Unit-I
Introduction and Classical Ciphers

Security

- Security is “freedom from risk or danger”.
- The ability of a system to protect information and system resources with respect to confidentiality and integrity.

Levels of security:

- ***Computer Security:*** Computer security is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

- ***Information Security:*** Information security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or digital.

- ***Network Security:*** Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources.

Security Goals (CIA Traid)

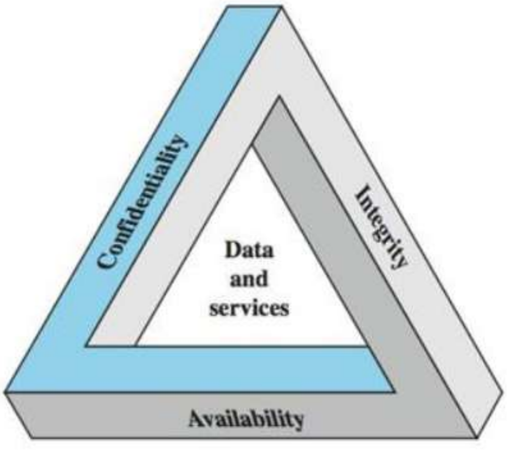


Fig: CIA Traid

- ***Confidentiality:*** It refers to the ability to hide the information from people who do not have the permission to access it. This helps to ensure that the data is not compromised and is not disclosed to unauthorized people. Some of the method employed to ensure confidentiality is encryption & cryptography. For example, credit card transactions over the internet. As a transaction is made the credit card number is encrypted by restricting access to the credit card number and user information.

- ***Integrity:*** It refers to the ability of protecting the data from modification or deletion by unauthorized people. Data integrity ensures that the data is the accurate and unmodified version of the original data.

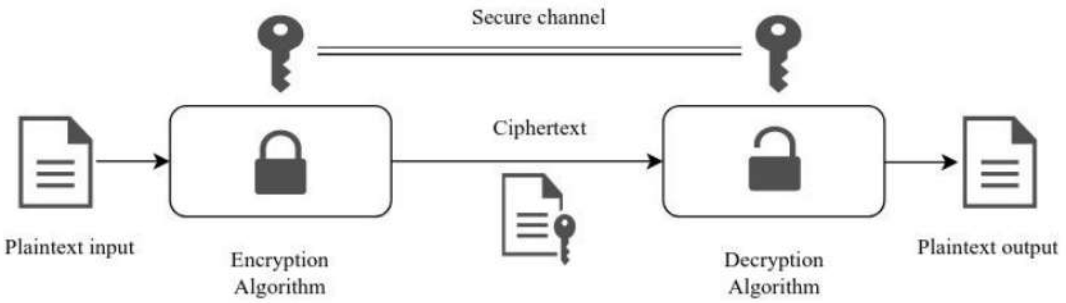
- ***Availability:*** Though it is highly necessary to ensure that the data is unavailable to unauthorized people, it is equally important to make sure that the data is available to authorized people. People who are authorized to access information must not face any issues when accessing information that is needed.

Cryptography

Cryptography is the science of keeping information secure by transforming it into form that unintended recipients cannot understand. It allows only the sender and intended recipient of a message to view its contents.

Terminologies:

- ***Plaintext:*** readable text with no information hidden.
- ***Ciphertext:*** text with information hidden (the encrypted data).
- ***Encryption:*** the process of converting plaintext to ciphertext.
- ***Decryption:*** the process of reverting ciphertext to plaintext.
- ***Cipher:*** algorithm used for encryption and decryption.
- ***Key:*** a secret piece of information which is used for encryption & decryption.



Cryptosystem

- The combination of algorithm, key and key management function used to perform cryptographic operations.
- It is a 5-tuple representation (E, D, M, K, C) where,

E – set of encryption algorithm

D – set of decryption algorithm

M – set of plain text

K – set of keys

C – set of ciphertext

Cryptanalysis

- Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems.
- Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

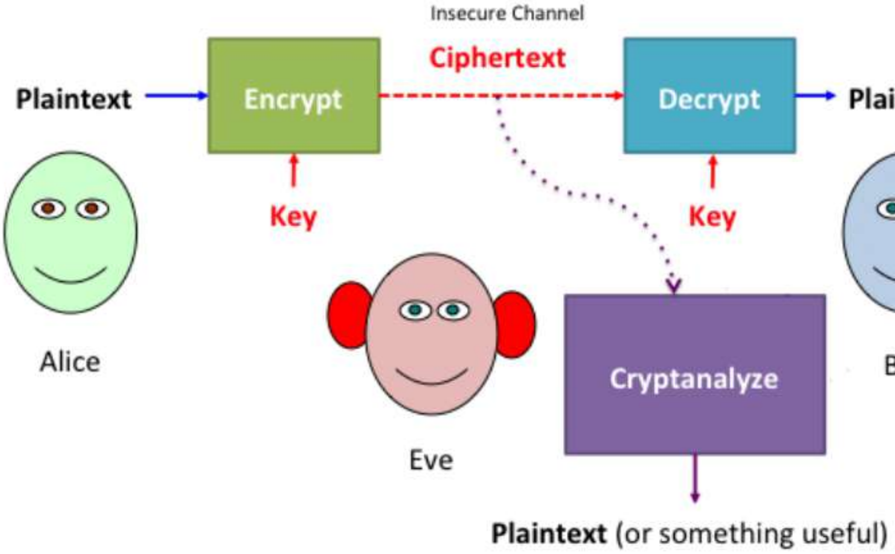


Fig: Cryptanalysis

Security Threats

Threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or even that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Classes of threats:

- ***Disclosure:*** unauthorized access to information.
  - Snooping
- ***Deception:*** acceptance of false data.
  - Modification, spoofing, repudiation of origin, denial of receipt
- ***Disruption:*** interruption/prevention of correct operation.
  - Modification
- ***Usurpation:*** unauthorized control of a system component.
  - Modification, spoofing, delay, denial of service

Security Attack

An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.

Attacks are typically categorized based on the action performed by the attacker. An attack, thus, can be ***passive*** or ***active***.

