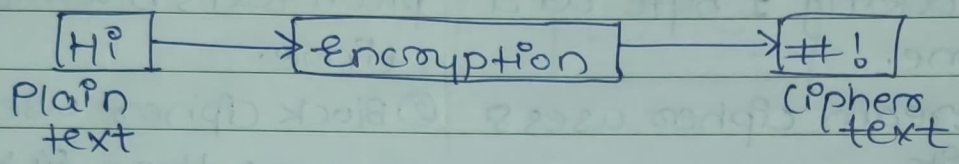
# Assignment no. 2

Page No.:
Date: 23/10/22

Q.1) What is Encryption and Decryption? Explain with diagram.

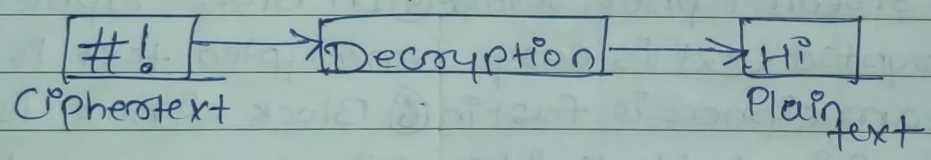
→ • Encryption:-

The process of encoding plain text messages into cipher text messages is called as encryption.




• Decryption:-

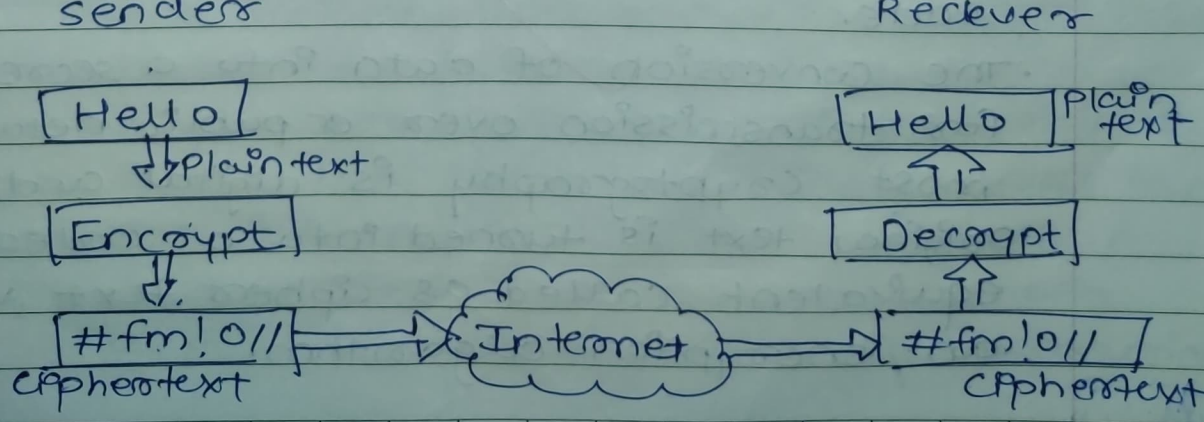
The reverse process of transforming cipher text messages back to plain text messages is called as decryption.




• Every encryption and decryption process has two aspects:-

a) The algorithm. b) The Key.

~~used for enc~~ It makes the process of cryptography secured.



Q.2) Differentiate between stream cipher and block cipher.

→

| Stream Cipher | Block Cipher. |
|---|---|
| ① Stream cipher converts plaintext into ciphertext by taking 1 byte at a time. | ① Block cipher converts the plain text by taking plain text's block at a time. |
| ② Stream cipher uses 8 bits. | ② Block cipher uses either or more than 64 bits. |
| ③ The complexity of stream cipher is complex. | ③ While block cipher is more complex. |
| ④ Stream cipher uses only confusion. | ④ Block cipher uses both confusion and defusion. |
| ⑤ In stream cipher, reverse encrypted text is easy. | ⑤ In Block cipher, reverse encrypted text is hard. |
| ⑥ Stream cipher is fast in comparision to block cipher. | ⑥ Block cipher is slow as compared to stream cipher. |

