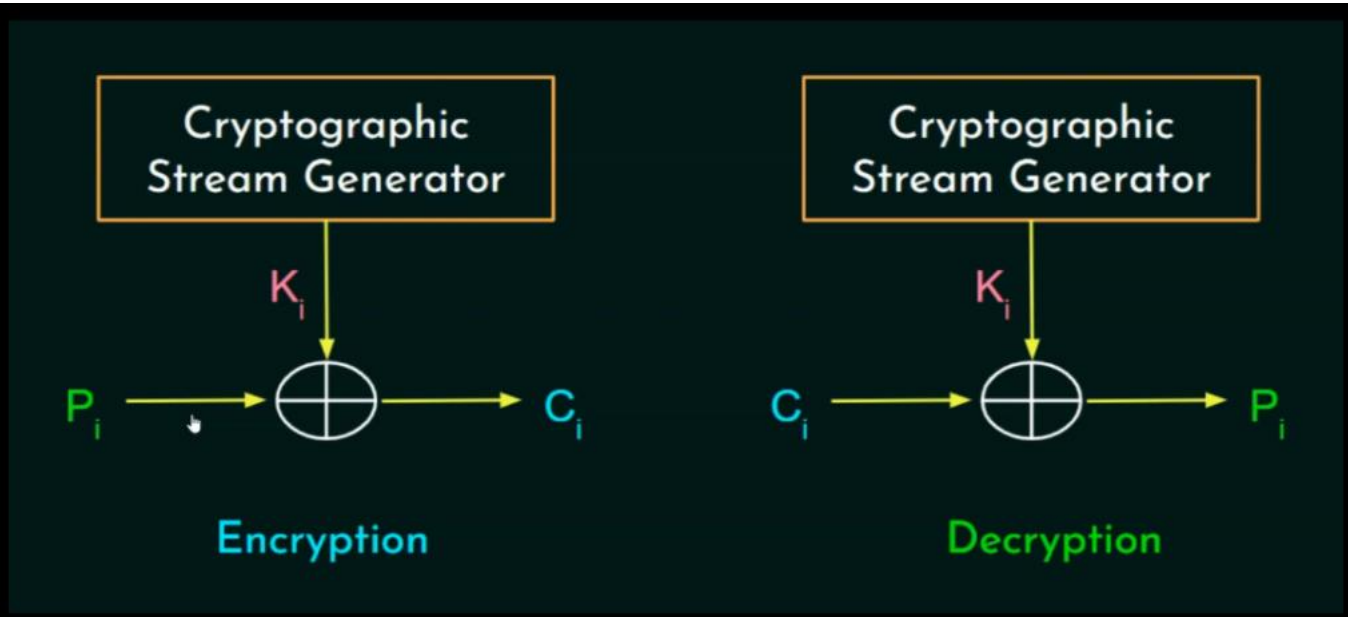

To get the plain text back,

Pi = Ci XOR Ki

XOR OPERATION:

Return true only if the input values are different.

ENCRYPTION AND DECRYPTION OF VERNAM CIPHER:


Cryptographic Stream Generator
$K_i$
$P_i$
$C_i$
Encryption
Cryptographic Stream Generator
$K_i$
$C_i$
$P_i$
Decryption

QUESTION:

Encrypt the plain text "hello world" with the key "cat" and decrypt the cipher text back using vernam cipher.