Passive Attack

- A passive attack make use of information from the system but doesn't affect the system resources.
- The goal of attacker is to obtain the information that is being transmitted.
- Passive attacks are difficult to detect because they do not involve any alteration of data.

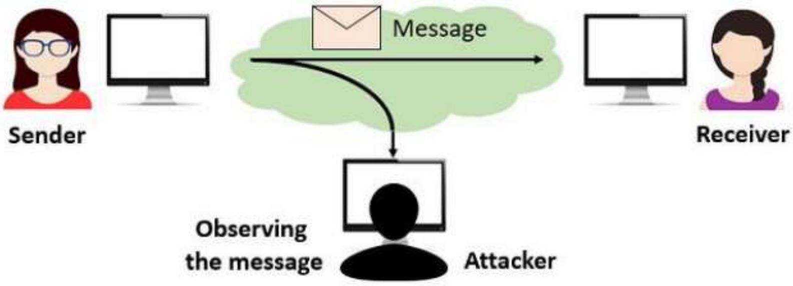


Fig: Passive Attack

- Two types of passive attacks:
  - ***Releases of message content:*** In this type, an attacker attempts to learn the contents of transmission.
  - ***Traffic analysis:*** Traffic analysis is the process of intercepting and examining message in order to deduce information from patterns in communication.

Active Attack

- These attacks attempts to alter system resources or affect their operations.
- It involves some modification of the data stream or creation of false stream.

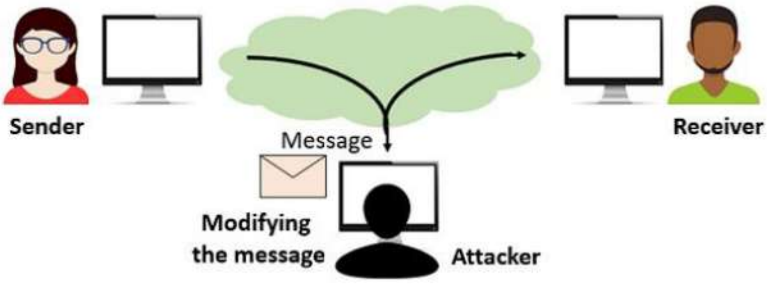


Fig: Active Attack

- It can be subdivided into four categories:
  - ***Masquerade:*** A masquerade is a type of attack where the attacker acts as an authorized user of a system to gain access to it or to gain greater privileges than they are authorized for.
  - ***Replay:*** It involves passive captures of data unit and its subsequent retransmission to produce an unauthorized effect.
  - ***Modification of message:*** In a message modification attack, some portion of message altered or that message are delayed or reordered to produce an unauthorized effect.
  - ***Denial of Service (DOS):*** In a DOS attack, users are deprived of access to a network or web resources. This is generally accomplished by overwhelming the target with more traffic than it can handle.

Various types of cryptanalytic attacks

1. ***Ciphertext-Only Attack:*** In this method, the attacker only has access to a set of ciphertexts but knows nothing about the plaintext data, the encryption algorithm being used or any data about the cryptographic key being used. The attacker's challenge is to figure out the 'key' which can then be used to decrypt all message.
2. ***Known-Plaintext Attack:*** In this method, the attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method.
3. ***Chosen-Plaintext Attack:*** In this method, the attacker chooses arbitrary plaintext data to be encrypted and then he receives the corresponding ciphertext. He tries to acquire the secret encryption key or alternatively to create an algorithm which would allow him to decrypt any ciphertext message encrypted using this key.
4. ***Chosen-Ciphertext Attack:*** In this method, the attacker can analyze any chosen ciphertexts together with their corresponding plaintexts. His goal is to acquire a secret key or to get as many information about the attacked system as possible.
5. ***Dictionary Attack:*** In this method, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext.
6. ***Brute-Force Attack:*** In this method, attacker tries all possible keys, and checks which one of them returns the correct plaintext.
7. ***Man-In-Middle Attack:*** A man-in-middle attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party. Generally, the attacker actively eavesdrops by intercepting public key message exchanged and retransmit the message while replacing the requested key with his own.

Security Services

A security service is something that enhances the security of data processing systems and information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the services.

1. ***Confidentiality:*** It is a security service that keeps the information secure from an unauthorized person. Encryption is a process to ensure the confidentiality.
2. ***Data integrity:*** The assurance that data received are exactly as sent by an authorized entity (i.e. contains no modification, insertion, deletion, or replay).
3. ***Authentication:*** The assurance that an entity of concern or the origin of communication is authentic. Two specific authentication services:

   - *Peer entity authentication:* When establishing a logical connection, assure that the other party is as claimed.

   - *Data origin authentication:* In a connectionless transfer, assure that the source of received data is as claimed.

4. ***Non-repudiation:*** Prevents either sender or receiver from denying message transmission or receipt of message.

   - *Origin non-repudiation:* preventing sender from denying that he has sent a message.

   - *Destination non-repudiation:* preventing receiver from denying that he has received a message.

