Introduction to Cryptology

Tutorial-08

RSA Public-Key Secrecy and Signature System

09.05.2023, v43

1

Design Summary for RSA Public Key Secrecy and Signature

Open directory

User A	User B
N_a	N_b
E_a	E_b

USER A:

$N_a = p_a * q_a$ open modulus of A
$p_a * q_a$ two secret large primes
$\varphi(N_a) = (p_a-1)*(q_a-1)$

E_a = open Encryption key of A
$D_a = E_a^{-1}$ [mod $\varphi(N_a)$]
gcd [E_a , $\varphi(N_a)$] = 1

USER B:

$N_b = p_b * q_b$ open modulus of B
$p_b * q_b$ two secret large primes
$\varphi(N_b) = (p_b-1)*(q_b-1)$

E_b = open Encryption key of B
$D_b = E_b^{-1}$ [mod $\varphi(N_b)$]
gcd [E_b , $\varphi(N_b)$] = 1

A sends to B:

$Y = M^{E_b} \bmod N_b$ **(Encrypt)** $\longrightarrow$ $Y^{D_b} = M^{E_b D_b} \bmod N_b = M$ **(Decrypt)**

A signs Document M for B:

$M^{D_a} \bmod N_a = S$ $\xrightarrow{(M,S)}$ $S^{E_a} = M^{D_a E_a} \bmod N_a = M'$ **(Verify M´= M)?**

Signed Message

If M´= M then the signature is true

2

Problem 8-1:

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.
2. User A Encrypts the message M = 6 to get the cryptogram Y_A and singes Y_A to generate S_A and sends both cryptogram Y_A and signature S_A to B.
3. Let user B verify the signature of A and decrypt the message.

Solution 8-1:

1. System set up

Open directory

User A	User B
$N_a = 21$	$N_b = 33$
$E_a = 5$	$E_b = 3$

USER A:

$N_a = p_a * q_a = 7*3 = \mathbf{21}$ open modulus of A
$p_a * q_a = \mathbf{7, 3}$ two secret primes
$\varphi(N_a) = (p_a-1)*(q_a-1) = (7-1)(3-1) = 12$

E_a = open Encryption key of A = 5
$D_a = E_a^{-1}$ [mod $\varphi(N_a)$] = 5^{-1} mod 12 = **5**

gcd [E_a , $\varphi(N_a)$] = 1, gcd [5,12] = 1

USER B:

$N_b = p_b * q_b = 11*3 = \mathbf{33}$ open modulus of B
$p_b * q_b = \mathbf{11,3}$ two secret large primes
$\varphi(N_b) = (p_b-1)*(q_b-1) = (3-1)(11-1) = 20$

E_b = open Encryption key of B = 3
$D_b = E_b^{-1}$ [mod $\varphi(N_b)$] = 3^{-1} mod 20 = 7

gcd [E_b , $\varphi(N_b)$] = 1, gcd [3,20] = 1

2. Encryption M = 6 to B: $\mathbf{Y_A} = M^{Eb} \bmod N_b = (6)^3 \bmod 33 = \mathbf{18}$
   Signing M = 6 by A: $\mathbf{S_A} = (Y_A)^{Da} \bmod 21 = (18)^5 \bmod 21 = \mathbf{9}$ => $(Y_A, S_A) = (18,9)$ is sent to B
3. Sinature verification by B: $\mathbf{Y_A} = (S_A)^{Ea} \bmod 21 = (9)^5 \bmod 21 = \mathbf{18 = Y_A}$ => **A is authentic**
   Decryption by B: $\mathbf{M} = Y_A^{Db} = (18)^7 \bmod 33 = \mathbf{6}$

3

Problem 8-2:

1. 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.
2. 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.
3. 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.
4. 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:

1. System set up

Open directory

User A	User B
$N_a = 55$	$N_b = 69$
$E_a = 7$	$E_b = 5$

USER A:

$N_a = p_a * q_a = 11*5 = \mathbf{55}$ open modulus of A
$p_a * q_a = \mathbf{11, 5}$ two secret primes
$\varphi(N_a) = (p_a-1)*(q_a-1) = (11-1)(5-1) = 40$