| **Plain Text** | **h** | **e** | **l** | **l** | **o** | **w** | **o** | **r** | **l** | **d** |
|---|---|---|---|---|---|---|---|---|---|---|
| Values of Plain Text(P) | 7 | 4 | 11 | 11 | 14 | 22 | 14 | 17 | 11 | 3 |
| Plain Text in Binary(Pi) | 00000111 | 00000100 | 00001011 | 00001011 | 00001110 | 00010110 | 00001110 | 00010001 | 00001011 | 00000011 |
| Key | c | a | t | c | a | t | c | a | t | c |
| Values of Key(K) | 2 | 0 | 19 | 2 | 0 | 19 | 2 | 0 | 19 | 2 |
| Key in Binary(Ki) | 00000010 | 00000000 | 00010011 | 00000010 | 00000000 | 00010011 | 00000010 | 00000000 | 00010011 | 00000010 |
| Pi XOR Ki | 00000101 | 00000100 | 00011000 | 00001001 | 00001110 | 00011111 | 00001100 | 00010001 | 00011000 | 00000001 |
| P XOR K | 5 | 4 | 24 | 9 | 14 | 31 | 12 | 17 | 24 | 1 |
| (P XOR K) mod26 | 5 | 4 | 24 | 9 | 14 | 5 | 12 | 17 | 24 | 1 |
| Cipher Text | F | E | Y | J | O | F | M | R | Y | B |

Cipher Text = FEYJO FMRYB

| **Cipher Text** | **F** | **E** | **Y** | **J** | **O** | **F** | **M** | **R** | **Y** | **B** |
|---|---|---|---|---|---|---|---|---|---|---|
| Values of Cipher Text(C) | 5 | 4 | 24 | 9 | 14 | 5 | 12 | 17 | 24 | 1 |
| Cipher Text in Binary(Ci) | 00000101 | 00000100 | 00011000 | 00001001 | 00001110 | 00000101 | 00001100 | 00010001 | 00011000 | 00000001 |
| Key | c | a | t | c | a | t | c | a | t | c |
| Values of Key (K) | 2 | 0 | 19 | 2 | 0 | 19 | 2 | 0 | 19 | 2 |
| Key in Binary(Ki) | 00000010 | 00000000 | 00010011 | 00000010 | 00000000 | 00010011 | 00000010 | 00000000 | 00010011 | 00000010 |
| Ci XOR Ki | 00000111 | 00000100 | 00001011 | 00001011 | 00001110 | 00010110 | 00001110 | 00010001 | 00001011 | 00000011 |
| C XOR K | 7 | 4 | 11 | 11 | 14 | 22 | 14 | 17 | 11 | 3 |
| (C XOR K) mod 26 | 7 | 4 | 11 | 11 | 14 | 22 | 14 | 17 | 11 | 3 |
| Plain Text | h | e | l | l | o | w | o | r | l | d |

Plain Text = hello world

d. ONE TIME PAD:

This is the improvement to the vernam cipher. The main difference between vernam cipher and one time pad is that vernam cipher uses repeating keyword while here the key is random in nature. So it results in the ultimate security. The random key is as long as the message so the key need not to be repeated. In addition to the randomness of the key, the key is used to encrypt

and decrypt a single message, and then it is discarded, and this is the reason we call it one time pad because the key is used one time only. So this cryptographic algorithm provide the ultimate security in the entire history of cryptographic algorithms. For each message a new key is required and the length of the key will be equal to the length of that plain text. This is unbreakable cipher. As a new key is used for every message, so the output is also random so there is no statistical relationship to the plain text because the cipher text contain no information whatsoever about the plain text, there is simply no way to break the code. And we can say that the security of one one-time pad is entirely due to randomness of the key.

## ENCRYPTION AND DECRYPTION OF ONE TIME PAD:

The encryption and decryption of one time pad is exactly the same as vernam cipher, just take a random key in place of "cat" which is repeated untill the key length equals the length of plain text, and here also take a random key and do the operation but keep the length of the random key and the plain text equal.

## TWO DIFFICULTIES WITH THIS CIPHER:

1. The practical problem of making large quantities of random keys.
2. Since it is a symmetric cipher so there is the problem of key distribution and protection.

Because of these difficulties, is of limited use and is primarily useful for low-bandwidth channels requiring very high security.

Since one time pad provide the highest level of security, we can say that one time pad offers perfect secrecy.

## PERFECT SECRECY:

A concept that, given an encrypted message (or ciphertext) from a perfectly secure encryption system (or cipher), absolutely

nothing will be revealed (exposed) about the unencrypted message (or plaintext) by the ciphertext.

