



# *Cryptography*

W.C. Shiu

wcshiu@hkbu.edu.hk

Department of Mathematics  
Hong Kong Baptist University



Cryptography – p. 1/1



## *Crytosystem*

Encryption function  $E$ : transfers plaintext to  
ciphertext

Decryption function  $D$ : transfers ciphertext to  
plaintext

$D$  is the inverse function of  $E$  and vice versa.



Cryptography – p. 2/1

# Public Key Cryptosystem

Each user provide a public key, i.e., publish the encryption function  $E$ .

Keep the decryption function  $D$  in security.

Suppose Mary wants to send a plaintext  $m$  to Peter.

1. She uses Peter's encryption function  $E_P$  to change the message  $m$  to  $c = E_P(m)$ .
2. When Peter receives the ciphertext message  $c$ . He uses his decryption function transfers the message to  $D_P(c) = D_P(E_P(m)) = m$ .

# A Public Key Cryptosystem – RSA Cryptosystem

Suppose a user's public key is  $(n, b)$ .

The security of RSA is based on the hope that the encryption function  $E(m) = m^b \pmod n$  is one-way, so it will be computational infeasible for any opponent to decrypt a ciphertext.

# Number Theory

## – Some Basic Knowledge

Suppose  $a$  and  $m$  are relative prime, i.e.,  $(a, m) = 1$ .  
Then there are integers  $s$  and  $t$  such that  $as + mt = 1$ .  
Here  $s$  and  $t$  can be found by using Euclidean algorithm.

Suppose  $n$  is an integer greater than 1. Let  $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$  be the ring of the complete residue system modulo  $n$ .

Theorem: Let  $m \geq 2$ . Suppose  $(a, m) = 1$ . Then there is a unique  $b \in \mathbb{Z}_m$  such that  $ab \equiv 1 \pmod{m}$ .  $b$  is called the **inverse** of  $a$  and is denoted by  $a^{-1}$ .

# Number Theory

## – Some Basic Knowledge

Let  $\phi(m)$  denote the number of positive integers less than or equal to  $m$  that are relatively prime to  $m$ . This function is called the **Euler  $\phi$ -function**.

Euler's Theorem: If  $(a, m) = 1$ , then  $a^{\phi(m)} \equiv 1 \pmod{m}$ .

## ***RSA Cryptosystem***

Let  $n = pq$ , where  $p$  and  $q$  are primes (very large). Choose a unit  $a \in \mathbb{Z}_{\phi(n)}$  (i.e.,  $(a, \phi(n)) = 1$ ). Then there is a  $b$  such that  $ab \equiv 1 \pmod{\phi(n)}$ . Thus, we have  $ab = t\phi(n) + 1$  for some  $t \geq 1$ . Suppose  $x \in \mathbb{Z}_n^*$ , the set of units of  $\mathbb{Z}_n$ . Then

$$\begin{aligned}(x^b)^a &\equiv x^{t\phi(n)+1} \pmod{n} \\ &\equiv (x^{\phi(n)})^t x \pmod{n} \\ &\equiv x \pmod{n}.\end{aligned}$$

We leave an exercise for you to show that

$(x^b)^a \equiv x \pmod{n}$  if  $x \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$ .

Cryptography – p. 7/1

## ***RSA Cryptosystem***

In order to setup the system, we follow the following steps

1. Generate two large primes  $p$  and  $q$ .
2. Compute  $n = pq$  and  $\phi(n) = (p - 1)(q - 1)$ .
3. Choose a random number  $b$  ( $0 < b < \phi(n)$ ) such that  $(b, \phi(n)) = 1$ .
4. Compute  $a = b^{-1} \pmod{\phi(n)}$  using the Euclidean algorithm.
5. Publish  $(n, b)$  as public key.

In practice,  $n$  is very large. Using the best algorithms known and fastest computers, it would

Cryptography – p. 8/1



## Example 1

Suppose Peter chooses  $p = 101$  and  $q = 113$ .  
Then  $n = 11413$  and  
 $\phi(n) = 100 \times 112 = 11200 = 2^6 5^2 7$ . Choose  $b$   
which is not divisible by 2, 5 or 7.

