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:

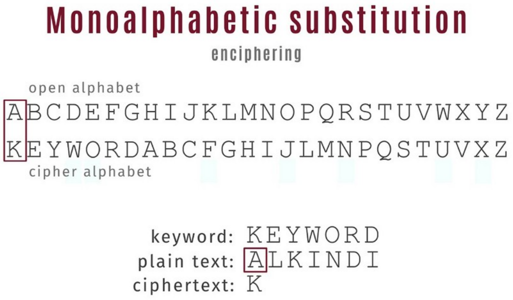
- **Encryption**:Cyper text act as authenticator.
- **MAC**:Message is passed with the key and fix length of code is generated.
- **Hash function**:Message is passed to generate a fixed length of code is generated.

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.



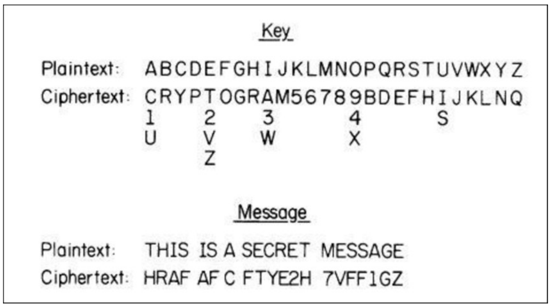
Monoalphabetic substitution

enciphering

```
open alphabet
ABCDEFGHIJKLMNOPQRSTUVWXYZ
KEYWORDABCFGHIJLMNPQSTUVXZ
cipher alphabet

   keyword: KEYWORD
plain text: ALKINDI
ciphertext: K
```

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.



Key

```
Plaintext:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext: CRYPTOGRAM56789BDEFHIJKLNQ
            1  2   3    4    S
            U  V   W    X
               Z
```

Message

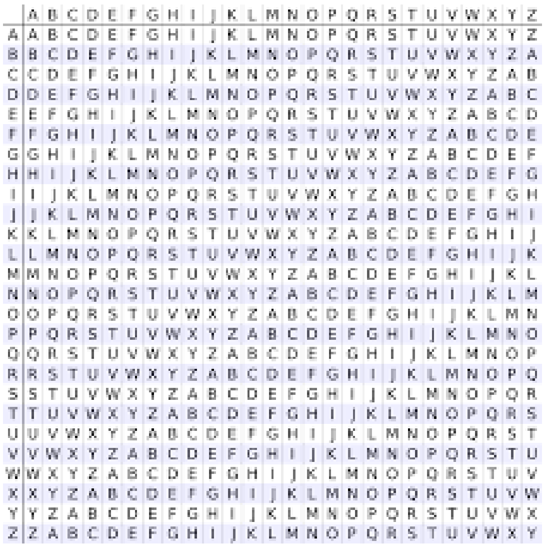
```
Plaintext:  THIS IS A SECRET MESSAGE
Ciphertext: HRAF AF C FTYE2H 7VFF1GZ
```

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*.

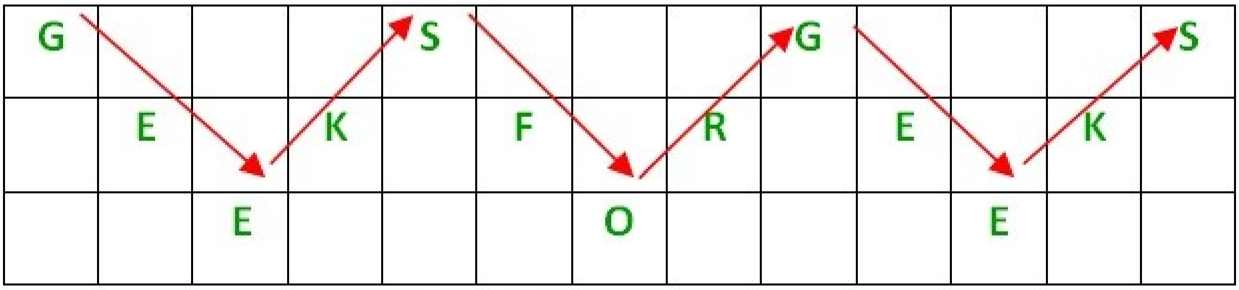


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

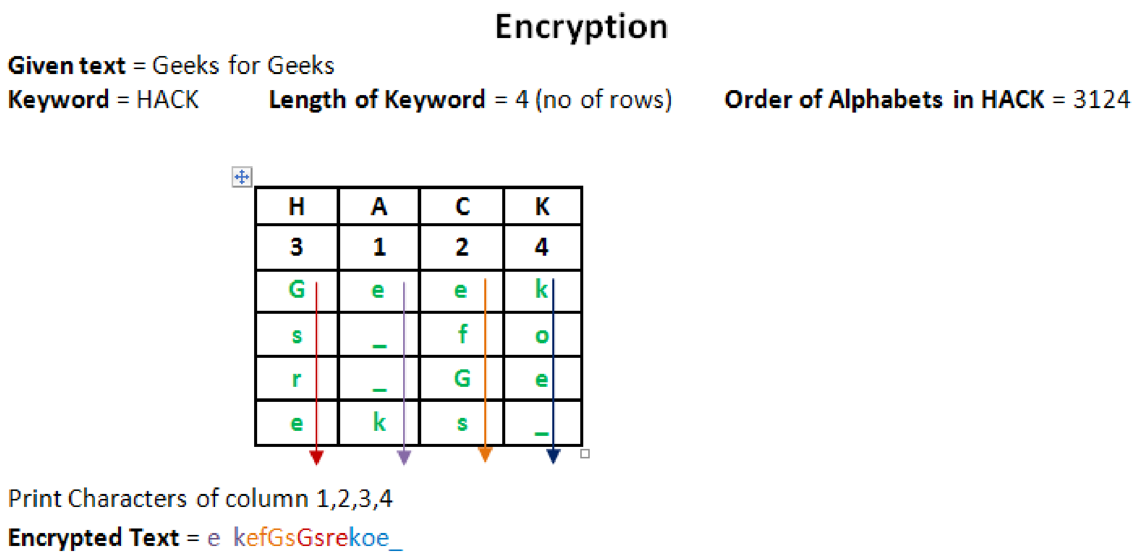


G				S				G				S
	E		K		F		R		E		K	
		E				O				E		

© copyright geeksforgeeks.org

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.