E_a = open Encryption key of A = 7
$D_a = E_a^{-1}$ [mod $\varphi(N_a)$] = 7^{-1} mod 40 = **23**

gcd [E_a , $\varphi(N_a)$] = 1, gcd [7,40] = 1

USER B:

$N_b = p_b * q_b = 23*3 = \mathbf{69}$ open modulus of B
$p_b * q_b = \mathbf{23,3}$ two secret large primes
$\varphi(N_b) = (p_b-1)*(q_b-1) = (23-1)(3-1) = 44$

E_b = open Encryption key of B = 5
$D_b = E_b^{-1}$ [mod $\varphi(N_b)$] = 5^{-1} mod 44 = 9

gcd [E_b , $\varphi(N_b)$] = 1, gcd [5,44] = 1

2. Encryption M = 2 to B: $\mathbf{Y_A} = M^{Eb} \bmod N_b = (2)^5 \bmod 69 = \mathbf{32}$
   Signing M = 2 by A: $\mathbf{S_A} = (M)^{Da} \bmod 55 = (2)^{23} \bmod 55 = \mathbf{8}$ => $(Y_A, S_A) = (32,8)$ is sent to B

4

Solution 8-2 cont.:

3. Decryption by B: $\mathbf{M} = Y_A^{Db} = (32)^9 \bmod 69 = \mathbf{2}$
   Sinature verification by B: $\mathbf{M} = (S_A)^{Ea} \bmod 55 = (8)^7 \bmod 55 = \mathbf{2 = M}$ => **A is authentic**

   Signing M = 2 by B: $\mathbf{S_B} = (M)^{Db} \bmod 69 = (2)^9 \bmod 69 = \mathbf{29}$ => $(S_B) = 29$ is sent to A

4. One possibility is to encrypt S_A as well using E_b. That is $Y_{Sa} = (S_a)^{Eb} = 8^5 \bmod 69 = 13$.
   User B can then decrypt Y_{Sa} to get the signature and then check it..

5

Problem 8-3:

A 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.

1. Compute the two prime factors p and q of m
2. Break the system and decrypt a received cryptogram Y = 7

Solution 8-3:

1. $\varphi(m) = (p-1)(q-1) = m-p-q+ \Rightarrow$ $s = (p + q) = m - \varphi(m) + 1$
   $s = 1243-1120+1 = \mathbf{124}$
   $m = p * q = \mathbf{1243}$

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

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

2. Decryption if the open encryption key E = 27:
   $D = E^{-1} \bmod \varphi(m)$
   that is $\mathbf{D = 27^{-1} (mod\ 1120) = 83}$
   [27^{-1} is computed by the extended gcd algorithm gcd(1120,27) = 1]
   => $\mathbf{27^{-1} = 83}$

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

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.

1. 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.
2. 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.
3. User B encrypts the message M = 3, and send the resulting cryptogram Y_A to A. User B then signs the cryptogram Y_A and generates the signature S_B. Compute Y_A and S_B.
4. Decipher the cryptogram Y_A on user A's site and verify the Signature S_B.
5. User A signs the received message M and sends his signature S_A back to B. Compute the signature S_A.
6. How many open keys are possible for each user?

7

Solution 8-4:

1. 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 , φ (N_A) = (13-1)(7-1) = 72
gcd [E_A, φ (N_A)] = 1 => select 11 as gcd (72,11) = 1
E_A = 11
D_A = -13 mod 72 = 59 (see computation below)

$D_A = 11^{-1}$ 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

2. 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 , φ (N_B) = (17-1)(3-1) = 32
gcd (E_B, φ (N_B)] =1 => select 21 as gcd (32,21) = 1
E_B = 21
D_B = -3 mod 32 = 29 (see computation below)

$D_B = 21^{-1}$ 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

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

$$Y_A = (M)^{E_A} \bmod N_A \qquad S_B = (Y_A)^{D_B} \bmod N_B$$

$$Y_A = (3)^{11} \bmod 91 = 61 \qquad S_B = (61)^{29} \bmod 51 = (10)^{29} = 28$$