In practice, Peter will not factor  $\phi(n)$ . He will  
verify that  $(\phi(n), b) = 1$  using the Euclidean  
algorithm.



## Example 1

Suppose Peter chooses  $p = 101$  and  $q = 113$ .  
Then  $n = 11413$  and  
 $\phi(n) = 100 \times 112 = 11200 = 2^6 5^2 7$ . Choose  $b$   
which is not divisible by 2, 5 or 7.

Suppose Peter chooses  $b = 3533$ . Then by  
Euclidean algorithm he will get  $a = b^{-1} = 6597$   
mod 11200.



## Example 1

Peter's secret key is  $a = 6597$ . Peter publishes  $n = 11413$  and  $b = 3533$  in a directory as a public key.

Suppose Mary wants to send the plaintext 9726 to Peter. She computes

$$9726^{3533} \equiv 5761 \pmod{11413}$$

and sends the ciphertext 5761 over the channel.

When Peter receives the ciphertext 5761, he uses his secret key to compute

$$5761^{6597} \equiv 9726 \pmod{11413}.$$

Cryptography – p. 9/1

*Possible plaintext message units*  
 $\neq$  *possible ciphertext message units*

Suppose we are working in an  $N$ -letter alphabet. Let  $k < l$  be suitably chosen positive integers, such that for example  $N^k$  and  $N^l$  have approximately 200 decimal digits.

We take as our plaintext message units all blocks of  $k$  letters, which we regard as  $k$ -digit base- $N$  integers.

Similarly take ciphertext message units to be blocks of  $l$  letters in our  $N$ -letter alphabet.

Then each user must choose his/her large primes  $p$  and  $q$  so that  $n = pq$  satisfies

$$N^k < n < N^l.$$

Cryptography – p. 10/1

## Example 2

Let  $N = 26$ ,  $k = 3$  and  $l = 4$ . Suppose we want to send the message "YES" to a user  $A$  with public key  $(n_A, e_A) = (46927, 39423)$ . Then we find the numerical equivalent of "YES":

$$24 \times 26^2 + 4 \times 26 + 18 = 16346$$

and compute  $16346^{39423} \equiv 21166 \pmod{46927}$ .

$$21166 = 1 \times 26^3 + 5 \times 26^2 + 8 \times 26 + 2$$

this is equivalent of "BFIC".

## Example 2

Let  $N = 26$ ,  $k = 3$  and  $l = 4$ .

$$21166 = 1 \times 26^3 + 5 \times 26^2 + 8 \times 26 + 2$$

this is equivalent of "BFIC".

The user  $A$  knows the secret key  $(n_A, d_A) = (46927, 26767)$ .

So  $A$  computes  $21166^{26767} \equiv 16346 \pmod{46927}$  and get the message "YES".

## Numerical Signature

在進行秘密通訊中，如何才能鑒別收方收到的訊息確實是發方傳出的呢？

且發方如何確保內容沒有被收方竄改呢？

銀行  $B$  在網上收到用戶  $A$  說要轉帳十萬圓，那麼銀行必須要確定該訊息是否由  $A$  發出。

同時，如果  $A$  事後否認曾發過此訊息，銀行必須能夠提出證明這訊息確實由  $A$  發出。

## Numerical Signature

Suppose user  $A$  wants to send a signed message  $m$  to user  $B$ . He uses the following steps:

1.  $A$  uses his own encryption function to change the plaintext to  $s = E_A(m)$ .
2.  $A$  uses the public key of user  $B$  to transfer  $s$  to be  $E_B(s) = E_B(E_A(m))$ . And then sends to  $B$ .
3. When  $B$  receives the ciphertext message  $E_B(s)$ , by using her decryption function transfers the message to  $D_B(E_B(s)) = s$ .
4.  $B$  uses the public key of  $A$  to transfer  $s$  to  $D_A(s) = D_A(E_A(m)) = m$ .