181240116001
~~Assign~~· Vishwas Acharya

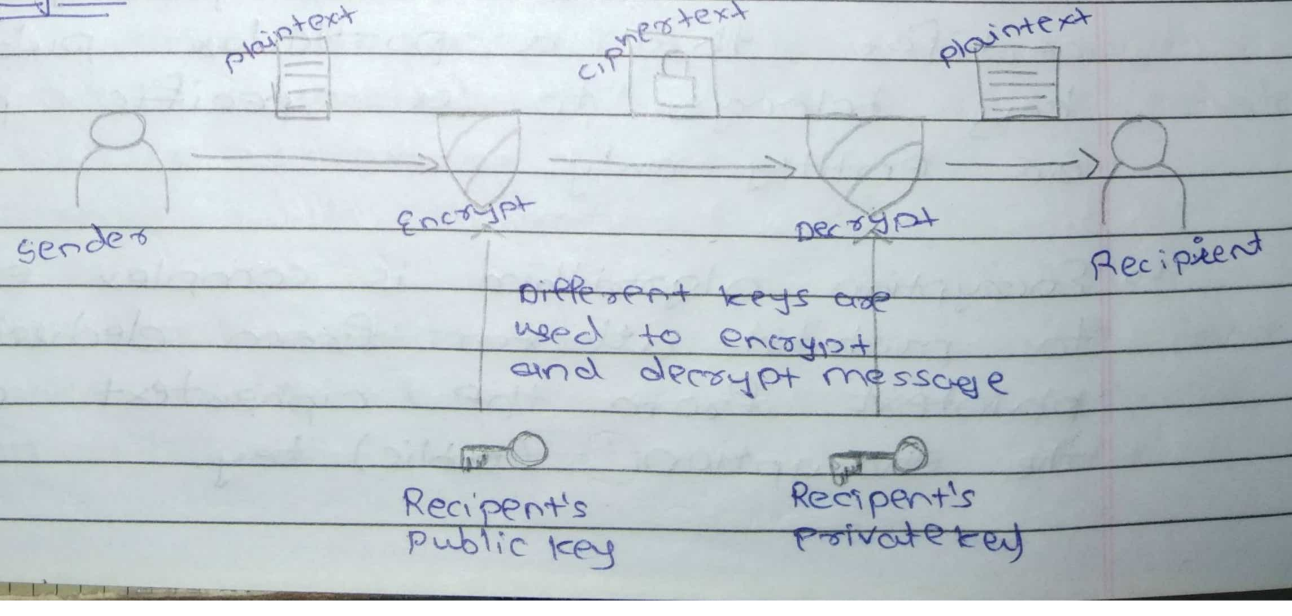
Page No.: 1
Date: / /

CNS
Assignment-4

1) Explain Public key Cryptosystems with applications.

Ans
- Unlike symmetric key cryptography, we do not find historical use of public-key cryptography.
- It is a relatively new concept.
- Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.
- With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale.
- The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems.

- Figures:-



- Public key encryption scheme

↳ Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.

↳ Each receiver possesses a unique decryption key, generally referred to as his private key.

↳ Receiver needs to publish an encryption key, ~~as~~ referred to as his public key.

↳ Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver.

↳ Generally, this type of cryptosystem involves trusted third party which certifes that a particular public key belongs to a specific person or entity only.

↳ Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.

↳ Though private and public keys are related mathematically, it is not be fasible to calaulate the private key from the public key.

↳ In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

- There are three types of Public key Encryption schemes

↳ RSA Cryptosystem.
↳ ElGeamal Cryptosystem
↳ Elliptic Curve Cryptography (ECC)

2) Explain RSA algorithm with example.

Ans - The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key. (i.e. two different, mathematically linked keys).

- As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

- The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.

The following illustration highlights how asymmetric cryptography works:

- **How it works**

↳ The RSA algorithm ensures that the keys, in the above illustration, are as secure as possible.

↳ The following steps highlight how it works:

1. **Generating the keys**

↳ Selecting two large prime numbers, x and y. The prime numbers need to be large so that they will be difficult for someone to figure out.

↳ Calculate $n = x * y$

↳ Calculate the totient function; $\phi(n) = (x-1)(y-1)$

↳ ~~to~~ Select an integer e, such that e is co-prime to $\phi(n)$ and $1 < e < \phi(n)$. The pair of numbers (n, e) makes up the public key.