The one time pad is the only cryptosystem that exhibits (shows) what is referred to as perfect secrecy.

e. HILL CIPHER:

It is a multi-letter cipher developed by lester hill in 1929. It encrypts a group of letters which can be diagraph, trigraph or polygraph.

There should be understanding of some topics before understanding the hill cipher which are:

- Matrix aritmetic modulo 26
- Square marix
- Determinant
- Multiplicative inverse

ENCRYPTION AND DECRYPTION OF HILL CIPHER:

**Encryption:**

$C = E(K,P) = P \times K \bmod 26$

**Decryption:**

$P = D(K,C) = C \times K^{-1} \bmod 26$

Decryption requires $K^{-1}$, the inverse matrix K.

QUESTION:

**Question:** Encrypt "pay more money" using Hill cipher with key

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

**Solution:**

| p | a | y | m | o | r | e | m | o | n | e | y |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 0 | 24 | 12 | 14 | 17 | 4 | 12 | 14 | 13 | 4 | 24 |

Key = 3 x 3 matrix.

PT = pay mor emo ney

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

Encryption

$$C_1 = (P_1K_{11} + P_2K_{21} + P_3K_{31}) \bmod 26$$
$$C_2 = (P_1K_{12} + P_2K_{22} + P_3K_{32}) \bmod 26$$
$$C_3 = (P_1K_{13} + P_2K_{23} + P_3K_{33}) \bmod 26$$

Encryption,

**Encrypting: pay**

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

$$(C_1\ C_2\ C_3) = (15\ 0\ 24)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (15x17+0x21+24x2 \quad 15x17+0x18+24x2 \quad 15x5+0x21+24x19) \bmod 26$$

$$= (303\ 303\ 531) \bmod 26$$

$$= (17\ 17\ 11)$$

$$= (R\ R\ L)$$

**Encrypting: mor**

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

$$(C_1\ C_2\ C_3) = (12\ 14\ 17)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (12x17+14x21+17x2 \quad 12x17+14x18+17x2 \quad 12x5+14x21+17x19) \bmod 26$$

$$= (532\ 490\ 677) \bmod 26$$

$$= (12\ 22\ 1)$$

$$= (M\ W\ B)$$

**Encrypting: emo**

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

$$(C_1\ C_2\ C_3) = (4\ 12\ 14)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (4x17+12x21+14x2 \quad 4x17+12x18+14x2 \quad 4x5+12x21+14x19) \bmod 26$$

$$= (348\ 312\ 538) \bmod 26$$

$$= (10\ 0\ 18)$$

$$= (K\ A\ S)$$

**Encrypting: ney**

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

$$(C_1\ C_2\ C_3) = (13\ 4\ 24)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (13x17+4x21+24x2 \quad 13x17+4x18+24x2 \quad 13x5+4x21+24x19) \bmod 26$$

$$= (348\ 312\ 538) \bmod 26$$

$$= (15\ 3\ 7)$$

$$= (P\ D\ H)$$

Plaintext : pay more money

Ciphertext : RRLMWBKASPDH

Decryption,

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

| R | R | L | M | W | B | K | A | S | P | D | H |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 17 | 17 | 11 | 12 | 22 | 1 | 10 | 0 | 18 | 15 | 3 | 7 |

## The Hill Algorithm

To find the determinant of K: $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

$$\text{Det} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$= 17(18\times19 - 2\times21) - 17(19\times21 - 2\times21) + 5(2\times21 - 2\times18) \bmod 26$

$= 17(342 - 42) - 17(399 - 42) + 5(42 - 36) \bmod 26$

$= 17(300) - 17(357) + 5(6) \bmod 26$

$= 5100 - 6069 + 30 \bmod 26$

$= -939 \bmod 26$

$= -3 \bmod 26$

$= 23$

$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adjoint } K$$

To find Adjoint K

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

$$\text{Adj } K = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$

$$\text{Adj } K = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$

$$\text{Adj } K = \begin{matrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 \end{matrix}$$

$$= \begin{matrix} 18 & 21 & 21 & 18 \\ 2 & 19 & 2 & 2 \\ 17 & 5 & 17 & 17 \\ 18 & 21 & 21 & 18 \end{matrix}$$

