“ PUBLIC KEY ENCRYPTION & RSA ”

CHAPTER FOUR

By : Eman Talib Jasim

Department of Information Technology 2018-2019

Contents

Public Key Crypto system

- Objective
  - Reason behind development of public key cryptosystem is to handle most difficult problem associated with symmetric ciphers .
    - Key Distribution .
    - Digital signatures .
  - Public key cryptosystems are the asymmetric ciphers .

- The asymmetric ciphers rely on one key for encryption and different but related key for decryption.

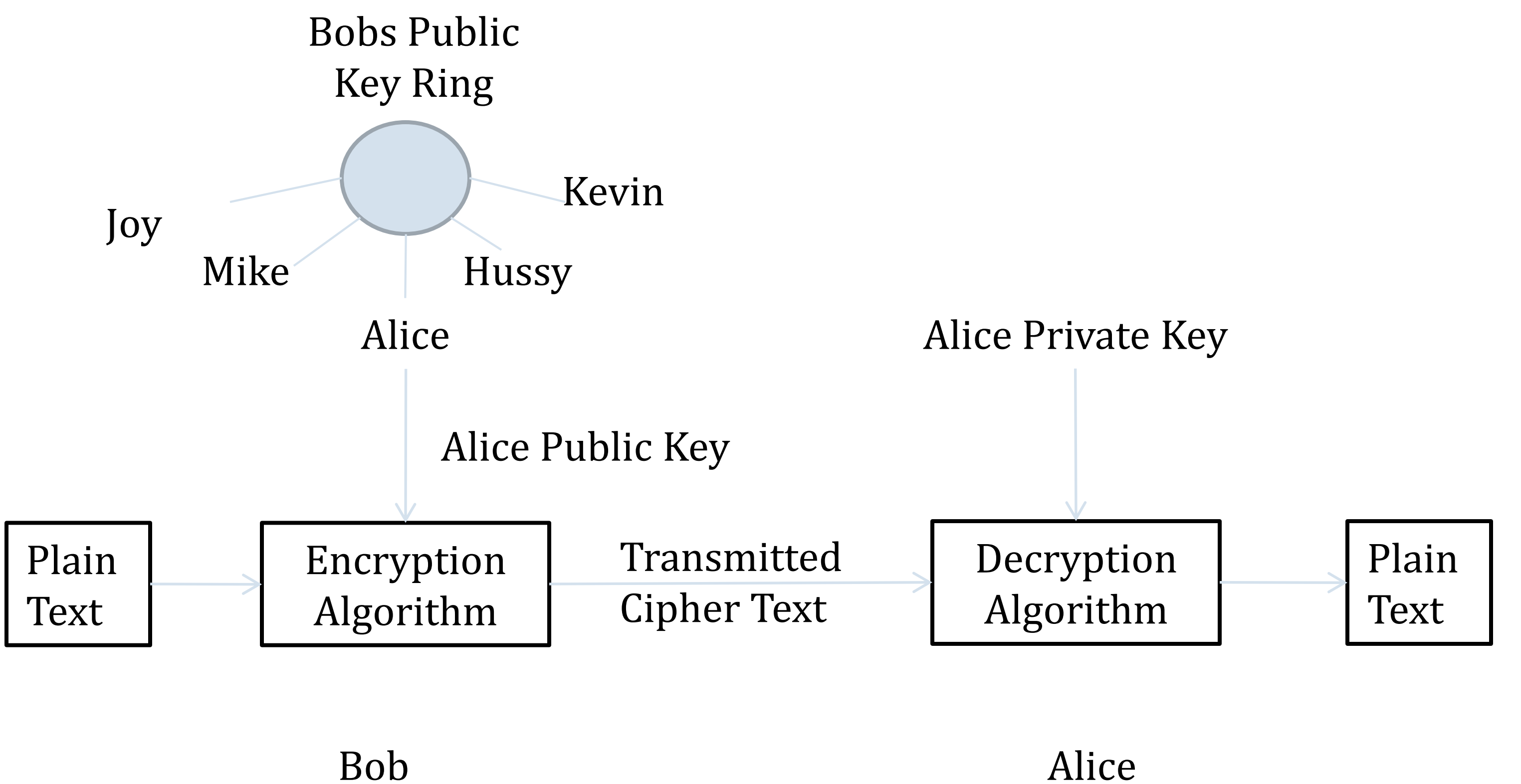
- Characteristics of Public key Encryption
  - It is computationally infeasible to determine the decryption key, if knowledge of cryptographic algorithm and encryption key is given.

Components of Public key Encryption

- **Plaintext**
  - This is the readable message or data that is fed into algorithm as input .
- **Encryption Algorithm**
  - Is the algorithm performs various transformation on the plaintext .
- **Public and Private key**
  - This is pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.
  - The exact transformation performed by the algorithm depend on the public or private key that is provided as input.