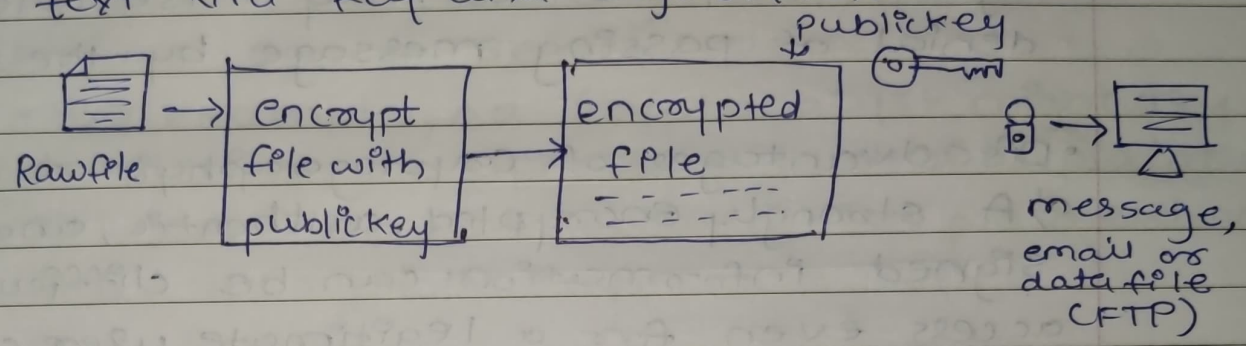
Q.3) Define cryptography process in details.

→
- Cryptography means act of writing in code or cipher.
- Cipher is a message written in a secret code.
- The conversion of data into a secret code for transmission over a public network most cryptography is digital and the original text is turned into a coded equivalent called as cipher text via an encryption algorithm.

• It has two methods :-

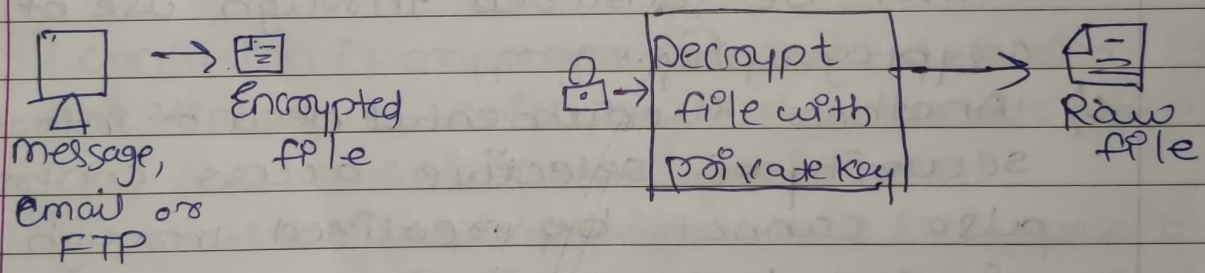
a) Encryption :-

The message is converted into cipher text via key and algorithm.




b) Decryption :-

The cipher text is converted ~~to~~ to plain text message ~~#~~ via key and algorithm.




Q.4) What are the advantages and disadvantages of cryptography?

→ • Advantages of Cryptography :-

a) Confidentiality :- Encryption technique can guard information and communication from unauthorized access of internet.

b) Authentication :- The cryptographic techniques such as MAC and digital signatures can protect information.

c) Data Integrity :- the cryptographic hash functions are playing vital role in assuring

users about data integrity.

d) Non-repudiation:- The digital signature provides non-repudiation service to guard against dispute that may arise due to denial of passing message by the sender.

• Disadvantages of Cryptography:-

a) A strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legitimate user at crucial time of decision-making.

b) High availability, one of the fundamental aspects of information security, cannot be ensured through use of cryptography.

c) Another fundamental need of information security of selective access control also cannot be realized through use of cryptography.

d) Cryptography doesn't guard against the vulnerabilities and threats that emerge from poor design of system, protocols and procedure.

Q.5) Define Crypt Analysis process.