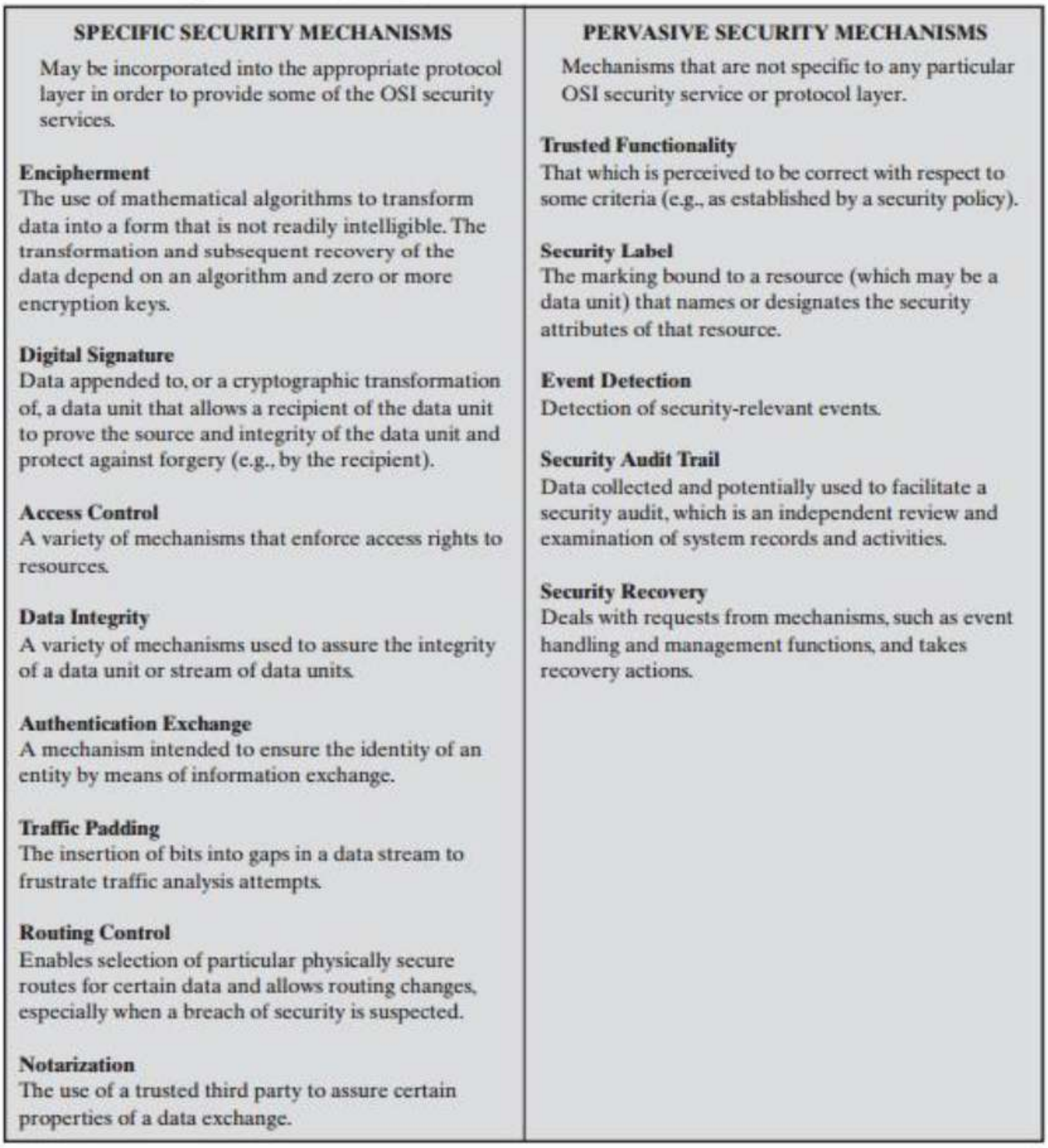
5. ***Access control:*** The prevention of the unauthorized use of a resource (i.e. this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

6. ***Availability:*** Making system or resources available upon demand by legitimate users.

Security Mechanisms

A mechanism that is designed to detect, prevent, or recover from a security attack. Following table lists the security mechanisms defined in X.800.

Security Mechanisms (X.800)



SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

Policy and Mechanism

- **Policy** are the rules of what are allowed to do and what are not.
- **Mechanisms** are procedure to ensure policy.

Example:

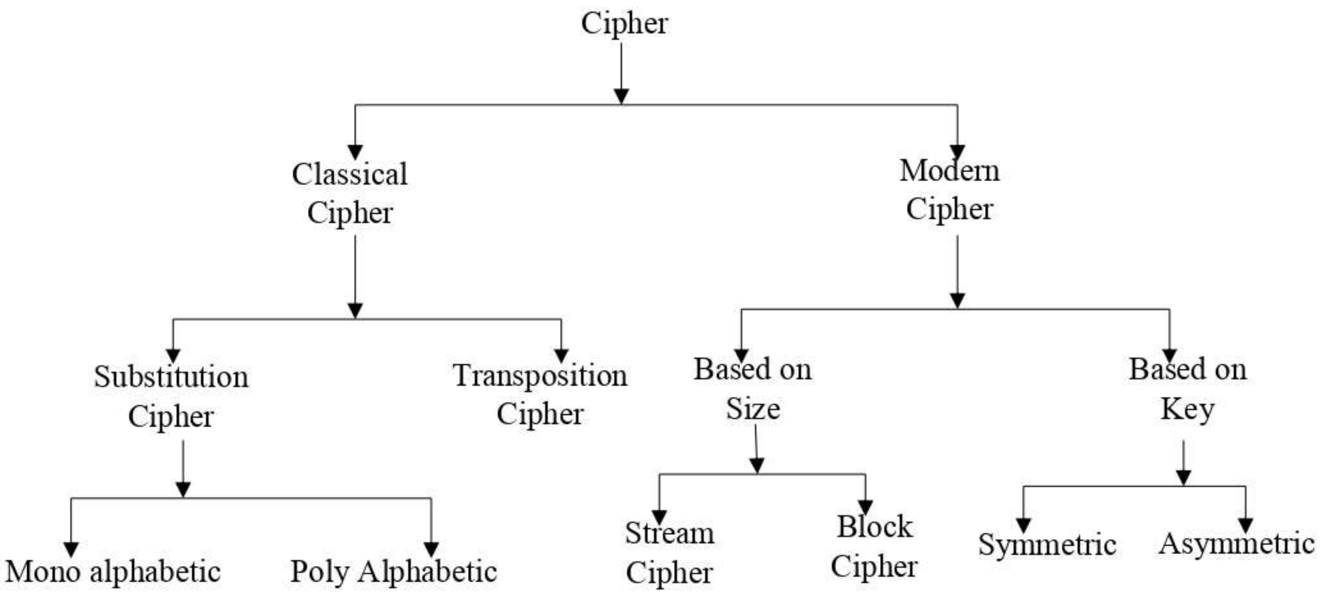
In a University

Policy → one cannot copy other's assignment

Mechanism → password protected

Suppose Sagar fails to protect his assignment and Jayanta copies it. → Jayanta breaks the policy.

