Name: Chhagan Kumawat
Roll no: 2023020167.

PAGE NO.
DATE / /

Assignment No 2.

Q1 What are the basic priciples of cryptography? How does cryptography contribute to hlw security.

→ Priciples of cryptography :-

1) Confidentiality :-
Ensures that information is only accessible to those who are authorized to access it.

2) Integrity :-
Ensures that the information has not been altered or tempered with during transmission or storage.
- Techniques such as cryptographic hash fun ensure the integrity of data by generating a fixed-size string that uniquely represents the original data.

3) Authentication :-
- Verifies the identity of the individual or systems involved in communication.
- Cryptography method such as digital signature and certificate authenticate user and devices conforme their identity.

4) Non-Reputation :-
Ensures that once a party sends a message, they cannot deney having sent it. Digital signatures provide proof that a specific individual sent a msg, this preventing denial of participation in a transaction.

5) Availablity :-
Ensure that authorized user have reliable access to information & resource when needed. While primarily

a concern in broader nlw security.

* Contribute of Cryptography to N/w. Security :-
- It plays a crucial role in a security nlw's by addres various vulnerabilities & ensuring secure communication.

1) Securing Data Transmission :-
Encryption protocols like SSL/TLS ensure that the data transmitted over nlw's remains confidential. & secure from eavesdropping by attackers.

2) Authentication of User & devices :-
Cryptographic techniques authenticate the entities communicating in a nlw.

3) Protecting Against Data Tempering :-
Integrity checking mechanism like MAC's & digital signatures prevent unauthorized modification of data.

4) Ensuring Secure Access :-
PKI enable secure access control by managing digital certificates.

Q2 What is Encryption & Decryption. Discuss the diff. bet symmetrics & asymmetrics cryptography algorithms. Enlist the all types of symmetric cryptography and explain any one.

→ Encryption :-
The process of converting plaintext into ciphertext using an encryption algorithm & a key.
- Encryption ensures that only authorized users who have the key can read the encrypted information.

- Decryption :-
The reverse process of encryption, where the ciphertext is converted back into plaintext using a decryption algorithm & a key.
- Only authorized user with the correct key can decrypt the information & access the original data.

- Difference.

Criteria	Symmetric Cryptography	Asymmetric Cryptography
1) Key	Single, shared key for both encryption & decryption.	Two key public key for encry -on, private key for decrypti
2) Speed	Faster	Slower
3) Security	Key distribution is a challe	Easier key distributio.
4) Use Case	Used for encrypting large amounts of data	Used for secure key exchange & authentica
5) Encryption Type	Block or Stream cipher	Based on mathematical problem like factoring large primes or elliptic curves.

→ Type of Symmetric Cryptography Algorithm :-
-① Block Ciphers :-
Encrypt data in fixed size blocks.
ex. AES, DES.

2) Stream Ciphers :-
Encrypt data one bit or byte at a time
ex. RC4 ; Scalse 20.

CO3 Short notes :-

1) Steganography :-
— Steganography is the practice of hiding secret information within non-secret data in such a info. within the existance.
- Steganography is the practice of concealing message or info. within other non-secret text or data to prevent detection.

→ Key Concepts :-
1) Carrier medium :-
The file or media when the hidden msg is embeded

2) Payload :-
The actual msg or data being concealed.

3) Stego file :-
The output file after embedding the payload into the carrier medium.

4) Encoding method :-
① LSB encoding, ② Transform domain.
3) Meta hiding.

5) Application :-
1) Covert Communication
2) Digital watermarking
3) Cybersecurity.

2) Block Cipher principle :-
Block cipher priciples are fundamental to understanding how block ciphers work in Cryptography.
- They are essential for security digital communication and data.

- Key priciple of Block Cipher :-
1) Fixed Block size :-
Block ciphers work by dividing plaintext into fixed-sized blocks.
— Common blocks size include 64. bit.

2) Key :-
The same key is used for both encryption & decryption.

3) Substitution - Permutation N/w (SPN) :-
Most block ciphers, like AES, user an SPN structure where the encryption involves rounds of substitution & permutation.

4) Rounds :-
It uses multiple round of transmission to achieve confusion & diffusion, essential for security.

— Popular Block cipher Algorithms :-
1) Data Encryption (DES)
2) Triple DES
3) Advanced Encryption Standard.

3) Data Encryption standard (DES) :-
The Data Encryption Standard is a symetric-key block cipher that was widely used for data encryption in the late 20th century.

- Key features :-
1) Block size
2) key size
3) Rounds :-
DES performs 16 round of encryption.

4) Feistal Structure :-
DES is based on the Feistal N/W a structure that divides the data block into two halves.

5) S-Boxes :-
DES is relied on sboxes to introduce non-linearity into the encryption process.

6) P-Box.

- DES Encryption process :-
1) inital Permutation
2) Round Function
3) Final Permutation.

- Security Concerns :-
1) Brute force vulnerability.
2) Differential & linear Cryptanalysis.

4) International Data Encryption Algorithm (IDEA)
- The International Data Encryption Algorithm is a symmetric-key block cipher that was designed to provide strong encryption & improved security over older algorithm like DES.

- Key features :-
1) Block size :-
It operates on 64-bit blocks of data.

2) Key-size :-
It used a 128-bit key for encryption & dic.

3) Structure :-
It is based on a feistel-like structure.

4) Round :-
Each of the 8 rounds.

- Security :-
1) Resilience to cryptanalysis
2) Brute-force Resistance.

- Advantages :-
1) Efficiency
2) strong security
3) low memory Requirement.

- Disadvantage :-
1) Block size
2) Patent.

- Application
1) Pretty Good privacy
2) Other cryptographic system.