

# Introduction to Cryptology

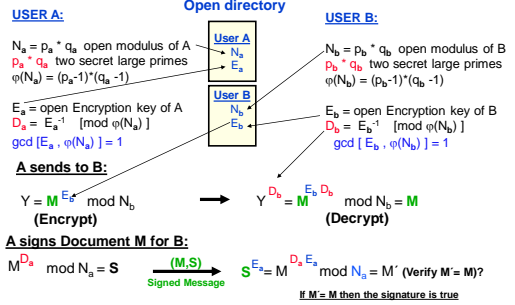
## Tutorial-08 RSA Public-Key Secrecy and Signature System

09.05.2023, v43

Page: 1

1

## Design Summary for RSA Public Key Secrecy and Signature



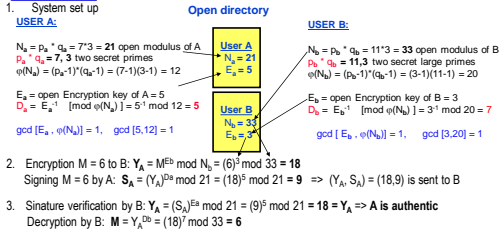
Page: 2

2

### Problem 8-1:

- Set up an RSA Public-key directory for two users A and B using the prime numbers 7,3 and 11,3 respectively. Use the open keys 5, 3 for A and B respectively.
- User A Encrypts the message  $M = 6$  to get the cryptogram  $Y_A$  and signs  $Y_A$  to generate  $S_A$  and sends both cryptogram  $Y_A$  and signature  $S_A$  to B.
- Let user B verify the signature of A and decrypt the message.

### Solution 8-1:



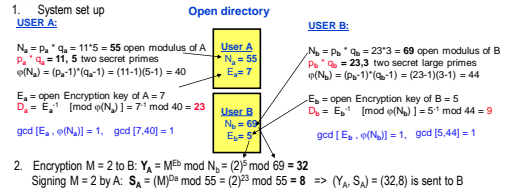
Page: 3

3

### Problem 8-2:

- Set up an RSA Public-key directory for two users A and B using the prime numbers 11,5 and 23,3 respectively. Use the open keys 7, 5 for A and B respectively.
- User A encrypts the message  $M = 2$  to send the cryptogram  $Y_A$  to B and signs  $M$  to generate his signature  $S_A$ . Compute  $Y_A$  and  $S_A$  sent to B.
- Decrypt the message at user's B site and verify user A's signature  $S_A$ .  
 User B signs the received message and sends it back to A. Compute his signature  $S_B$ .
- In 2, M can be revealed by any other user by decrypting  $S_A$  using the open key  $E_a$ . Propose a possible solution to counteract that possibility and keep M secret.

### Solution 8-2:



Page: 4

4

### Solution 8-2 cont.:

- Decryption by B:  $M = Y_A^{D_b} = (32)^9 \pmod{69} = 2$   
 Signature verification by B:  $M = (S_A)^{E_b} \pmod{N_b} = (8)^5 \pmod{69} = 2 = M \Rightarrow$  A is authentic  
 Signing  $M = 2$  by B:  $S_B = (M)^{D_b} \pmod{N_b} = (2)^9 \pmod{69} = 29 \Rightarrow (S_B) = 29$  is sent to A
- One possibility is to encrypt  $S_B$  as well using  $E_a$ . That is  $Y_{S_B} = (S_B)^{E_a} \pmod{N_a} = 8^5 \pmod{55} = 13$ .  
 User B can then decrypt  $Y_{S_B}$  to get the signature and then check it.

Page: 5

5

### Problem 8-3:

An RSA system using the public modulus  $m = 1243$ . The public encryption key was 27. It was possible through a security gap in the computer operating system to find out that Euler function is 1120.

- Compute the two prime factors  $p$  and  $q$  of  $m$
- Break the system and decrypt a received cryptogram  $Y = 7$

### Solution 8-3:

- $\varphi(m) = (p - 1)(q - 1) = m - p - q + 1 \Rightarrow s = (p + q) = m - \varphi(m) + 1$   
 $s = 1243 - 1120 + 1 = 124$   
 $m = p \cdot q = 1243$

$$p \text{ or } q = (s \pm \sqrt{s^2 - 4m}) / 2 = (124 \pm \sqrt{124^2 - 4 \times 1243}) / 2$$

$$\Rightarrow p = 113, q = 11$$

- Decryption if the open encryption key  $E = 27$ :

$$D = E^{-1} \pmod{\varphi(m)}$$

$$\text{that is } D = 27^{-1} \pmod{1120} = 83$$

$$[27^{-1} \text{ is computed by the extended gcd algorithm } \gcd(1120, 27) = 1]$$

$$\Rightarrow 27 \cdot 83 = 2241$$

$$M = Y^D = (7)^{83} \pmod{1243} = 662$$

Page: 6

6

**Problem 8-4:** A RSA cryptosystem with two users A and B having the secret prime number pairs for A: 13 and 7 and for B: 17 and 3 is used.

