uc3m | Universidad Carlos III de Madrid

CRYPTOGRAPHY AND COMPUTER SECURITY

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Asymmetric encryption"

Proposed exercises

Exercise 1:

Given the following RSA ciphers, perform the corresponding computation considering that the parameters provided correspond to the receiver:

a) p = 5, q = 7, and d = 11. Encrypt the message M = 2 and decrypt the result

b) p = 3, q = 11, and e = 7. Encrypt the message M = 5 and decrypt the result

c) n = 55, and e = 7. Encrypt the message M = 10 and decrypt the ciphertext C= 35

d) n = 91, and d=11. Encrypt the message M = 3 and decrypt the ciphertext C=41

Solución:

a) N = p • q => N = 5 • 7 = 35

ϕ (35) = ϕ (5) • ϕ (7) = 4 x 6 = 24

d • e mod ϕ (35) = 1 => 11 • e mod 24 =1 => e = 11

C = 2^{11} mod 35; **C = 18**

M = 18^{11} mod 35; **M = 2**

b) N = p • q =>N=3 • 11=33

ϕ (33) = ϕ (3) • ϕ (11) = 2 • 10= 20

d • e mod ϕ (33) = 1 => 7 • d mod 20 = 1 => **d = 3**

C = 5^7 mod 33; **C = 14**

M = 14^3 mod 33; **M = 5**

c) N = 55 => p = 5, q = 11

ϕ (55) = ϕ (5) • ϕ (11) = 4 • 10 = 40

d • e mod ϕ (55) = 1 => 7, d mod 40 = 1 => **d = -17 = 23**

C = 10^7 mod 55; **C = 10**

M = 35^{23} mod 55; **M = 30**

d) N = 91 => p = 7, q = 13

ϕ (91) = ϕ (7) • ϕ (13) = 6 • 12 = 72

d • e mod ϕ (91) = 1 => 11 • e mod 72 = 1 => **e = -13 = 59**

C = 3^{59} mod 91; **C = 61**

M = 41^{11} mod 91; **M = 20**

Exercise 2:

a) What is the strength of RSA? What length must the keys in RSA have? What is the "trap-door" to generate the keys in RSA?

b) Martin wants to send an encrypted message to Laura using RSA, with p=5, q=11 and d=7. If the message is M=10. What does Laura receive? Is it a good election p, q and d? Why?

Solución:

a.1) The strength of RSA lies on the difficulty of factoring large numbers

a.2) Nowadays, the keys used must have a length between 1024 and 2048 bits.

a.3) The prime numbers p and q (secret) are the trap-door of the system. If p and q are known it is easy to calculate d having e, while the complexity to factor N is

O(e((ln(N)lnln(N))1/2)

b) To encrypt it is necessary to use Laura's public key e. We have d = 7 and $e \cdot d = 1 \bmod \Phi(N)$.

$\Phi(55) = \Phi(5) \cdot \Phi(11) = 4 \cdot 10 = 40$; $7 \cdot e = 1 \bmod 40$ like g.c.d(7,40)=1 we can apply Euler or Euclides

Euler: $a^{-1} = a^{\Phi(n)-1} \bmod . \, n \Rightarrow \Phi(n) = \Phi(40) = \Phi(23) \cdot \Phi(5) = (23 - 22) \cdot 4 = 16$

$e = d^{-1} = d^{\Phi(40)-1} = 7^{15} \pmod{40} = (7^2)^7 \cdot 7 \pmod{40} = 9^7 \cdot 7 = (9^2)^3 \cdot 9 \cdot 7 = 81^3 \cdot 63 \pmod{40} = 13 \cdot 23 = 23$ $\quad e = 23$

To encrypt M=10; $C = M^e \pmod N = 10^{23} \bmod 55$

We know that $10^2 \pmod{55} = -10$ y $10^3 \pmod{55} = -10 \cdot 10 = -100 \pmod{55} = 10$

Thus, $10^{23} = (10^3)^7 \cdot 10^2 \pmod{55} = 10^7 \cdot (10^2) = 10^9 \bmod 55 = (10^3)^3 \bmod 55 = 10$

p, q y d must be large primes and besides we can see that Martin message is invariant after encryption (M=C). Therefore, the election of p, q and d is not good.

