Public Key Cryptography

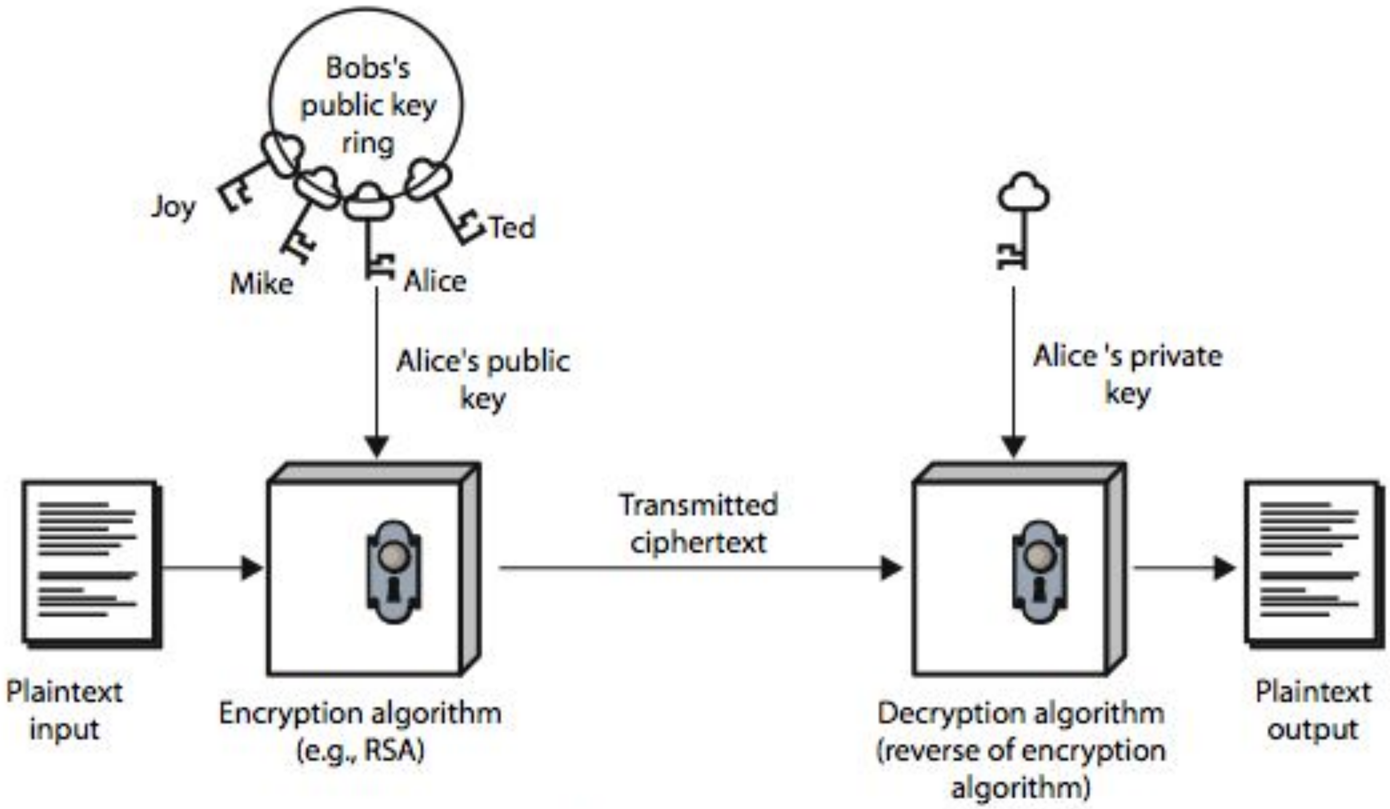
Private-Key Cryptography

- Traditional private/secret/single key cryptography uses one key
- Shared by both sender and receiver
- If this key is disclosed communications are compromised

Public-Key Cryptography

- Public-key/two-key/asymmetric cryptography involves the use of two keys:
  – a public-key, which may be known by anybody, and can be used to encrypt messages
  – a private-key, known only to the recipient, used to decrypt messages, and sign (create) signatures
- is asymmetric because
  – those who encrypt messages or verify signatures cannot decrypt messages or create signatures

Public-Key Cryptography



(a) Encryption

Public-Key Characteristics

- Public-Key algorithms rely on two keys where:
  - It is computationally infeasible to find decryption key knowing only algorithm & encryption key
  - It is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known

General Idea

- Each entity in the community should create its own private and public keys
  - Opponent should not be able to advertise his/her key to the community pretending that it is receiver's public key (manage through Public keys Distribution)
  - Plaintext & ciphertext are treated as integers in asymmetric-key cryptography.