Performing the operation - Column wise

Entering the matrix - Row wise

$$= \begin{matrix} 18\times19-2\times21 & 2\times5-17\times19 & 17\times21-18\times5 \\ 21\times2-19\times21 & 19\times17-5\times2 & 5\times21-21\times17 \\ 21\times2-2\times18 & 2\times17-17\times2 & 17\times18-21\times17 \end{matrix}$$

$$= \begin{matrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{matrix} \bmod 26$$

$$= \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = \frac{1}{23} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = 17 \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = 17 \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$K^{-1} = \begin{pmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{pmatrix} \bmod 26$$

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

A matrix multiplied by its inverse matrix gives an identity matrix in the output. Lets verify the K^-1.

$$K \times K^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \quad K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

This is demonstrated as

$$\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix}\begin{pmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{pmatrix} = \begin{pmatrix}443 & 442 & 442\\ 858 & 495 & 780\\ 494 & 52 & 365\end{pmatrix} \bmod 26$$

$$= \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

**Decrypting:** RRL

$$(P_1\ P_2\ P_3) = (R\ R\ L)\begin{pmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{pmatrix} \bmod 26$$

Decryption

$$(C_1\ C_2\ C_3) = (17\ 17\ 14)\begin{pmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{pmatrix} \bmod 26$$

$$= (17x4+17x15+11x24 \quad 17x9+17x17+11x0 \quad 17x15+17x6+11x17) \bmod 26$$

$$= (587\ 442\ 544) \bmod 26$$

$$= (15\ 0\ 24)$$

$$= (P\ A\ Y)$$

**Decrypting:** MWB

$$(P_1\ P_2\ P_3) = (M\ W\ B)\begin{pmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (12\ 22\ 1)\begin{pmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{pmatrix} \bmod 26$$

$$= (12x4+22x15+1x24 \quad 12x9+22x17+1x0 \quad 12x15+22x6+1x17) \bmod 26$$

$$= (402\ 482\ 329) \bmod 26$$

$$= (12\ 14\ 17)$$

$$= (M\ O\ R)$$

**Decrypting: KAS**

$$(P_1\ P_2\ P_3) = (K\ A\ S) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (10\ 0\ 18) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (10x4+0x15+18x24 \quad 10x9+0x17+18x0 \quad 10x15+0x6+18x17) \bmod 26$$

$$= (472\ 90\ 456) \bmod 26$$

$$= (4\ 12\ 14)$$

$$= (E\ M\ O)$$

**Decrypting: PDH**

$$(P_1\ P_2\ P_3) = (P\ D\ H) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$(C_1\ C_2\ C_3) = (15\ 3\ 7) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (15x4+3x15+7x24 \quad 15x9+3x17+7x0 \quad 15x15+3x6+7x17) \bmod 26$$

$$= (273\ 186\ 362) \bmod 26$$

$$= (13\ 4\ 24)$$

$$= (N\ E\ Y)$$

Cipher Text : RRL MWB KAS PDH
Plain Text : PAY MOR EMO NEY = Pay more money

f. PLAYFAIR CIPHER:

A.k.a Playfair square or Wheatstone Playfair Cipher. It is a symmertric encryption technique.
It was inverted by British scientist Charles Whatstone.
It was named after his friend Baron Playfair who promoted its use.
It was used by british army in world war 1 and 2.

