Unit 3

Symmetric v/s Asymmetric Cryptography

Problem With Symmetric Key

- ***Problem !***
- Suppose sender & receiver may be in different countries.
- ✔ E.g:- Online shopping website
- ❖ How they will exchange the key & agree on it?
- ✔ Physically visit
- ✔ Courier
- ✔ Internet & ask for confirmation.

Not Convenient

- **If Intruder gets the key, he can unlock the things.**
- ***Problem 2***
- Separate/Unique key for each communication is needed.
- ✔ E.g:- A to B & A to C or B to C
- To overcome Interruption Attack

Key Length & Encryption Strength

- The strength of any encryption algorithm lies on:

1. The algorithm used
2. Length of Encryption key.
3. The algorithm said to be strong if it takes more time to find out the key by the hacker.

Application of PKC

- PGP Email Application.
- In communication with Web Server.
- Online Transactions, the communication is encrypted using a *random number* which is generated by the server & send securely.
- Sending secret key.
- Digital signatures

Strength & Weakness of Public Key

Pros

- Key distribution is easy
- Scalable due to that
- Can provide authentication and non-repudiation

Cons

- Very mathematically intense(large key & Complex Algo)
- Slow due to that(huge chunks)
- More computation time.
- Used for small data & msg.
- Misuse of Public Key is possible.
- Known Cipher text Attack is possible.

Comparison

1. Key used for encryption & decryption.
2. Speed of encryption & decryption.
3. Key agreement/exchange/distribution.
4. Number of keys for n participants.
5. Usages

Asymmetric Encryption	Symmetric Encryption
1.Public key Encryption	1.Secret Key Encryption
2.Two key/Different Key	2.One /Same/common key
3.One public One Secret	3.Keep Secret
4.One for Encryption & Other for Decryption	4.Same key for both the operation
5.Slower	5.Faster & Efficient
6. Small Data	6.Large Data
7.No Issues	7. Problem of Key Exchange.

Advantage of Public-key crypto

- Suppose N entities, how can any pair of them establish a secret key?
  - Need **n*(n-1) /2** keys. Where n=No. of parties involved
  - Key management is challenging
- Public-key crypto advantage
  - Each entity only needs to know **N-1** authentic public keys & Private Key

Information Protections by Symmetric Cryptography

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	No
Non-repudiation	No

Table 11-3 Information protections by symmetric cryptography

Information Protections by Asymmetric Cryptography

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	Yes
Non-repudiation	Yes

Table 11-6 Information protections by asymmetric cryptography