Data Integrity:

- Accuracy and completeness of data
- Security controls focused on integrity are designed to prevent data from being modified or misused by an unauthorized party
- Security Controls
    - Encryption
    - User access controls
    - Version control
    - Backup and recovery procedures
    - Error detection software

Authentication:

- process for establishing your identity to gain access to a system
- Typically Two steps
    - Identify Yourself(email id, phone number, mid, uid)
    - Prove your identity(passwords)
- MFA(Multi factor authentication)
    - OTP, finger print, iris scan

Ways to Authenticate:

- Something you are
  - Scanned Body Part
- Something You have
  - OTPs on mobile, Token only sent previously to authenticated devices.
- Something You know
  - Pin, Password, passphrase

DES ALGORITHEM:

the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key.In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.

1.The initial permutation is performed on plain text.

2.Next, the initial permutation (IP) produces two halves of the permuted block; says Left Plain Text (LPT) and Right Plain Text (RPT).

3.Now each LPT and RPT go through 16 rounds of the encryption process.

4.In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block

5.The result of this process produces 64-bit ciphertext.

Initial permutation(IP)

The first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block, and so on.This is nothing but jugglery of bit positions of the original plain text block.

Split

The table is split into two half Left Plain Text (LPT) and Right Plain Text (RPT).

Expansion permutation

During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. Bits are permuted as well hence called expansion permutation. This happens as the 32-bit RPT is divided into 8 blocks, with each block consisting of 4 bits. Then, each 4-bit block of the previous step is then expanded to a corresponding 6-bit block, i.e., per 4-bit block, 2 more bits are added.This process results in expansion as well as a permutation of the input bit while creating output. The key transformation process compresses the 56-bit key to 48 bits. Then the expansion permutation process expands the 32-bit RPT to 48-bits. Now the 48-bit key is XOR with 48-bit RPT and the resulting output is given to the next step, which is the S-Box substitution.

S-Box

It is the process that accepts the 48- bit input from the XOR operation involving the compressed key and expanded RPT and produces a 32-bit output using the substitution technique.The substitution is performed by 8 substitution boxes called S-Boxes.Each of the eight S-boxes has 6-bit input and 4-bit output. The 48- bit input block is divded into 8 sub-blocks and each such block is given to a s-box.The output of all the s-boxes are then combined to form a 32-bit block, which is given to the next stage of a round, the p-box permutation.

P-Box

Output of s-box consists of 32-bits,these are permuted using a P-box.This involves simple permutaion (swapping of each bit with another bit,without any expansion of compression).This is called as p-box permutation.

XOR or swap

All these operations are performed only on the 32-bit right half portion of the 64-bit original plain text(RPT).The left half protion(LPT) was untouched.The LPT is now XORed with the output produced by P-box permutaiton.The result of this XOR operation becomes the new right half (RPT).The old right half (RPT) becomes the newleft half(LPT) in a process of swapping.

Final Permutation

At the end of the 16 rounds,the final permutation is performed (only once).This is a simple transpostion.For Ex: the 40th input bit takes the position of the 1st output bit and so on. The output of the final permutation is the 64- bit encryption block.

Caesar cipher

Each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on.Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.

Block Encryption:

Electrical code book(ECB): The simplest mode of operation. Plain text message is divided into blocks of 64 bits each.Each such block is encrypted independently of the other blocks. For all blocks same key is used for encryption.If a plain text block repeats in teh original messages ,the corresponding cipher text block will also repeat in the encrypted message.suitable only for small messages.

Cipher Block Chaining(CBC): Chaining adds a feedback mechanism to a block cipher.The results of the encryption of the previous block are fed back into the encryption of the current block.In the first step; the first block of plain text and a random block of text , called initialization vector(IV) is used.The IV has no special meaning it is simply used to make each message unique.The value of IV is generated randomly.

Cipher Feedback(CFB): In this mode data is encrypted in units that are smaller(Eg: They could be of size 8 bits) than a defined block size(which is usually 64 bits).CFB mode works with i bits at a time (as we have seen,usually ,but not always,j=8).

Output feedback (OFB):OFB mode is extremely similar to the CFB. The only difference is that in the case of CFB. The cipher text is fed into the next stage of encryption process.In case of OFB , the output of the IV encryption process is fed into the next stage of encryption process. In this mode data is encrypted in units that are smaller(Eg: they could be of size 8 bits) than a defined block size(which is usually 64 bits).OFB mode works with j bits at a time (as we have seen, usually , but not always, j=8).

Counter Mode(CTR): Uses sequence numbers called as counters as the inputs. Usually a constanta is used as the inital counter value. Incremented for every iteration.The size of the counter block is same as that of the plain text block.

Diffe-Hellmen key exchange:

- First alice and bob agree upon 2 large prime numbers n and g.These 2 numbers need not be secret and can be shared publicly.
- Alice chooses another large random number X (private to her) and calculate A such that :
- Alice sends this to Bob.
- Bob chooses another large random number Y(private to him) and calculate B such that:
- Bob sends this to Alice.
- Alice now computes her secret key K1 as follows:
- Bob computes her secret key k2 as follows:
-