Cipher Hierarchy



Classical Cipher

- The historic technique that used only the pen, pencil and normal mathematics to hide information.
- Classical ciphers are too weak to use now and can be broken easily with computer.
- Use the single key for both encryption and decryption.
- Two basic components of classical ciphers: ***Substitution*** and ***Transposition.***

- ***Substitution Cipher:*** A substitution is a technique in which each letter or bit of plaintext is substituted or replaced by some other letter, number or symbol to produce cipher text. E.g. Caesar, Playfair, Hill Cipher etc.

- ***Transposition Cipher:*** In transposition technique, there is no replacement of alphabets or numbers occurs instead their positions are changed or reordering of position of plaintext is done to produce cipher text. E.g. Rail Fence Cipher

Substitution Cipher Types

- ***Monoalphabetic Cipher***
  - The cipher alphabet for each plain alphabet is fixed throughout the encryption process. E.g. If 'A' gets substituted by 'E' then every occurrence of 'A' will be substituted by 'E'.
  - In monoalphabetic cipher, the relationship between a character in the plaintext and the character in the ciphertext is one-to-one.

- ***Polyalphabetic cipher***
  - The cipher alphabet for the plain alphabet may be different at different places during the encryption process. E.g. Vigenere cipher
  - In polyalphabetic cipher, the relationship between a character in the plaintext and the character in the ciphertext is one-to-many.

Caesar Cipher

It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

Example:

Plaintext: HELLO WORLD
Ciphertext: KHOOR ZRUOG (with key/shift=3)

Encryption of a letter by a shift k can be described mathematically as,

$$\boldsymbol{c = (m + k)\ mod\ 26}$$

Similarly, Decryption

$$\boldsymbol{m = (c + 26 - k)\ mod\ 26}$$

$$\begin{cases} m = Plaintext \\ c = Ciphertext \\ k = key \end{cases}$$

Here, we number each English alphabet starting from 0 (A) to 25 (Z).

Q. Given the plaintext "HELLO", compute the ciphertext and decrypt it afterward for the Ceaser cipher with key = 4.

Sol

Plaintext = HELLO Key = 4

Encryption:

For H, $c = (m + k)\ mod\ 26 = (7 + 4)\ mod\ 26 = 11\ mod\ 26 = 11 = L$

For E, $c = (4 + 4)\ mod\ 26 = 8\ mod\ 26 = 8 = I$

For L, $c = (11 + 4)\ mod\ 26 = 15\ mod\ 26 = 15 = P$

For O, $c = (14 + 4)\ mod\ 26 = 18\ mod\ 26 = 18 = S$

$\therefore Ciphertext = LIPPS$

Decryption:

For L, $m = (c + 26 - k)\ mod\ 26 = (11 + 26 - 4)\ mod\ 26 = 33\ mod\ 26 = 7 = H$

For I, $m = (8 + 26 - 4)\ mod\ 26 = 30\ mod\ 26 = 4 = E$

For P, $m = (15 + 26 - 4)\ mod\ 26 = 37\ mod\ 26 = 11 = L$

For S, $m = (18 + 26 - 4)\ mod\ 26 = 40\ mod\ 26 = 14 = O$

$\therefore Plaintext = HELLO$

Q. Decrypt the ciphertext "TEXER MR GWMX" with key = 4.

(Sol^n: PATAN IN CSIT)

Playfair Cipher

The Playfair algorithm works on the basis of 5 × 5 matrix.

Matrix construction method:

- Given the keyword, write down its letter from left to right and top to down on the matrix, without repeating the letter and fill the remainder of the matrix with the remaining letters in the alphabetic order.
- $I\ and\ J$ are considered as same letter.

Encryption process:

- Each time a pair of letter is encrypted.
- The pair cannot contain same letter. If so, separate it with the filler(X).
  E.g. HELLO →HE LX LO

Rules:

1. If the two letters are in same row, then replace it with the letter one position ahead in the same row (circularly).
2. If the letters are in same column, then replace it with the letter on position below in the same column (circularly).
3. Otherwise, replace it with the letter that lies in its own row and column occupied by the other plaintext letter.

Decryption process:

- Decryption is nearly identical to the encryption process, except for rules 1 and 2 we must take the letters to the left and above respectively. Also we remove any extra filler(X) in the decrypted text to reveal the final plaintext.

Q. Find out cipher text of below plaintext using Playfair Cipher.
Plaintext: TREE IS GREEN, Keyword: ENVIRONMENT

Sol^n:

Keyword: ENVIRONMENT

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

Playfair matrix

Plaintext: TREE IS GREEN

Breaking the given plaintext as: TR EX EI SG RE EN

Ciphertext: BV VU NR QH EN NV

$\therefore Ciphertext = BVVUNRQHENNV$

Q. Construct a Playfair matrix with the key "CSIT AT PATAN". Using this matrix encrypt the message "CSIT IS THE BEST".

Sol^n:

Keyword: CSIT AT PATAN

Playfair matrix:

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

Plaintext: CSIT IS THE BEST

Breaking the given plaintext as: CS IT IS TH EB ES TX

Ciphertext: SI TA TI IK PD NA IY

$\therefore Ciphertext = SITATIIKPDNAIY$

Q. Decrypt the following ciphertext using Playfair cipher.
Keyword: KEYWORD Ciphertext: LCNKZKVFYOGQCEBW

Sol^n:

Keyword: KEYWORD

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

Ciphertext: LCNKZKVFYOGQCEBW

Breaking the given ciphertext as: LC NK ZK VF YO GQ CE BW

Plaintext: CO ME TO TH EW IN DO WX

$\therefore Plaintext = COME\ TO\ THE\ WINDOW$

Hill Cipher

- Hill cipher is a polygraphic substitution cipher based on linear algebra.
- Key is $n \times n$ matrix.
- Each time n plaintext is encrypted or n ciphertext is decrypted.

Encryption:

$$C = KP \bmod 26$$

Decryption:

$$P = K^{-1}C \bmod 26 \quad [where, K^{-1} = (detK)^{-1}Adj(K)]$$

Where, K is $n \times n$ key matrix, K^{-1} is its inverse matrix, P is plaintext matrix and C is ciphertext matrix.

Q. Encrypt and decrypt it afterward the message "HELP" using the Hill cipher with the key $\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}_{2\times2}$.Show your calculations and the result.