→ • Crypt analysis is the study of the cryptographic algorithms and the breaking of those ciphertext, secret codes, etc..

• The person practicing cryptanalysis is called cryptanalyst.

- It helps us to better understand the cryptosystems and also helps us improve th system by finding any weak point and thus work on the algorithm to create a more secure secret code.
- For example, a cryptanalyst might try to decipher a ciphertext to derive plaintex It can help us to deduce the plaintext or the encryption key.

Q.6) Differentiate between Confusion and Defusion
→

| Confusion | Diffusion |
|---|---|
| ① Confusion is cryptagrophic technique which is used to create ciphertext. | ① While defusion is used to create cryptic plain text. |
| ② This technique is possible through substitution algorithm. | ② While it is possible through transportation algorithm. |
| ③ If one bit, within cipher text is modified all bits are also modified. | ③ If one image within plain text is modified all images are also modified. |
| ④ ~~Vgu~~ Vagueness is increased in resultant. | ④ Redundancy is increased in resultant. |
| ⑤ Both block cipher and stream cipher uses confusion. | ⑤ Only block cipher uses diffusion. |
| ⑥ ~~Cipher text~~ The relation between ciphertext and key is masked by confusion. | ⑥ The relation between cipher text and plaintext is masked by diffusion. |

Q.7) What are the properties of trustworthy encryption system?

→ ① It is based on sound mathematics:-

Good cryptographic algorithms are not just invented. They are derived from solid principles.

② It has been analyzed by ~~componen~~ competent experts and found to be sound:-

~~③ It has stood the 'test of time':-~~

Even the best cryptographic experts can think of ~~the~~ only so many possible attacks. The developers may become too convinced of strength of their own algorithm. A review by critical outside experts is essential.

③ It has stood the "test of time".

As a new algorithm gains popularity, people continue to review both its mathematical foundations and the way it builds upon those foundations. Although a long period of successful use and analysis is not a guarantee of good algorithm, the flaws in many algorithm are discovered relative soon after their release.

Q.8) What are the characteristics of good encryption technique?

→ • The process of encoding plain text messages into cipher text messages is called as encryption.

• Characteristics of good encryption technique are as follows:-

a) It must be computationally easy to encipher and decipher a message given the appropriate key.

b) It must be computationally infeasible to derive the private key from the public key.

c) It must be computationally infeasible to determine private key from a chosen plaintext attack.

Q.9) Give any example which convert plain text into cipher text.

→ • Example 1:-

Plain text:- MANISH

Key:- 9.

M :- 12 + 9 = 21 - V

A :- 0 + 9 = 9 - J

N :- 13 + 9 = 22 - W

I :- 8 + 9 = 17 - R

S :- 18 + 9 = 27 - B

H :- 7 + 9 = 16 - Q

Cipher text:- VJWRBQ.

- Example 2 :-

Plain text :- JADHAV.

Key :- 10.

J :- 9 + 10 = 19 - T
A :- 0 + 10 = 10 - K
D :- 3 + 10 = 13 - N
H :- 7 + 10 = 17 - R
A :- 0 + 10 = 10 - K
V :- 21 + 10 = 31 - F

Cipher text :- TKNRKF.

- Example 3 :-

Plain text :- JONATHAN.

Key :- 5.

J :- 9 + 5 = 14 - N
O :- 14 + 5 = 19 - T
N :- 13 + 5 = 18 - S
A :- 0 + 5 = 5 - F
T :- 19 + 5 = 24 - Y
H :- 7 + 5 = 12 - M
A :- 0 + 5 = 5 - F
N :- 13 + 5 = 18 - S

Cipher text :- NTSFYMFS.

- Example 4:-

Plain text:- MORTAL

Key:- 3.

M:- 12 + 3 = 15 - P
O:- 14 + 3 = 17 - R
R:- 17 + 3 = 20 - U
T:- 19 + 3 = 22 - W
A:- 0 + 3 = 3 - D
L:- 11 + 3 = 14 - O

Cipher text:- PRUWDO.

02/11/22