ENCRYPTION AND DECRYPTION OF PLAYFAIR CIPHER:

## ENCRYPTION AND DECRYPTION OF PLAYFAIR CIPHER:

In plaiyfair cipher, we follow the following steps:

| Step 1 | Step 2 | Step 3 |
| --- | --- | --- |
| Construction of 5x5 matrix (matrix using keyword) | Formation of digrams (digrams) | Encryption & decryption (matrix + digrams) |

## STEP 1:

★ 5 x 5 matrix constructed using a keyword (Ex: Monarchy)

| | | | | |
| --- | --- | --- | --- | --- |
| 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:

## Example

Plaintext: attack

Digrams: at ta ck

Plaintext: neso academy

Digrams: ne so ac ad em yx

Plaintext: balloon

Digrams: ba ll oo n

Digrams: ba lx lo on

STEP 3:

Same Column | ↓ | Wrap around.

Same row | → | Wrap around.

Rectangle | ⇆ | Swap

Making Diagrams,

$$message = KEYNOTE$$

$$\underline{KE}\ \underline{YN}\ \underline{OT}\ \underline{EX}$$

Encrypting and decrypting keynote using “MONARCHY”.

**Case 1:** When both letters in the pair are in the same row

| Encryption | Decryption |
| --- | --- |
| Replace with the letter on the right (with wrapping to start of the row) | Replace with the letter on the left (with wrapping to end of the row) |
| $KE \rightarrow EF$ | $EF \rightarrow KE$ |

**Case 2:** When both letters in the pair are in the same column

| Encryption | Decryption |
| --- | --- |
| Replace with the letter below (with wrapping to start of the column) | Replace with the letter above (with wrapping to end of the column) |
| $YN \rightarrow GY$ | $GY \rightarrow YN$ |

**Case 3:** When both letters are neither in same row nor in same column

| Encryption | Decryption |
| --- | --- |
| Replace with the intersection of: (ROW × COLUMN) | Replace with the intersection of: (ROW × COLUMN) |
| $OT \rightarrow RP$ | $RP \rightarrow OT$ |
| $EX \rightarrow IU$ | $IU \rightarrow EX$ |

QUESTION 1:

Encrypt mosque using the "MONARCHY" using playfair cipher.

SOLUTION:

Example 2: mosque

| mo | sq | ue |
|---|---|---|
| ON | TS | ML |

QUESTION 2:

Decrypt the cipher text "ODZFQSEZSONTSW" with keyword "Neso App" using playfair technique.

SOLUTION:

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

OD ZF QS EZ SO NT SW

YO UA RE AW ES OM EX

Cipher text = ODZFQSEZSONTSW

Plain text = You are awesome.

g. BOOK CIPHER/ RUNNING KEY CIPHER:

The book cipher, also known as the running key cipher, operates on the same basic principles as the one-time pad cipher. In onetime pad cipher, the key has the same length as the plaintext and is deleted after use. Every time a new key is used to send a new message.

The key or onetime pad is extracted from the book, which is an improvement over the onetime pad in Book Cipher.

BOOK:

In a book cipher, the "book" is a pre-agreed text that both the sender and receiver have access to. This book acts as the key for encryption and decryption. Here's how it works:

- **Selecting the Book**: Both parties choose a book that they both own or can access easily. The book could be a novel, a textbook, a poem collection, etc.

- **Using the Book**: To encrypt a message, the sender uses the text from the book as the key. For example, if they decide to start

from the 5th word on the 12th page, they use the letters of the book's text to shift the characters of the plaintext.

- **Decryption**: The receiver, who knows which book and the exact starting point, uses the same book text to decrypt the message.

The advantage is that the book provides a long, complex key, making it harder to crack, and both parties just need to keep the book secret instead of exchanging large keys.

ENCRYPTION AND DECRYPTION OF BOOK CIPHER:

- Step 1: Convert plaintext to numeric form: A=0, B=1, C=3, ...Z=25.

- Step 2: Take a one-time pad or key from any of the books and convert it to numeric format. But the key has to be the same length as the plain text.

- Step 3: Now add the numeric forms of plain text and key and apply the mod 26.

