Name: Chhagan Kumawat
Roll no: 2023020106 7.

Assignment 3.

Q1. Discuss the priciples of public key cryptography?

→ Public key cryptography, also knows as assemmetric cryptography are a class of cryptography protocol that used two distinct but mathamatically related.

Keys: ① Public key ② Private key.

- These key are used for encryption & dicription providing secure communication authentication, & digital signature.

- key priciples of Public key cryptogr system :-

1) key pair :-
The public key is openly shared & freely anyone can access.
- The private key is kept secret & is used to decrypt data encrypted.

2) Asymmetrics Encryption:-
In this the public key is used to encryption a message, & only the corresponding private key can decrypt it.

3) Authentication:-
This provides authentication & data integrity.

4) Key management:-
public key cryptography simplifies key managemat compared to symmetric key systems.

5) Mathemetical Hardness:-
This ensure tha' security of the system.

6) One-way Function:-
A funct conceptin public key cryptossystems is the use of one-way functions.

7) Confidentiality & Non-Reputation:-
Ensured when a message is encrypted using the recipients publickey.
Provided through digital signatures.

8) Public Key Infrastructure (PKI):-
PKI is a framework for managing public keys & certificate which associates public key with the identities of individual organizations or devices.

Q 2). What is assymmetric cryptography Enlist the all types of asymmetric Cryptography & explained any

→ Asymmetric cryptography, also known as public-key cryptography, is a type of Cryptography system that one used a pair keys for encryption & decryption a public key is used for encryption, & the corresponding private key is used for decryption, or vice versa.

— Key feature
1) Public key 2) Privat key
3) Non-repudation 4) Security.

— Type of
1) RSA
2) Elliptic Curve cryptography
3) DSA
4) Diffire-Hellman key exchange
5) ElGamal 6) Lattice-Based Cryptography.

— RSA Cryptosystem:-
RSA - Rivest - Shamir - Adleman is based on the integer fasterization problem, commenly used for secure communication & digital signatures.
— RSA can be used for both encryption or decrypt & digital signature.

— How RSA Works:-
1) Key Generation 3) Decryption
2) Encryption 4) Digital signature.

— Security:-
RSA is vulnerable to certain type of attacks like chosen-ciphertext attacks which required careful padding & key management practice.

— Application:-
1) Secure Internet Communication
2) Email Encryption
3) Digital Signatures.

Q3. Explain the concept of message Integrity, Right msg

→ Message Integrity:-
It refers to the assurance that a msg has not been attened or tempered with during trasmision or storage.
— It ensure that the data sent
— This is critical in secure communications as it guarantees the accuracy & reliability of the msg, preventing unauthorized modifications.

→ Message Digest :-
It is a cryptography hai function output a fixed length string that uniquely represents a msg.
- It is essentially a fingerprint of the original message.
- Any small change in the message, even a single character, will result in a completely diff msg digest, making it an effective way to verify message integrity.

Q4. Write a short note on following
A RSA algorithm :-
The RSA algorithm is a widely used public-key cryptographic system for secure data transaction
- It is named after its inventors, Rivest, Shamir and Adleman who introduce it in 1977.
- RSA is primary used for secure communication & encryption as well as digital signature & authentication.

- Key concepts :-
1) Asymmetric cryptography
① Public key
② Private key

2) Methametical fundamentals
→ Step involved in RSA
① Key Generation
2) Encryption
3) Decryption.

B Diffie Hellman Key Exchange.
- It is a method for two parties to securely generate a shared secret key over an insecure communication channel.
- This shared key can then be used for encrypting communication using symmetric encryption.

- Key Concepts :-
① Asymmetric process for symmetric key
② Discrete logarithm problems.

- Steps in Diffie-Hellman Key :-
1) Agree on public parameters
② Generate private key
③ Compute public keys.
4) Generate the shared secret-

- Security :-
The security of the Diffie-Hellman key exchange relies on the Discrete logarithm problem.

- Vulnerabilities
- Man-in-the-middle attack

- Applications
① TLS / SSL
② IPSec
③ SSH

c) Digital signature

— It is a cryptographic mechanism used to verify the authenticity & integrity of digital msg or documents.

— It is serves the same purpose as a handwritten signature or a stamped seal but it provides far more inherent security.

— Key Concept :-

1) Authentication :-
Ensure the identify of the sender.

2) Integrity :-
Verifies that the message hasn't been tempered with during transaction.

3) Non-repudiation :-
The sender cannot deny having sent the msg because the digital signature binds the msg to the sender private key.

4) How it works :
1) Private Key
2) Public Key

— Steps for Digital Signature Creation :-
① Hashing the msg
② Signing the Hash

— Application :-
1 Secure email
2 S/w distribution
3 Legal docs
4 Cryptocurrencies

— Advantages
1 Security
2 efficiency
3 Legal validity.

R. Ramesh