Lecture 24 (Network Security)

1 What is Network Security

1. Confidentiality
2. Authentication
3. Message integrity
4. Access and availability

2 Malicious Actions

1. Eavesdropping
2. Impersonation
3. Hijacking
4. Denial of service

3 Basic Idea of Cryptography

Alice uses K_A and sends encrypted message to Bob who uses K_B and decodes the message.

$$m = K_B(K_A(m))$$

3.1 Types of Cryptography

1. Symmetric key - $K_A = K_B = K_S$

- One issue is on how do they agree on the key

1. Public key

- Public encryption key is known to all
- Private decryption key is known only to receiver

3.1.1 Symmetric Key Crypto - DES

1. Data Encryption Standard
2. Block cipher with cipher block chaining - messy implementation and not discussed in detail

3. 56-bit symmetric key and 64-bit plaintext input
4. Brute force decryption is possible within a day

3.1.2 Advanced Encryption Standard - AES

1. Data is processed in 128 bit blocks
2. 128, 192 or 256 bit keys are used
3. Brute force for each key takes 1s on DES and 149 trillion years for AES

3.1.3 Public Key Crypto

1. It should be impossible to compute private key
2. RSA - Rivest, Shamir, Adelson algorithm

3.1.3.1 RSA

1. Choose two large prime numbers p, q (having 1024 bits each)
2. Compute $n = pq, z = (p-1)(q-1)$
3. Choose $e(< n)$ with no common factors with z
4. Choose d such that $ed - 1$ is divisible by z
5. Public key is (n, e) and private key is $(n, d)
6. $c = m^e \mod n$
7. $m = c^d \mod n$
8. We can swap the public and private keys as well

RSA Drawbacks

1. Computation is slow since we need exponentiation of large numbers
2. Therefore, once RSA session is established, symmetric key is shared and encryption is then done using this key which is faster in computation

4 Authentication

1. When a device claims to be Alice, Bob sends a number **nonce** (n-once-in-a-lifetime)
2. Now, Alice sends it back after encrypting it with her private key
3. To verify the same, Bob can now decrypt it using her public key
4. This prevents impersonation but man-in-the-middle can still happen