In decryption, subtract the key from ciphertext numeric forms. Actually, it is exactly same as autokey and vigenere cipher but niether it uses repeating keywords nor a key and part of the plain text. It is more like one-time pad but here it add and subtracts rather than XORing.

QUESTION:

Encrypt MeetTommorow with "ANENCRYPTION" as key with book cipher.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Numeric form Plian Text | M | E | E | T | T | O | M | O | R | R | O | W |
| | 12 | 4 | 4 | 19 | 19 | 14 | 12 | 14 | 17 | 17 | 14 | 22 |
| | A | N | E | N | C | R | Y | P | T | I | O | N |
| Numeric from Key Text | 0 | 13 | 4 | 13 | 2 | 17 | 24 | 15 | 19 | 8 | 14 | 13 |

Add the numeric form of Plain text and Key Text:

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 12 | 4 | 4 | 19 | 19 | 14 | 12 | 14 | 17 | 17 | 14 | 22 |
| + | 0 | 13 | 4 | 13 | 2 | 17 | 24 | 15 | 19 | 8 | 14 | 13 |
| | 12 | 17 | 8 | 32 | 21 | 31 | 36 | 29 | 36 | 25 | 28 | 35 |
| mod 26 = | 12 | 17 | 8 | 6 | 21 | 5 | 10 | 3 | 10 | 25 | 2 | 9 |

The cipher text obtained is MRIGVFKDKZCJ.

Perform the reverse for decryption that is subtract the key from the cipher text and apply mod 26.

2. TRANSPOSITION TECHNIQUE:

In this technique, some sort of permutation is applied on the plaintext letters. For example, if the plain text is HIGH, the possible permutations can be GIHH, HGHI and many more. The position of the letters is going to be changed in the cipher text but there will not be new letters. The types of transposition techniques are:

I. KEYLESS:

This algorithm uses something known as depth which function as a key but is not actually called key in the subject of cryptography and thats why this transposition cipher is called keyless transposition cipher. This cipher is called rail fence cipher.

a. RAIL FENCE CIPHER:

In this cipher, the plain text is writen down as a sequence of diagonals and then read off as a sequence of rows.
Here the depth value is also taken into account.

QUESTION 1:

Encrypt the "neso academy is the best" with depth 2 using rail fence cipher.

Plaintext : neso academy is the best.
Depth : 2

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| n | | s | | a | | a | | e | | y | | s | | h | | b | | s | |
| | e | | o | | c | | d | | m | | i | | t | | e | | e | | t |

Ciphertext : NSAAEYSHBSEOCDMITEET

We can see why it was given the term "Rail Fence" by looking at the image, which actually looks like a rail fence.
After writing the message as a series of diagonals, you must read it as a series of rows in order to extract the ciphertext.
Therefore, after reading the first row, the ciphertext's first half will be NEAAEYSHBS and according to the second row the second half of the cipher text will be EOCDMITEET.
Combining both gives NEAAEYSHBSEOCDMITEET as cipher text

QUESTION 2:

Encrypt the "Thank you so much" with depth 3 using rail fence cipher.

Plaintext : Thank you very much
Depth : 3

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T | | | | k | | | | v | | | | m | | | |
| | h | | n | | y | | u | | e | | y | | u | | h |
| | | a | | | | o | | | | r | | | | c | |

Ciphertext: TKVMHNYUEYUHAORE

II. KEYED:

These transposition techniques uses key to generate the cipher text These techniques are columnar and improved columnar. Columnar requires only key and rectangle dimensions while improved columnar requires key, rectangle dimensions and the number of rounds to generate the cipher text.

a. ROW COLUMN TECHNIQUE/COLUMNAR TRANSPOSITION:

This is a bit more complex transposition cipher than rail fence.
Here the sender and receiver first select a rectangle of their, which can 3x3 or 2x4 or 5x3 or whatever dimensions they want.

ENCRYPTION AND DECRYPTION OF ROW COLUMN CIPHER:

Create a rectangle.
Write the plain text row by row.
The cipher text is reading the plain text column by column.
The key decides which column should be read first.