Encryption/Decryption

Encryption & Decryption in asymmetric-key cryptography are mathematical functions: applied over the number representing plaintext & ciphertext

Ciphertext defined as: C= f(Kpublic ,P)

Plaintext defined as: P= g(Kprivate ,C)

(here f and g are two separate function)

‘f’ needs a trapdoor to allow bob to decrypt the message

More on:

Function
Invertible Function
One Way Function : Ex n=p*q
Trapdoor : $y = x^k \bmod n$ (given x, k and n it is easy to calculate y)

RSA

- By Rivest, Shamir & Adleman of MIT in 1977
- Best known & widely used public-key scheme
- Based on two algebraic structure: Ring, Group
- Security due to cost of factoring large numbers (recommended size of prime number 512 bits)

RSA Key Setup

- Each user generates a public/private key pair by:
- Selecting two large primes at random p, q
- Computing their Product $n=p.q$
  - note **$\phi(n)=(p-1)(q-1)$**
- Selecting at random the encryption key e

  where **$1<e<\phi(n)$, $\gcd(e,\phi(n))=1$**
- Solve following equation to find decryption key d

  $e.d=1 \bmod \phi(n)$ and $0\leq d\leq n$
- Publish their public encryption key: $PU=\{e,n\}$
- Keep secret private decryption key: $PR=\{d,n\}$

RSA Use

- to encrypt a message M the sender:
  - obtains public key of recipient PU={e,n}
  - computes: $\mathbf{C = M^e \bmod n}$, where $0 \le M < n$
- to decrypt the ciphertext C the owner:
  - uses their private key PR={d,n}
  - computes: $\mathbf{M = C^d \bmod n}$
- note that the message M must be smaller than the modulus **n** (block if needed)

RSA Example - Key Setup

1. Select primes: $p=17$ & $q=11$
2. Compute $n = pq = 17 \times 11 = 187$
3. Compute $\phi(n)=(p-1)(q-1)=16 \times 10=160$
4. Select e: $\gcd(e,160)=1$; choose $e=7$
5. Determine d: $de=1 \bmod 160$ and $d < 160$ Value is $d=23$ since $23 \times 7=161= 10 \times 160+1$
6. Publish public key $PU=\{7,187\}$
7. Keep secret private key $PR=\{23,187\}$
8. If the plaintext is 88 then C ?.......11

Attacks on RSA

Factorization Attack

- It is infeasible to factor in a reasonable time
- Eve can factor **n** and obtain **p** and **q**
- She can calculate $\phi(n)=(p-1)*(q-1)$
- Eve can calculate **‘d’** (because **e** is public)
- Now Eve can decrypt any encrypted message.
- Note: factoring an integer of 1024 bit would take an infeasible long period of time

Chosen-Ciphertext attack

- Assume Alice creates ciphertext **C** and sends **C** to Bob.
- Eve intercept **C** and uses the following steps to find P:
    1. Eve chooses a random integer **X** in Z*
    2. Eve calculate **y**= **C** * **X**^{e} mod n

Eve sends **y** to Bob for decryption and get **Z** = y^d mod n

(chosen-ciphertext attack)

Eve can easily find P:

- $Z = y^d \bmod n = (C * X^e)^d \bmod n = (C^d * X^{ed}) \bmod n$
  $= (C^d * X) \bmod n = (P*X) \bmod n$
- $Z = (P*X) \bmod n$ -> $\mathbf{P = Z * X^{-1} \bmod n}$

(Eve can used extended Euclidean algorithm to find multiplicative inverse of X)

Cycling attack

- Ciphertext is a permutation of the plaintext (They are integers from the same interval (0 – n-1))
- Continuous encryption of the ciphertext will eventually result in the plaintext.

Hybrid Cryptosystem

- A hybrid cryptosystem can be constructed using any two separate cryptosystems:
- a **key encapsulation scheme**, which is a **public-key cryptosystem**, and
- a **data encapsulation scheme**, which is a **symmetric-key cryptosystem**.
- To encrypt a message addressed to Alice in a **hybrid cryptosystem**, Bob does the following:
- Obtains Alice's public key.
- **Generates a fresh symmetric key** for the data encapsulation scheme.
- **Encrypts the message** under the data encapsulation scheme, **using** the **symmetric key** just generated.
- **Encrypt the symmetric key** under the key encapsulation scheme, **using Alice's public key.**
- Send both of these encryptions to Alice.
- To decrypt this hybrid ciphertext, Alice does the following:
- Uses her private key to decrypt the symmetric key contained in the key encapsulation segment.
- Uses this symmetric key to decrypt the message contained in the data encapsulation segment.