Information security

Information security:
Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

Confidentiality:
Confidentiality is the protection of transmitted data from passive attacks. It is used to prevent the disclosure of information to unauthorized individuals or systems.

Authentication:
Authentication means verifying that users are who they say they are and that each input arriving at destination is from a trusted source.

Integrity:
Integrity means that data cannot be modified without authorization

Non-repudiation:
Non-repudiation means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction.

Access Control:
This refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive. It is the ability to limit and control the access to host systems and applications via communication links.

Availability:
Availability means information must be available when needed.

Mechanisms:

- **Encipherment:** It refers to the process of applying mathematical algorithms for converting data into a form that is not intelligible. This depends on algorithm used and encryption keys
- **Access Control**: A variety of techniques used for enforcing access permissions to the system resources.
- **Notarization**: The use of a trusted third party to assure certain properties of a data exchange.
- **Data Integrity**: A variety of mechanisms used to assure the integrity of a data.
- **Authentication** : A mechanism intended to ensure the identity of an entity by means of information exchange.
- **Bit stuffing**:Bit stuffing is the mechanism of inserting one or more non-information bits into a message to be transmitted, to break up the message sequence.
- **Digital signature**:It uses an advanced mathematical technique to check the authenticity and integrity of digital messages and documents.
    - **How it works:**
        - Using a mathematical algorithm will generate two keys: a public key and a private key. When a signer digitally signs a document, a cryptographic hash is generated for the document.
        - That cryptographic hash is then encrypted using the sender's private key, which is stored in a secure HSM box. It is then appended to the document and sent to the recipients along with the sender's public key.
        - The recipient can decrypt the encrypted hash with the sender's public key certificate. A cryptographic hash is again generated on the recipient's end.
        - Both cryptographic hashes are compared to check its authenticity. If they match, the document hasn't been tampered with and is considered valid.

- **Sand Boxing:**Sandbox environments provide a proactive layer of network security defense against new and Advanced Persistent Threats (APT).

Error Detecting Techniques:

Single parity check:

- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.

- if the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.

    - At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.

- This technique generates the total number of 1s even, so it is known as even-parity checking.

  1.

- **Two-Dimensional parity check:**Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.

- **Checksum:**

    1. A digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data.
    2. Checksum security uses the generated hash (a series of alphanumeric characters generated using a 1-way mathematical equation) value of a file and compares it against the expected checksum (usually provided by the supplier of the file) value.

- **Cyclic redundancy check:**

1. **Sender Side (Generation of Encoded Data from Data and Generator Polynomial (or Key)):**

i. The binary data is first by adding k-1 zeros in the end of the data.

ii. Use modulo -2 binary divisiion to divide binary data by the key and store remainder of division.

iii. Append the remainder at the end of the data to form the encoded data and send the same.

2. **Receiver Side (Check if there are errors introduced in transmission)**
   Perform modulo-2 division again and if the remainder is 0, then there are no errors.

Encryption with digital signature: Data is encrypted using sender's private key and hash is created of encypted data. The encypted data along with the hash is sent to the receiver. Receiver will convert the encrypted data to hash (hash1) and match with the hash sent by the sender. If both hash and hash1 match's then the reciever decrypt the data using the reciever's private key.

Ways of authenication:

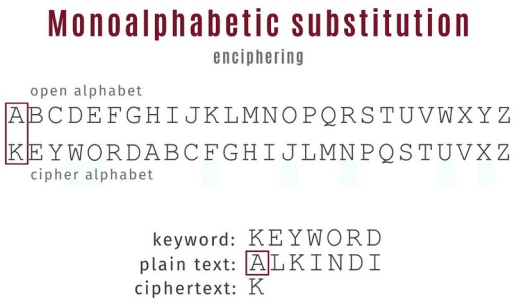
- **Encryption**:Cyper text act as authenticator.
- **MAC**:Message is passed with the key and fix length of code is generated.
- **Hash function**:Message is passed to generate a fixed length of code is generated.

CRYPTOGRAPHY

Key terms:

- **Plan text:**Data sender wants to send.
- **Cipher text:**Data converted using encryption methods.
- **Cyptography:**Conversion of plan text into cipher text and cipher text back to the plan text.
- **Cryptoanalysis:**Breaking of cipher text wihtout knowing the key.
- **Cyptology:**Cyptography+Cryptoanalysis.

Mono aplhabetical cipher:The substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext.



Homophonic substitution cipher: The Homophonic Substitution cipher is a substitution cipher in which single plaintext letters can be replaced by any of several different ciphertext letters. They are generally much more difficult to break than standard substitution ciphers.

Phishing: Phishing is a method of trying to gather personal information using deceptive e-mails and websites.

Eg:Spear Phishing,Whaling,Vishing,Email Phishing.

Botnet:A botnet(short for “robot network”) is a network of computers infected by malware that are under the control of a single attacking party.

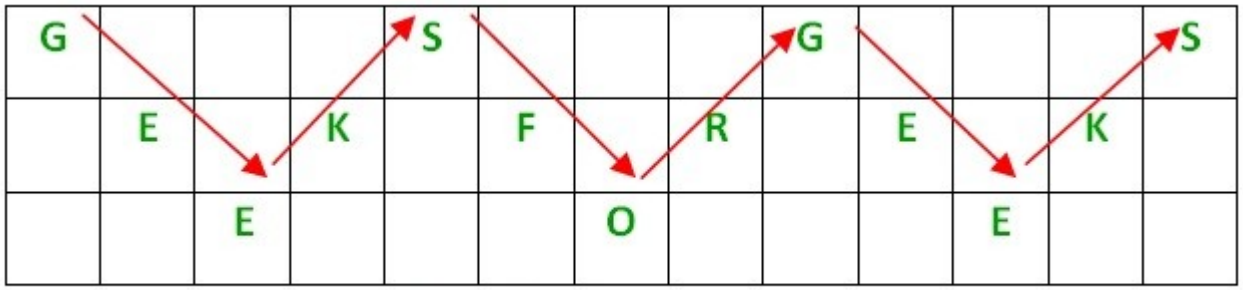
Polygram/polyalphabetic cipher :A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the *Vigenère square or Vigenère table*.

	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

Transportation Techniques:

Rail fence techniques:

- In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in a zig-zag manner.After each alphabet has been written, the individual rows are combined to obtain the cipher-text.



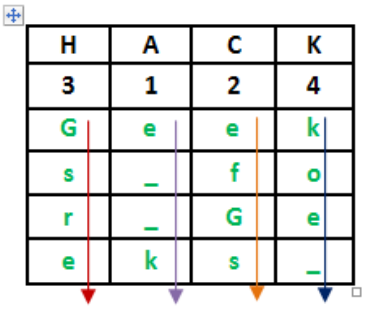
Columnar transposition :

1. The message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.
2. Width of the rows and the permutation of the columns are usually defined by a keyword.
3. For example, the word HACK is of length 4 (so the rows are of length 4), and the permutation is defined b the alphabetical order of the letters in the keyword. In this case, the order would be “3 1 2 4”.
4. Any spare spaces are filled with nulls or left blank or placed by a character (Example: _).
5. Finally, the message is read off in columns, in the order specified by the keyword.

Encryption

Given text = Geeks for Geeks

Keyword = HACK **Length of Keyword** = 4 (no of rows) **Order of Alphabets in HACK** = 3124



H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

Print Characters of column 1,2,3,4

Encrypted Text = e kefGsGsrekoe_

Symmetric key cryptography:A symmetric cipher is one that uses the same key for encryption and decryption.

Problems: The only secure way of exchanging keys would be exchanging them personally.

Sender must have seperate key for each individual.