NOTE: Two integers are co-prime if the only positive integer that divides them is 1.

↳ Calculate d such that $ed = 1 \bmod \phi(n)$. d can be found using the extended euclidean algorithm. The pair (n,d) makes up the private key.

2. ENCRYPTION

↳ Given a plaintext P, represe~~nt~~ted as a number, the ciphertext C is calculated as:

$C = P^e \bmod n$

3. DECRYPTION

↳ Using the private key (n,d) the plaintext can be found using:

$P = C^d \bmod n.$

3) Explain Diffie-Hellman key exchange algorithm with example.

Ans → The purpose of diffie-Hellman algorithm is to enable two users to securely exchange a key that can be used for subsequent encryption of message.

- This algorithm depends for its effectivness on the difficulty of computing discrete ~~algorithms~~. logarithm.

- **Primitive root**

- let p be a prime number
- Then a is a primitive root for p, if the powers of a modulo p generates all integers from 1 to p-1 in some permutation.

$$\boxed{a \bmod p, a^2 \bmod p, \ldots, a^{p-1} \bmod p}$$

- **Discrete Logarithm**

- For any integer b and a primitive root a of prime number p, we can find a unique exponent i such that.

$$\boxed{b = a^i (\bmod p) \text{ where } 0 \leq i \leq (p-1)}$$

- The exponent i is referred as the discrete logarithm of b for the base a, mod p. It expressed as below.

$$\boxed{bdlog_{a,p}(b)}$$

- User A and user B agree on two large prime numbers q and α
- User A and User B can use insecure channel to agree on them.
- User A selects a random integer $X_A < q$ and calculates Y_A

- **Global Public Elements**

↳ q = prime number
↳ α = $\alpha < q$ and α is primitive root of q.

- **User A key Generation**

↳ Select private X_A $\quad X_A < q$
↳ Calculate public Y_A $\quad Y_A = \alpha^{X_A} \bmod q$

- **User B key generation**

↳ Select private X_B $\quad X_B < q$
↳ Calculate public Y_B $\quad Y_B = \alpha^{X_B} \bmod q$

- **Example**

- Alice and bob agrees on a prime number $q = 23$
- $\alpha = 5$ as primitive root of q
- Alice selects a private integer $X_A = 6$
- Alice computes $Y_A = \alpha^{X_A} \bmod q \Rightarrow Y_A = 5^6 \bmod 23 = 8$
- Bob selects a private integer $X_B = 15$
- Bob computes $Y_B = \alpha^{X_B} \bmod q \Rightarrow Y_B =$ ~~15~~ $5^{15} \bmod 23 = 19$
- Alice sends Y_A to Bob and Bob sends Y_B to Alice
- Alice compute key $k = (Y_B)^{X_A} \bmod q \Rightarrow k = (19)^6 \bmod 23$
  $k = 2$
- Bob computes key $k = (Y_A)^{X_B} \bmod q \Rightarrow k = (8)^{15} \bmod 23$
  $k = 2$

4) Explain Man-in-Middle attack in detail.

Ans - When there is an unwanted proxy in the network intercepting and modifying the requests/response, this proxy is called a Man-in-the middle.

- The network then is said to be under a Man in the middle attack.
- The interesting point lies in the fact that this rouge proxy is often misunderstood as a legitimate endpoint in a communication by the other endpoint.

• Example :-

- Suppose you ar connected to a WiFi network and doing a transaction with your bank.
- An attacker is also connected to the same WiFi.
- The attacker does the following:

1. Attacker sends the rogue ARP packets in the network the map the IP address of the access point to the MAC address of attacker's device.

2. Each device connected in the network caches the entry contained in the rogue packets.

3. Your device uses ARP to send the packets destined for your bank's web server to the access point (whith is the default gateway for the network).

4. The packets get sent to the attacker's machine.

5. Attacker can now read and modify the requests contained in the packets before forwarding them.

- This way the attacker is suitabley situated between you and your bank's server. Ever bit of sensitive data that you send to your server including your login password, is visible to the attacker. ARP cache poisoning is one of the many ways to perform an MITM attack; other ways are:

1. DNS Spoofing
2. IP spoofing
3. Setting up a rogue WiFi AP
4. SSL spoofing etc.