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

Decryption:

$$M = (Y_A)^{D_A} \bmod N_A$$
$$M = (3^{11})^{59} \bmod 91$$
$$M = 3^{649 \bmod 72} \bmod 91 = 3^1$$

Verification:

$$\text{check if:} \quad (S_B)^{E_B} \bmod N_B = Y_A \bmod N_B$$
$$(61^{29})^{21} \bmod 51 = 61 \bmod 51$$
$$61^{609 \bmod 32} \bmod 51 = 10$$
$$61^{1} \bmod 51 = 10$$
$$10 = 10 \quad => \quad \text{signature is authentic!}$$

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

$$S_A = (M)^{D_A} \bmod N_A$$
$$S_A = (3)^{59} \bmod 91 = 61$$

6. How many open keys are possible for each user?
# of keys for user A = φ [φ (N_A)] = φ (72) = φ (2*2*2*3*3) = 72 (1 -1/2) (1 – 1/3) **= 24 keys**
# of keys for user B = φ [φ (N_B)] = φ (32) = φ (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.

1. Choose the appropriate open keys 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.
2. 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 .
3. Decipher the cryptogram C_B on Alice´s side.
4. Verify the signature S_B on Alice's side.
5. Alice signs the value *M^3 mod N_A* and sends her signature S_A back to Bob. Calculate the signature S_A. Verify S_A on Bob's side.
6. How many public key pairs are selectable for Alice and how many for Bob.
7. Why is the system not secure if M is signed instead of M^3 ?

10

Solution 8-5:

1. Set up Alice
N_A = 11 * 23 = 253, φ (N_A) = (11-1)(23-1) = 220
gcd [E_A, φ (N_A)] = 1 => select 37 as gcd (220,37) = 1
E_A = 37
D_A = -107 mod 220 = 113 (see computation below)

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

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE		GCD	
220	37	1	0	0	1	5	35				
37	35	0	1	1	-5	1	2				
35	2	1	-1	-5	6	17	1				
2	1	-1	18	6	-107	2	0	INVERSE=	-107	GCD=	1

Set up Bob
N_B = 31 * 7 = 217 , φ (N_B) = (31-1)(7-1) = 180
gcd (E_B, φ (N_B)] = 1 => select 11 as gcd (180,11) = 1
E_B = 11
D_B = -49 mod 180 = 131 (see computation below)

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

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE		GCD	
180	11	1	0	0	1	16	4				
11	4	0	1	1	-16	2	3				
4	3	1	-2	-16	33	1	1				
3	1	-2	3	33	-49	3	0	INVERSE=	-49	GCD=	1

11

Solution 8-5 cont.:

2. Encryption M = 12 to Alice:

$$C_B = (M)^{E_A} \bmod N_A$$
$$C_B = (12)^{37} \bmod 253 = 243$$

Signing M^3 by Bob:

$$S_B = (M^3)^{D_B} \bmod N_B$$
$$S_B = (12^3)^{131 \bmod 180} \bmod 217 = 209$$

3. Decription by Alice:

$$M = (C_B)^{D_A} \bmod N_A => M = (243)^{113} \bmod 253 = 12$$

4. Signature Verification by Alice:

$$\text{check if:} \ (S_B)^{E_B} \bmod N_B = M$$
$$(209)^{11} \bmod 217 = 209 = M^3 \bmod N_B = 12^3 \bmod 217 => \text{signature is authentic!}$$

5.

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

Signature Verification by Bob: $M^3 \bmod N_A = (S_A)^{E_A} \bmod N_A = (188)^{37 \bmod 220} \bmod 253 = 210$
$= 12^3 \bmod 253 = M^3 \bmod N_A =>$ signature is authentic!

6.
# of keys for user A = φ [φ (N_A)] = φ (220) = φ (2^2 * 5* 11) = 220(1 – 1/2) (1 – 1/5)(1 – 1/11) **= 80 keys**
# of keys for user B = φ [φ (N_B)] = φ (180) = φ (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 unsecure 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 mod 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 mod N is a one-way function (N = p*q) if p and q are not known.

M^3