

Public Key Cryptosystem

Contents:

- What is public key cryptosystem.
- Public key vs secret key algorithms.
- RSA public key system.

A taxonomy of Cryptosystems

- Ciphers in terms of encryption process
 - Stream ciphers (symmetric key only)
 - Block ciphers
 - Symmetric key or secret key block ciphers
 - Asymmetric key or public key ciphers
- Ciphers in terms of number of keys
 - Symmetric key cipher (secret key cipher)
 - Stream cipher
 - Block cipher
 - Asymmetric key cipher (public key cipher)

What is public key cryptography

- Has a pair of keys, one is public and the other is private.
- Given a public key, it is computationally infeasible to find the corresponding private key.
- Public key is used for message encryption, can be done by anyone in public.
- Private key is used for owner to decrypt encrypted messages correctly.
- Public keys can be put in a publicly accessible directory like telephone yellow pages.
- Some of the public key systems can be used for digital signatures.

Public Key v.s. Secret Key Cryptosystem

- Secret key cryptosystem normally employs faster algorithms than those in public key systems.
- Public key system is more convenient to use as no pre-established common key is required.
- Public key system should be used in conjunction with secret key system.
 - Public key algorithm is used for encryption of **session keys** which are then used for message encryption using secret key algorithms.
- **Note:** Secret key system = Symmetric key system.
Public key system = Asymmetric key system.

How Can Secret Information Be Transmitted Through Public Channels

- Secret key distribution can be a problem. (cost v.s. security)
- Diffie-Hellman key exchange 1977:

Common knowledge to A and B :

p , a large prime, and $g < p$, a random number.

$A \longrightarrow B$: $\alpha = g^{r_1} \bmod p$, where r_1 is a random number.

$B \longrightarrow A$: $\beta = g^{r_2} \bmod p$, where r_2 is random number.

A compute: $K_1 = \beta^{r_1} \bmod p$.

B compute: $K_2 = \alpha^{r_2} \bmod p$.

Common key: Then $K_1 = K_2$ is the common key.

The security of Diffie-Hellman key exchange.

- **Discrete logarithm problem:**
Given p , g and $G = g^x \bmod p$, how to compute x .
- It is a hard problem.

Design Principle of Public Key System

- Use one-way trapdoor function. A one-way trapdoor function $f_\lambda(x)$ satisfies the following properties:
 - One-way:** Given x , it is trivial to compute $y = f_\lambda(x)$. Given y , without knowing the trapdoor parameter λ , it is computationally infeasible to find x .
 - Invertible:** Given y , with the knowledge of λ , it is easy to find x .
- When a trapdoor is used as public key system.
 - Encryption is $y = f_\lambda(x)$.
 - Decryption is finding x given y , which can be done only by someone knowing the secret λ .

RSA Public Key System

- Invented by Rivest, Shamir, and Adleman in 1979 (paper and patent for twenty years).
- It is a typical example of how *pure* mathematics can be used directly in the commercial world.
- It revived the mathematical branch — *Number Theory*. Today *Computational Number Theory* is very popular.
- It is based on the computational infeasibility of integer factorization. E.g. Given a composite number 6, how to find its prime factors 3 and 2 such that $2 \times 3 = 6$.

RSA

Set up: User to set up system before use.

- choose large primes p and q , set $n = pq$;
- choose random number e satisfying $\gcd(e, (p-1)(q-1)) = 1$, $1 < e < (p-1)(q-1)$; **public key:** (e, n) ;
- compute d such that $ed \bmod (p-1)(q-1) = 1$; (e and d are called inverses of each other in the sense of modulo $(p-1)(q-1)$.); **private key:** (d, n) .

Message: A number $m < n$.

- Chop message into small blocks with the size of each block being less than that of n , in binary representation.

Encryption: $c = m^e \bmod n$.

Decryption: $m = c^d \bmod n$.

RSA: An Example

- ▶ $p = 13, q = 23, n = pq = 299,$
 $(p - 1)(q - 1) = 264.$
- ▶ $e = 5, d = 53.$ (Check:
 $ed \bmod (p - 1)(q - 1) =$
 $265\%264 = 1!!)$
- ▶ Message $m = (16, 29, 123, 234).$
- ▶ Encryption: $c = (282, 48, 223, 104).$
 - ▶ $16^5 \bmod 299 = 282.$
 - ▶ $29^5 \bmod 299 = 48.$

- ▶ $123^5 \bmod 299 = 223.$
- ▶ $234^5 \bmod 299 = 104.$
- ▶ Decryption: $c^d \bmod n = m.$
 - ▶ $282^{53} \bmod 299 = 16.$
 - ▶ $48^{53} \bmod 299 = 29.$
 - ▶ $223^{53} \bmod 299 = 123.$
 - ▶ $104^{53} \bmod 299 = 234.$

RSA Security

- If factorization of n , the public modulus, can be done, then RSA system is broken.
- If RSA is broken, no one can prove the factorization of n can be done.
- Breaking RSA system is no harder than factorization of n , and it is publicly *believed* that it is no easier either.
- Practical use: p and q are of 512 bits long, or 1024 bits long for high confidential message encryption.

RSA Factoring Challenge

- RSA Factoring Challenge was sponsored by RSA Laboratories, to learn about the actual difficulty of factoring large numbers of the type used in RSA keys. It involved a set of eight challenge numbers, ranging in size from 576 bits to 2048 bits. The challenge ended in 2007.
- On December 3, 2003, a team of researchers in Germany and other countries announced the factoring of RSA-576, a 576-bit or 176-digit number. Prize money: US\$10,000.
- The next challenge number RSA-640, a 193-digit number, was factored on November 2, 2005. Prize money: US\$20,000.
- The challenge number next to this is RSA-704, a 212-digit number. This is not yet factored. Prize money was: US\$30,000.

RSA versus DES

- RSA is about 1000 times slower than DES.
- DES is based on *tricky* design (as are other block ciphers such as IDEA), while RSA is based on hardness of mathematical problems (as are other public key algorithms).
- DES is suitable for bulk message encryption, and RSA suits for short message encryption.

Use [RSA] In Conjunction With [DES/AES]

- Use RSA (or any other public key system) to encrypt *session keys*. (A session key is a key temporarily used only for a communication session.)
- Use DES (or any other secret key system) for real message encryption during a session (using that session key).
- No common secret key is required as would be the case when DES is used alone.
- Speed of encryption and decryption can be roughly the same as DES, provided that the length of message is far larger than that of the session key (normally 128 bits).
- Note: We use DES here, but it could be any secret key block cipher.

Other Public Key Systems

- ElGamal: Discrete logarithm based system.
- Rabin: Similar to RSA, with security equivalent to factorization.
- McEliece public key cryptosystem: Based on error-correcting codes.
- There are many many other public key cryptosystems in public literature.

Where Can Public Key Systems Be Used?

- Together with a secret key cipher (as stated above).
- Largely used for digital signatures (next lecture).
Note that some public key systems need to be modified to provide signature functionalities.
- In E-commerce, digital signatures are, in some sense, more important than simple encryption.

Is Data Encryption Good Enough for E-Commerce?

- Symmetric key ciphers are fast, but a common secret key needs to be agreed in advance before decryption can be done in the other end.
- Asymmetric key ciphers are convenient to use but a bit slow.
- Combination of symmetric key cipher and asymmetric key cipher gains speed and convenience. It is perfect for data encryption.
- But security in E-commerce is not just about data confidentiality! It is more about **entity authentication**.
- Next lecture is about digital signature, a fundamental mechanism to achieve entity authentication.