- Find out the adequate open key of user A from the following list of integers: [21, 18, 11]. Compute the corresponding secret key for user A.
- Find out the adequate open key of user B from the following list of integers: [26,21,22]. Compute the corresponding secret key for user B.
- User B encrypts the message  $M = 3$ , and send the resulting cryptogram  $Y_B$  to A. User B then signs the cryptogram  $Y_B$  and generates the signature  $S_B$ . Compute  $Y_A$  and  $S_B$ .
- Decipher the cryptogram  $Y_A$  on user A's site and verify the Signature  $S_B$ .
- User A signs the received message M and sends his signature  $S_A$  back to B. Compute the signature  $S_A$ .
- How many open keys are possible for each user?

7

**Solution 8-4:**

- Find out the adequate open key of user A from the following list of integers: [21, 18, 11]. Compute the corresponding secret key for user A.

$$N_A = 13 * 7 = 91, \phi(N_A) = (13-1)(7-1) = 72$$

$$\text{gcd}[E_A, \phi(N_A)] = 1 \Rightarrow \text{select 11 as gcd}(72,11) = 1$$

$$E_A = 11$$

$$D_A = -13 \text{ mod } 72 = 59 \text{ (see computation below)}$$

$$D_A = 11^{-1} \text{ mod } 72 = -13 = 72-13 = 59$$

$n_1$	$n_2$	$b_1$	$b_2$	q	r
72	11	0	1	6	6
11	6	1	-6	1	5
6	5	-6	7	1	1
5	1	7	-13	5	0

- Find out the adequate open key of user B from the following list of integers: [26,21,22]. Compute the corresponding secret key for user B.

$$N_B = 17 * 3 = 51, \phi(N_B) = (17-1)(3-1) = 32$$

$$\text{gcd}[E_B, \phi(N_B)] = 1 \Rightarrow \text{select 21 as gcd}(32,21) = 1$$

$$E_B = 21$$

$$D_B = -3 \text{ mod } 32 = 29 \text{ (see computation below)}$$

$$D_B = 21^{-1} \text{ mod } 32 = -3 = 32-3 = 29$$

$n_1$	$n_2$	$b_1$	$b_2$	q	r
32	21	0	1	1	11
21	11	1	-1	1	10
11	10	-1	2	1	1
10	1	3	-3	10	0

8

- User B encrypts the message  $M = 3$ , and send the resulting cryptogram  $Y_B$  to A. User B then signs the cryptogram  $Y_B$  and generates the signature  $S_B$ . Compute  $Y_A$  and  $S_B$ .

$$Y_A = (M)^{E_A} \text{ mod } N_A \quad S_B = (Y_B)^{D_B} \text{ mod } N_B$$

$$Y_A = (3)^{11} \text{ mod } 91 = 61 \quad S_B = (61)^{29} \text{ mod } 51 = (10)^{29} = 28$$

- Decipher the cryptogram  $Y_A$  on user A's site and verify the Signature  $S_B$ .

**Decryption:**  $M = (Y_A)^{D_A} \text{ mod } N_A$   
 $M = (3)^{11 \cdot 59} \text{ mod } 91$   
 $M = 3^{649 \text{ mod } 72} \text{ mod } 91 = 3^1$

**Verification:**  $(S_B)^{E_B} \text{ mod } N_B = Y_A \text{ mod } N_B$   
 $(28)^{21} \text{ mod } 51 = 61 \text{ mod } 51$   
 $61^{609 \text{ mod } 32} \text{ mod } 51 = 10$   
 $61^1 \text{ mod } 51 = 10$   
 $10 = 10 \Rightarrow \text{signature is authentic!}$

- User A signs the received message M and sends his signature  $S_A$  back to B. Compute the signature  $S_A$ .

$$S_A = (M)^{E_A} \text{ mod } N_A$$

$$S_A = (3)^{11} \text{ mod } 91 = 61$$

- How many open keys are possible for each user?  
**# of keys for user A =  $\phi(\phi(N_A)) = \phi(72) = \phi(2^2 \cdot 3^2) = 72(1-1/2)(1-1/3) = 24$  keys**  
**# of keys for user B =  $\phi(\phi(N_B)) = \phi(32) = \phi(2^5) = 32(1-1/2) = 16$  keys**

9

**Problem 8-5:** Assume having a setup of RSA cryptosystem with two peers Alice (A) and Bob (B) having the secret prime number pairs (11,23) and (31,7) respectively.