Sol

Given,

$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}_{2\times2}$

Plaintext = HELP

P =HE LP

Encryption:

$$C = KP \; mod \; 26$$

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} H \\ E \end{bmatrix} mod \; 26 = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} 7 \\ 4 \end{bmatrix} mod \; 26 = \begin{bmatrix} 33 \\ 34 \end{bmatrix} mod \; 26 = \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} H \\ I \end{bmatrix}$$

$$\begin{bmatrix} C_3 \\ C_4 \end{bmatrix} = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} L \\ P \end{bmatrix} mod \; 26 = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} 11 \\ 15 \end{bmatrix} mod \; 26 = \begin{bmatrix} 78 \\ 97 \end{bmatrix} mod \; 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$

$\therefore Ciphertext = HIAT$

Decryption:

$$P = K^{-1}C \; mod \; 26 \;\; where, K^{-1} = (detK)^{-1}Adj(K)$$

To decrypt, we need to find K^{-1}. So,

$\det(K) = (5 * 3) - (2 * 3) = 9$

$(detK)^{-1} = x \; i.e. 9^{-1} = x$

$(9 * x) \; mod \; 26 = 1$
$(9 * 3) \; mod \; 26 = 1$ (*Use Hit and Trial method*)

The inverse of 9 is 3 since $(9 * 3) \; mod \; 26 = 1$.

$$K^{-1} = (detK)^{-1}Adj(K) = 3\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} mod \; 26 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

$\therefore Decryption \; key \; matrix = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$

Now,

Ciphertext = HI AT

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} H \\ I \end{bmatrix} mod \; 26 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 7 \\ 8 \end{bmatrix} mod \; 26 = \begin{bmatrix} 241 \\ 212 \end{bmatrix} mod \; 26 = \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} H \\ E \end{bmatrix}$$

$$\begin{bmatrix} P_3 \\ P_4 \end{bmatrix} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} A \\ T \end{bmatrix} mod \; 26 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 0 \\ 19 \end{bmatrix} mod \; 26 = \begin{bmatrix} 323 \\ 171 \end{bmatrix} mod \; 26 = \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} L \\ P \end{bmatrix}$$

$\therefore Plaintext = HELP$

Q. Decrypt the following ciphertext using Hill Cipher.

$$\boldsymbol{K = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}}\text{, } \textbf{\textit{Ciphertext = TFBJLBDFBK}}$$

Sol^n:

$$P = K^{-1}C \, mod \, 26 \, where, K^{-1} = (detK)^{-1}Adj(K)$$

$\det(K) = 7 * 11 - 11 * 8 = 77 - 88 = -11 \, mod \, 26 = 15$

$15^{-1} = x$

$(15 * x) \, mod \, 26 = 1$
$\therefore 15^{-1} = 7$ since, $(15 * 7) \, mod \, 26 = 1$

$$K^{-1} = (detK)^{-1}Adj(K) = 7\begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix} = \begin{bmatrix} 77 & -56 \\ -77 & 49 \end{bmatrix} mod \, 26 = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$$

Now,

Ciphertext = TF BJ LB DF BK

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} T \\ F \end{bmatrix} mod \, 26 = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 19 \\ 5 \end{bmatrix} mod \, 26 = \begin{bmatrix} 585 \\ 134 \end{bmatrix} mod \, 26 = \begin{bmatrix} 13 \\ 4 \end{bmatrix} = \begin{bmatrix} N \\ E \end{bmatrix}$$

$$\begin{bmatrix} P_3 \\ P_4 \end{bmatrix} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} B \\ J \end{bmatrix} mod \, 26 = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 1 \\ 9 \end{bmatrix} mod \, 26 = \begin{bmatrix} 223 \\ 208 \end{bmatrix} mod \, 26 = \begin{bmatrix} 15 \\ 0 \end{bmatrix} = \begin{bmatrix} P \\ A \end{bmatrix}$$

$$\begin{bmatrix} P_5 \\ P_6 \end{bmatrix} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} L \\ B \end{bmatrix} mod \, 26 = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 11 \\ 1 \end{bmatrix} mod \, 26 = \begin{bmatrix} 297 \\ 34 \end{bmatrix} mod \, 26 = \begin{bmatrix} 11 \\ 8 \end{bmatrix} = \begin{bmatrix} L \\ I \end{bmatrix}$$

$$\begin{bmatrix} P_7 \\ P_8 \end{bmatrix} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} D \\ F \end{bmatrix} mod \, 26 = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 3 \\ 5 \end{bmatrix} mod \, 26 = \begin{bmatrix} 185 \\ 118 \end{bmatrix} mod \, 26 = \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} D \\ O \end{bmatrix}$$

$$\begin{bmatrix} P_9 \\ P_{10} \end{bmatrix} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} B \\ K \end{bmatrix} mod \, 26 = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}\begin{bmatrix} 1 \\ 10 \end{bmatrix} mod \, 26 = \begin{bmatrix} 245 \\ 231 \end{bmatrix} mod \, 26 = \begin{bmatrix} 11 \\ 23 \end{bmatrix} = \begin{bmatrix} L \\ X \end{bmatrix}$$

$\therefore Plaintext = NEPALIDOLX$

Q. Encrypt and Decrypt the message "SAFE MESSAGES" using the Hill cipher with the key $\boldsymbol{\begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{pmatrix}}$***.***

Sol^n:

Plaintext = SAFE MESSAGES

Encryption:

P = SAF EME SSA GES

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}\begin{bmatrix} S \\ A \\ F \end{bmatrix} mod \, 26 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}\begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} mod \, 26 = \begin{bmatrix} 111 \\ 211 \\ 174 \end{bmatrix} mod \, 26 = \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix} = \begin{bmatrix} H \\ D \\ S \end{bmatrix}$$

$$\begin{bmatrix} C_4 \\ C_5 \\ C_6 \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}\begin{bmatrix} E \\ M \\ E \end{bmatrix} mod \, 26 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix}\begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} mod \, 26 = \begin{bmatrix} 164 \\ 144 \\ 212 \end{bmatrix} mod \, 26 = \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix} = \begin{bmatrix} I \\ O \\ E \end{bmatrix}$$

$$\begin{bmatrix} C_7 \\ C_8 \\ C_9 \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} S \\ S \\ A \end{bmatrix} mod\ 26 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix} mod\ 26 = \begin{bmatrix} 180 \\ 198 \\ 378 \end{bmatrix} mod\ 26 = \begin{bmatrix} 24 \\ 16 \\ 14 \end{bmatrix} = \begin{bmatrix} Y \\ Q \\ O \end{bmatrix}$$

$$\begin{bmatrix} C_{10} \\ C_{11} \\ C_{12} \end{bmatrix} = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} G \\ E \\ S \end{bmatrix} mod\ 26 = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{bmatrix} \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} mod\ 26 = \begin{bmatrix} 314 \\ 364 \\ 208 \end{bmatrix} mod\ 26 = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} C \\ A \\ A \end{bmatrix}$$

$\therefore Ciphertext = HDSIOEYQOCAA$

Decryption:

$$P = K^{-1}C\ mod\ 26 where, K^{-1} = (detK)^{-1}Adj(K)$$

$\det(K) = 2(24 - 221) - 8(42 - 136) + 15(91 - 32) = 1243$

$1243^{-1} = x$

$(1243 * x)\ mod\ 26 = 1$

$\therefore 15^{-1} = 5$ since, $(1243 * 5)\ mod\ 26 = 1$

Calculating cofactor matrix we get,

$$Cofactor\ matrix = \begin{bmatrix} -197 & 94 & 59 \\ 147 & -108 & 38 \\ 76 & 71 & -48 \end{bmatrix}$$

$$Adj(k) = \begin{bmatrix} -197 & 147 & 76 \\ 94 & -108 & 71 \\ 59 & 38 & -48 \end{bmatrix} mod\ 26 = \begin{bmatrix} 11 & 17 & 24 \\ 16 & 22 & 19 \\ 7 & 12 & 4 \end{bmatrix}$$

$$K^{-1} = 5 \begin{bmatrix} 11 & 17 & 24 \\ 16 & 22 & 19 \\ 7 & 12 & 4 \end{bmatrix} = \begin{bmatrix} 55 & 85 & 120 \\ 80 & 110 & 95 \\ 35 & 60 & 20 \end{bmatrix} mod\ 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix}$$

Now,

Ciphertext = HDS IOE YQO CAA

$$\begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} H \\ D \\ S \end{bmatrix} mod\ 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 7 \\ 3 \\ 18 \end{bmatrix} mod\ 26 = \begin{bmatrix} 330 \\ 338 \\ 447 \end{bmatrix} mod\ 26 = \begin{bmatrix} 18 \\ 0 \\ 5 \end{bmatrix} = \begin{bmatrix} S \\ A \\ F \end{bmatrix}$$

$$\begin{bmatrix} P_4 \\ P_5 \\ P_6 \end{bmatrix} = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} I \\ O \\ E \end{bmatrix} mod\ 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \\ 4 \end{bmatrix} mod\ 26 = \begin{bmatrix} 186 \\ 168 \\ 264 \end{bmatrix} mod\ 26 = \begin{bmatrix} 4 \\ 12 \\ 4 \end{bmatrix} = \begin{bmatrix} E \\ M \\ E \end{bmatrix}$$

$$\begin{bmatrix} P_7 \\ P_8 \\ P_9 \end{bmatrix} = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} Y \\ Q \\ O \end{bmatrix} mod\ 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 24 \\ 16 \\ 14 \end{bmatrix} mod\ 26 = \begin{bmatrix} 408 \\ 382 \\ 624 \end{bmatrix} mod\ 26 = \begin{bmatrix} 18 \\ 18 \\ 0 \end{bmatrix} = \begin{bmatrix} S \\ S \\ A \end{bmatrix}$$

$$\begin{bmatrix} P_{10} \\ P_{11} \\ P_{12} \end{bmatrix} = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} C \\ A \\ A \end{bmatrix} mod\ 26 = \begin{bmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} mod\ 26 = \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} mod\ 26 = \begin{bmatrix} 6 \\ 4 \\ 18 \end{bmatrix} = \begin{bmatrix} G \\ E \\ S \end{bmatrix}$$

∴Plaintext = SAFE MESSAGES

Vigenere Cipher

- It is a **Polyalphabetic** substitution cipher.
- It is based on the matrix of alphabet i.e. 26×26 matrix.
- Plaintext is assumed to be in row and key is assumed to be in column.
- The length of key and plaintext must be same. (Repeat the letters of key over and over until it is the same length as the plaintext).

Encryption:

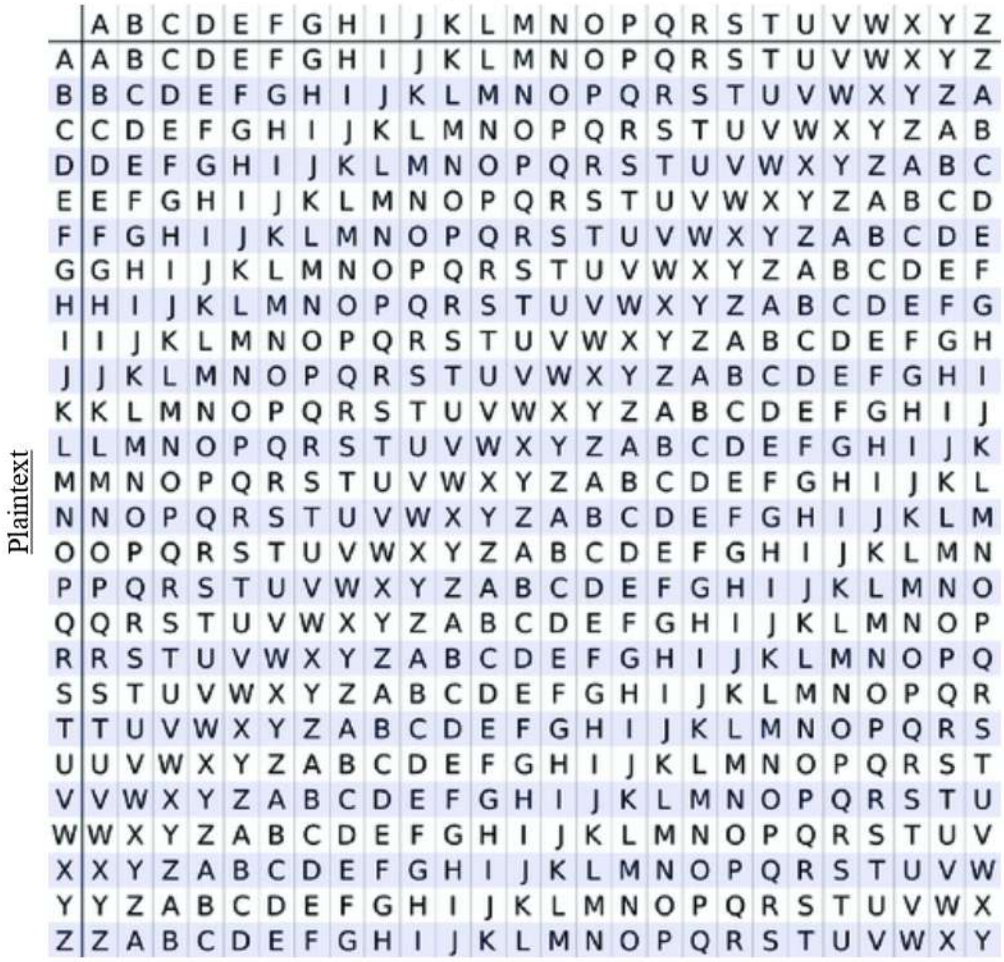
- Ciphertext letter is the intersection of plaintext letter and corresponding key letter in the table.