Plaintext : "Kill Corona Virus at twelve am tomorrow"

| Key → | 4 | 3 | 1 | 2 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Plaintext (Input) → | K | i | l | l | c | o | r |
| | o | n | a | v | i | r | u |
| | s | a | t | t | w | e | l |
| | v | e | a | m | t | o | m |
| | o | r | r | o | w | y | z |

Ciphertext : LATARLVTMOINAERKOSVOCIWTWOREOYRULMZ

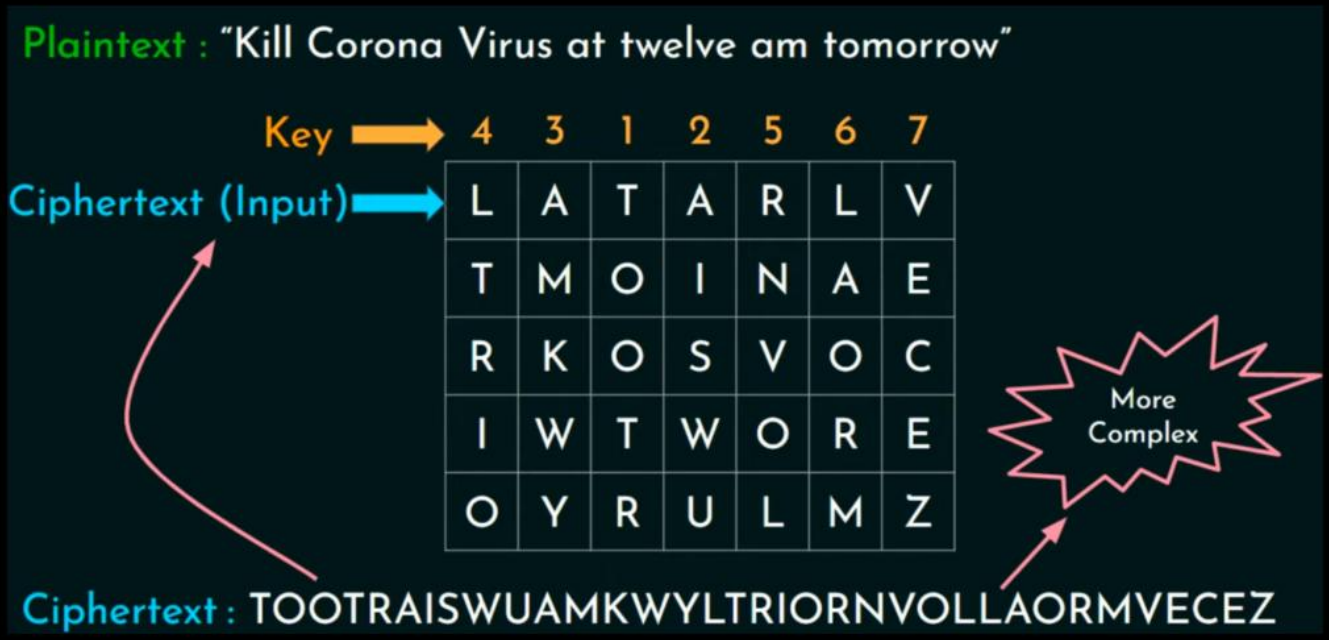
To decypt use the key

| **4** | **3** | **1** | **2** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|
| K | I | L | L | C | O | R |
| O | N | A | V | I | R | U |
| S | A | T | T | W | E | L |
| V | E | A | M | T | O | M |
| O | R | R | O | W | Y | Z |

Write column by column according to the key and read row by row.

b. COLUMNAR TRANSPOSITION WITH MULTIPLE ROUNDS/IMPROVED COLUMNAR TRANSPOSITION:

It is same as the simple columnar method but offers an improvement. This columnar method is applied to the plaintext more than once.




The rounds are also decided by the sender and receiver before the communication.