- **Cipher text**
  - This is scrambled message produced as output after transformation on plain text.
  - It depends on the plain text and the key .
  - Example: for a given message two different keys will produce two different cipher text.

- **Decryption Algorithm**
  - This algorithm accepts the cipher text and the matching key and produces the original plaintext .



(a) Encryption

- Essential Steps
  - Each user generates a pair of keys to be used for the encryption and decryption of message.
  - Each user places one of two keys in a public register or other accessible file .
    - This is public key .
    - The companion key is kept private .
    - Each user maintains a collection of public keys obtained from others.
    - Example
      - If Bob wishes to send confidential file to Alice, Bob encrypts the file using Alice public key .
      - When Alice receives the encrypted file, Alice decrypts the file using private key.

- In this approach
  - All participants have an access to public keys and have private key (generally generated locally)
  - Private keys are not distributed .
  - As long as private key is protected and secret, incoming communication is secure .
  - At any time user can change its private key and publish companion key for public and replaces its old public key.

- Applications of Public Key Cryptosystem
  - The public key systems are characterized by the use of a cryptographic algorithm with two keys .
    - One held private .
    - One available publically.
  - Depending on application, the sender uses either senders private key or receiver's public key or both to perform some type of cryptographic function .
  - There are three categories of Public cryptosystem
    - Encryption/ Decryption .
    - Digital Signature .
    - Key Exchange .

- Encryption / Decryption
  - The sender encrypts a message with recipient’s public key.
- Digital signature
  - The sender “signs” the message with its private key
  - Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is function of the message.
- Key Exchange
  - Two side cooperate to exchange a session key.
  - Several different approaches are possible, involving the private key(s) of one or both parties.

- Requirements for Public-Key Cryptography.
  - It is computationally easy for party ‘B’ to generate a pair
    - Public Key → $PU_{(b)}$
    - Private key → $PR_{(b)}$
  - It is computationally easy for sender ‘A’, knowing the public key and the message to be encrypted, ‘M’ to generate the corresponding cipher text .
    - $C=E(PU_{(b)}, M)$
  - It is computationally easy for receiver ‘B’ to decrypt the resulting cipher text using private key to recover the original message.
    - $M=D\ (PR_{(b)}, C)=D[PR_{(b)}, E(PU_{(b)}, M)]$

- It is computationally infeasible for an adversary, knowing the public key, PU(b) to determine private key, PR (b)

- It is computationally infeasible for an adversary, knowing the public key, PU(b) and cipher text C to recover original message.

- The two keys can be applied in either order
  - $M=D[PU_{(b)}, E(PR_{(b)},M)]=D[PR_{(b)}, E(PU_{(b)}, M)]$

- Strength and Weakness of Public key
  - Weakness
    - Extremely slow .
    - Costly .
  - Strengths
    - Solves problem of passing the key .
    - Allows establishment of trust context between the parties .

- Comparison between Asymmetric Cipher and Symmetric Ciphers
  - Asymmetric Cipher
    - Public key Encryption .
    - Two keys are used
      - Public key for encryption .
      - Private key for decryption .
    - Generally slower than symmetric ciphers .
    - Public keys are safe to published anywhere (even on internet) because to get a private key from a public key could take hundred years of work.

- Symmetric Ciphers
  - Also known as secret key encryption .
  - One key is used
    - For encryption and decryption .
  - Usually very fast .
  - Keys must be kept secured .

- RSA Algorithm
  - This scheme was devised by Rivest, Shamir and Adlemen.
  - Is the most popular public key encryption method .
  - Key length for RSA is variable .
  - Long key provides more security and short key provides less security but makes the algorithm more efficient .
  - Most commonly used key length is 512 bits (64 byte) .
  - The plain text block must be less than the key length .
  - RSA is much slower than DES .

- Algorithm
  - Generates two large random primes ‘p’ and ‘q’ of approximately equal length such that their product n=pq is of required bit length, and p<>q
    - Let *n=pq* and *m=(p-1) (q-1)*
      - Choose an integer ‘e’ , *1<‘e’<m* such that *gcd(e,m)=1*
      - Compute the secret exponent ‘d’, 1<d<m such that

$$d=e^{-1}(\text{mod } m)$$

$$d \,.\, e \ (\text{mod } m) = 1$$

    - The Public key KPU=(e,n)
    - The Private key KPR=(d,n)

- The values of ‘p’, ‘q’ and ‘m’ should also be kept secret.

- ‘n’ is known as the modulus
- ‘e’ is known as encryption exponent
- ‘d’ is known as decryption exponent

- **Encryption**
  - Sender A does the following
    - Obtains recipient B’s public key (e,n)
    - Represents the plain message as a positive integer ‘M’
    - Computes the cipher text

      $C=M^e \bmod n$
    - Sends Cipher text C to B