- Choose the appropriate open key  $E_A$  and  $E_B$  from the following lists. List (A) = {11, 220, 37} and list (B) = {9,22,11} respectively. Compute the corresponding secret keys  $D_A$  and  $D_B$  respectively.
- Bob enciphers the message  $M = 12$  which should be sent to Alice as the cryptogram  $C_B$ . In a further step Bob signs  $M^3$  to generate the signature  $S_B$  and sends it to Alice. Calculate  $C_B$  and  $S_B$ .
- Decipher the cryptogram  $C_B$  on Alice's side.
- Verify the signature  $S_B$  on Alice's side.
- Alice signs the value  $M^3 \text{ mod } N_A$  and sends her signature  $S_A$  back to Bob. Calculate the signature  $S_A$ . Verify  $S_A$  on Bob's side.
- How many public key pairs are selectable for Alice and how many for Bob.
- Why is the system not secure if M is signed instead of  $M^3$ ?

10

**Solution 8-5:**

- Set up Alice

$$N_A = 11 * 23 = 253, \phi(N_A) = (11-1)(23-1) = 220$$

$$\text{gcd}[E_A, \phi(N_A)] = 1 \Rightarrow \text{select 37 as gcd}(220,37) = 1$$

$$E_A = 37$$

$$D_A = -107 \text{ mod } 220 = 113 \text{ (see computation below)}$$

$$D_A = 37^{-1} \text{ mod } 220 = -107 + 220 = 113$$

$n_1$	$n_2$	$b_1$	$b_2$	q	r	INVERSE VALUE	GCD
220	37	0	1	5	35		
37	30	1	-5	1	7		
30	2	-14	5	6	2		
2	-1	18	-6	-10	2		
						INVERSE: -107	GCD: 1

Set up Bob

$$N_B = 31 * 7 = 217, \phi(N_B) = (31-1)(7-1) = 180$$

$$\text{gcd}[E_B, \phi(N_B)] = 1 \Rightarrow \text{select 11 as gcd}(180,11) = 1$$

$$E_B = 11$$

$$D_B = -49 \text{ mod } 180 = 131 \text{ (see computation below)}$$

$$D_B = 11^{-1} \text{ mod } 180 = -49 + 180 = 131$$

$n_1$	$n_2$	$b_1$	$b_2$	q	r	INVERSE VALUE	GCD
180	11	0	1	16	4		
11	4	1	-16	2	3		
4	3	-1	16	3	1		
3	1	-2	3	3	0	INVERSE: -49	GCD: 1

11

**Solution 8-5 cont.:**

- Encryption  $M = 12$  to Alice:

$$C_B = (M)^{E_B} \text{ mod } N_B \quad S_B = (M^3)^{D_B} \text{ mod } N_B$$

$$C_B = (12)^{11} \text{ mod } 217 = 243 \quad S_B = (12^3)^{131} \text{ mod } 217 = 209$$

- Decryption by Alice:

$$M = (C_B)^{D_A} \text{ mod } N_A \Rightarrow M = (243)^{113} \text{ mod } 253 = 12$$

- Signature Verification by Alice:

check if:  $(S_B)^{E_B} \text{ mod } N_B = M$

$$(209)^{11} \text{ mod } 217 = 209 = M^3 \text{ mod } N_B = 12^3 \text{ mod } 217 \Rightarrow \text{signature is authentic!}$$

- 

Signing  $M^3$  by Alice:  $S_A = (M^3)^{D_A} \text{ mod } N_A \Rightarrow S_A = (12^3)^{113} \text{ mod } 253 = 188$

Signature Verification by Bob:  $M^3 \text{ mod } N_A = (S_A)^{E_A} \text{ mod } N_A = (188)^{37} \text{ mod } 253 = 210 = 12^3 \text{ mod } 253 = M^3 \text{ mod } N_A \Rightarrow \text{signature is authentic!}$

- # of keys for user A =  $\phi(\phi(N_A)) = \phi(220) = \phi(2^2 * 5 * 11) = 220(1-1/2)(1-1/5)(1-1/11) = 80$  keys  
# of keys for user B =  $\phi(\phi(N_B)) = \phi(180) = \phi(2^2 * 3^2 * 5) = 180(1-1/2)(1-1/3)(1-1/5) = 48$  keys

12

**Solution 8-5 cont.:**

7. The system is insecure as if A or B sign M, as the public key of the sender allows anybody to reveal M, that is M is not kept secret

Signing an exponentiated version of M makes this kind of attack impossible, because the attacker will get a value that correspond to  $M^3 \bmod N$  and there is no algorithm to compute the Cubic root modulo a composite m without factoring N (as in Rabin-lock). That is, if the prime factors p and q for N are not known then  $M^3 \bmod N$  is a one-way function ( $N = p \cdot q$ ) if p and q are not known.