Decryption:

- Decryption is performed by finding the position of the ciphertext letter in a column, corresponding to the key letter, of the table, and then taking the label of the row in which it appears as the plaintext letter.

Vigenere Table:

Key



Plaintext

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

Example

Plaintext: CAPSULE

Key: FAD

Encryption:

Repeat the letters of k so that the number of letters in P & k becomes equal. i.e.

P: C A P S U L E
k: F A D F A D F

$Ciphertext = HASXUOJ$

Decryption:

Ciphertext: H A S X U O J
Key: F A D F A D F

Plaintext =CAPSULE

Q. Configure a Vigenere table for the characters from A-H. Use the table to encrypt the text DAD CAFE EACH BABE using the key FADE.

<u>Solⁿ</u>:

Vigenere table for the characters from A-H:

Key

Plaintext	A	B	C	D	E	F	G	H
A	A	B	C	D	E	F	G	H
B	B	C	D	E	F	G	H	A
C	C	D	E	F	G	H	A	B
D	D	E	F	G	H	A	B	C
E	E	F	G	H	A	B	C	D
F	F	G	H	A	B	C	D	E
G	G	H	A	B	C	D	E	F
H	H	A	B	C	D	E	F	G

Plaintext: D A D C A F E E A C H B A B E
Key: F A D E F A D E F A D E F A D

$Ciphertext = AAGGFFHAFCCFFBH$

One Time Pad (Vernam Cipher)

- It is a type of substitution cipher.
- One time pad technique uses a random key of the same length of messa**ge.**
- **Each key is used only once, and both sender and receiver must destroy** their key after use.
- There should be only two copies of the key: one for the sender and one for the receiver.
- Sender generates new key for every new message while sending message to receiver so it called as one time pad.

Encryption:

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

Decryption:

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

Q. Encrypt and decrypt the message "HELLO" with the key "NCBTA" using One time pad cipher.

Sol^n:

Plaintext: HELLO
Key: NCBTA

Encryption:

Plaintext (P)	H	E	L	L	O
Numerical Plaintext	7	4	11	11	14
	+				
Key (K)	N	C	B	T	A
Numerical Key	13	2	1	19	0
P + K	20	6	12	30	14
(P+K) mod 26	20	6	12	4	14
Ciphertext(C)	V	G	M	E	O

$\therefore Ciphertext = VGMEO$

Decryption:

Ciphertext(C)	V	G	M	E	O
Numerical Ciphertext	20	6	12	4	14
	-				
Key (K)	N	C	B	T	A
Numerical Key	13	2	1	19	0
C - K	7	4	11	-15	14
(C-K) mod 26	7	4	11	11	14
Plaintext (P)	H	E	L	L	O

$\therefore Plaintext \ = \ HELLO$

Rail-Fence Cipher

- The Rail Fence Cipher is a form of ***transposition cipher***.
- It depends on the matrix whose dimension is defined by the length of plaintext (or ciphertext) and a number of rails.
  No. of rows = no. of rails (key)
  No. of columns = length of plaintext / ciphertext

Encryption:

- The plaintext is written in diagonally, from top to bottom and after reaching rails, it goes bottom to top and so on.
- The ciphertext is written in row-wise from the matrix.

Decryption:

- Construct the rail matrix according to length of ciphertext (columns) and number of rails (rows). Once we've got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively).
- Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in diagonal manner to obtain the original text.

Q. Given the plaintext "ABRA KA DABRA", compute the ciphertext for the Railfence cipher with rails = 3.

Solⁿ:

Plaintext: ABRA KA DABRA
No. of rails = 3

A				K				B		
	B		A		A		A		R	
		R				D				A

$\therefore Ciphertext = AKBBAAARRDA$

Q. Encrypt the plaintext "CAPTAIN AVENGER" with rails = 4 using Railfence cipher.

Solⁿ:

Plaintext: CAPTAIN AVENGER
No. of rails = 4

C						N						E	
	A				I		A				G		R
		P		A				V		N			
			T						E				

$\therefore Ciphertext = CNEAIAGRPAVNTE$

Q. Decrypt the ciphertext "CAVEATIAEGRPNN" with no. of rails = 3 using Railfence cipher.

Solⁿ:

Ciphertext: CAVEATIAEGRPNN
No. of rails = 3

*				*				*				*	
	*		*		*		*		*		*		*
		*				*				*			

C				A				V				E	
	A		T		I		A		E		G		R
		P				N				N			

∴Plaintext =CAPTAINAVENGER

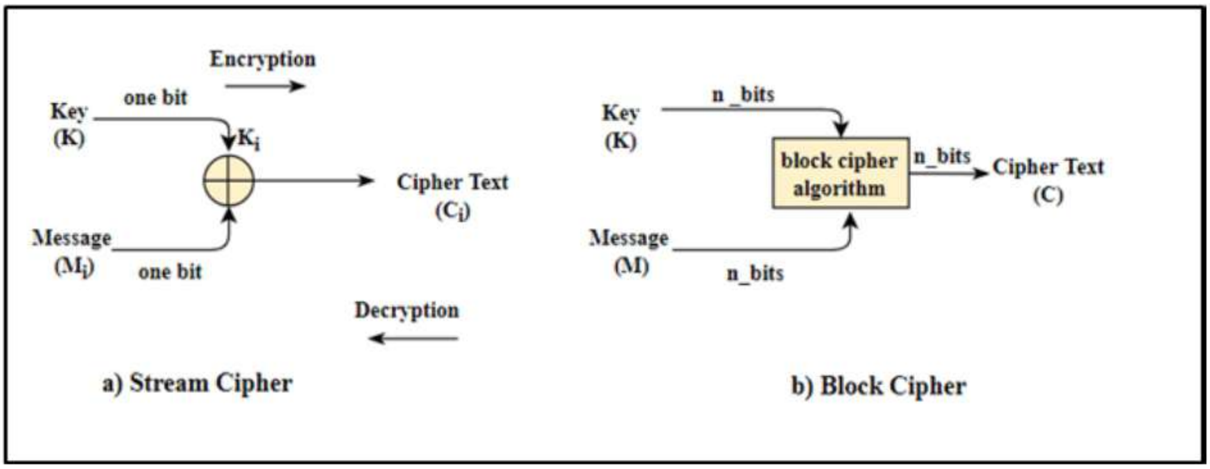
Modern Ciphers

Modern Ciphers can be divided by two criteria: ***Based on size*** and ***Based on key***.

Based on Size

- Stream Cipher
- Block Cipher

- *A **stream cipher*** is one that encrypts or decrypts one bit or one byte at a time. E.g. Classical stream ciphers are vigenere cipher, vernam cipher etc.
- A ***block cipher*** is one that encrypts or decrypts a fixed sized block of bits at one time. E.g. DES, AES



Stream Cipher vs. Block Cipher

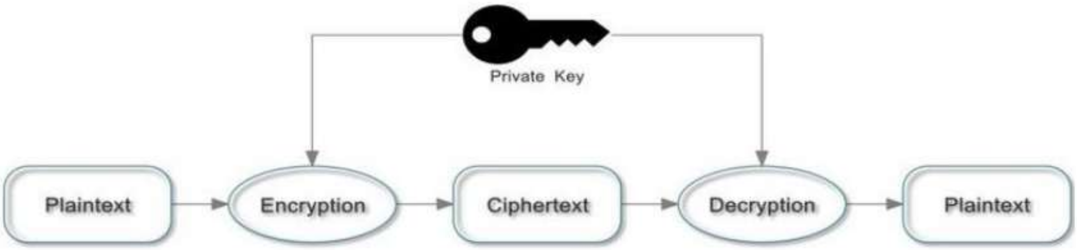
Stream Cipher	Block Cipher
1. Each time a bit is encrypted or decrypted at a time.	**1.** Each time a block of bits is encrypted or decrypted.
Advantages:	***Disadvantages:***
2. Faster than block cipher.	**2.** Slower than stream cipher.
3. Low error propagation i.e. an error in bit can only damage that bit.	**3.** High error propagation i.e. an error in bit can corrupt the whole block.
Disadvantages:	***Advantages:***
4. Low diffusion i.e. a secrecy of a bit is dependent only on a single bit.	**4.** High diffusion i.e. a secrecy of a single bit is depend on a whole block.
5. Susceptibility to malicious insertion and modification.	**5.** Immunity to insertion of symbol.
6. ***Example:*** One time pad	**6.** ***Example:*** DES (Data Encryption Standard)

Based on Key

- Symmetric cryptography
- Asymmetric cryptography

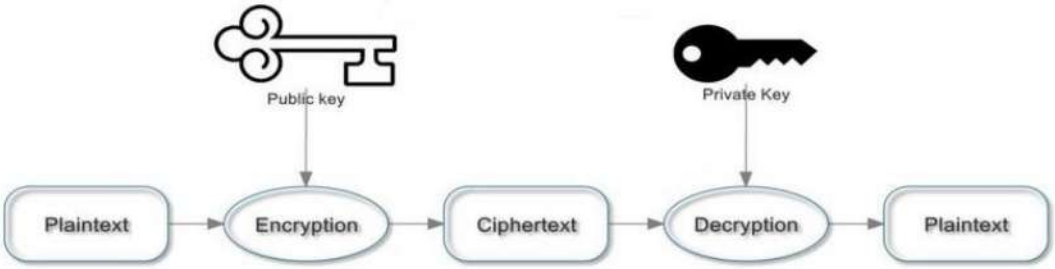
Symmetric Cryptography (Private key cryptography):

- These technique use single key for encryption as well decryption.
- The sender and receiver must have a shared key set up in advance and kept secret from all other parties; the sender uses this key for encryption and receiver use the same key for decryption.



Asymmetric Cryptography (Public key cryptography):

- These technique use two key, namely private and public keys. One key is used for encryption and the other is used for decryption.
- Public key is publically available while private key is kept secret.



Symmetric vs Asymmetric Cryptography

Symmetric Cryptography	***Asymmetric Cryptography***
In symmetric cryptography, single or same key is used for both encryption as well as decryption.	In asymmetric cryptography, two separate keys are used, one for encryption and the other for decryption.
It is faster than asymmetric cryptography.	Because of different keys used for encryption and decryption, it is slower than symmetric cryptography.
It utilizes less resources as compared to asymmetric cryptography.	It uses more resources as compared to symmetric cryptography.
Its strength of secrecy is weak.	Its strength of secrecy is relatively strong.
Key must be kept secret.	Public key is publically available.
E.g. Caesar, DES	E.g. RSA

Please let me know if I missed anything or anything is incorrect.

poudeljayanta99@gmail.com