Exercise 3:

Alice and Bob are playing a popular game by e-mail. The game keeps in secret the messages exchanged by both players in each game. The messages are encrypted and sent with 27 elements where A=0 ,… …, Z=26. They use RSA algorithm to encrypt their communications. Alice's public key is $(e_A, N_A) = (7, 33)$. Bob's public key is $(e_B, N_B) = (5, 39)$.

Alice receives the ciphertext: 26 , 2 , 15 , 16 , 6 , 0 , 13 and Bob receives: 22 , 8 , 10 , 9 , 18 , 0.

Calculate the first three values sent and the first three values received by Alice.

Solution:

Alice uses her private key to decrypt the messages received.

First we calculate the private key (we can do it because N_A is small):

$\Phi(N_A) = 2 \cdot 10 = 20$

$e_A \cdot d_A = 1(\text{mod. } \Phi(N_A))$; $d_A \cdot 7 = 1(\text{mod. } 20)$ _ $d_A = 3$

Alice decrypts the message letter by letter.

26^3 (mod. 33) = 20 - > T

2^3 (mod. 33) = 8 - > I

15^3 (mod. 33) = 9 - > J

Calculation of Bob's private key

$\Phi(N_B) = 2 \cdot 12 = 24$
$e_B \cdot d_B = 1(\text{mod. } \Phi(N_B))$; $d_B \cdot 5 = 1(\text{mod. } 24)$ _ $d_B = 5$
Bob decrypts the message sent by Alice with his private key letter by letter:
22^5 (mod. 39) = 16 - > P
8^5 (mod. 39) = 8 - > I
10^5 (mod. 39) = 4 - > E

Exercise 4:
Alice and Bob use RSA algorithm to encrypt their communications with the following public keys:

$(n_A; e_A) = (55; 9)$ y $(n_B; e_B) = (39; 5)$

a) Calculate the ciphertext C_B that Bob must send to Alice if the message is:

MANDA DINERO

and calculate too the message corresponding to the answer of Alice

NO TENGO.

b) Decrypt the ciphertext C_A received by Bob

Note: Letters A-Z (without Ñ) are coded as 0-25, the dot as 26, and the blank as 27

Solución:

a)
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
Bob must send to Alice the message MANDA DINERO coded:
M -> 12 A ->0 N->13 D->3 ‘ ‘ ->27 I->8 E->4 R->17 O->14
Bob must use the public key of Alice $(n_A; e_A) = (55; 9)$, because only Alice can open the ciphertext CB.
Alice will use $CB = M^{eA} \bmod n_A$.
C_B -> C{M}= 12^9 mod 55 =12
C{A}= 0^9 mod 55 = 0
C{N}= 13^9 mod 55 = 28
C{D}= 3^9 mod 55 = 48
C{ }= 27^9 mod 55 = 42
C{I}= 8^9 mod 55 = 18
C{E}= 4^9 mod 55 = 14
C{R}= 17^9 mod 55 = 2
C{O}= 14^9 mod 55 = 4
Then C_B = [12,0,28,48,0,42,48,18,28,14,2,4] (mod 55)
The answer of Alice, NO TENGO, has been encrypted. She uses Bob’s public key
$(n_B; e_B) = (39; 5)$ to encrypt. $C_A = M^{eB} \bmod n_B$.
N->13 O->14 ‘ ‘ ->27 T->19 E->4 G->6 .->26
C_A -> C{N}= 13^5 mod 39 = 13
C{O}= 14^5 mod 39 = 14
C{ }= 27^5 mod 39 = 27
C{T}= 19^5 mod 39 = 28
C{E}= 4^5 mod 39 = 10
C{G}= 6^5 mod 39 = 15

$C\{.\} = 26^5 \bmod 39 = 26$
Then, CA = [13,14,27,28,10,13,15,14,26] (mod 39)

b) Bob uses his private key to decrypt C_A = [13,14,27,28,10,13,15,14,26] (mod 39). Thus, $M_A=C_A^{dB}(\bmod N_B)$

$n_B= 3 \cdot 13 =39$
$\Phi(n_B)=2\cdot 12=24$
$e_B\cdot d_B=1(\bmod \Phi(n_B))=$; $d_B\cdot 5=1(\bmod 24)$ $d_B=5$
MA -> $M\{13\}= 13^5 \bmod 39= 13$ -> N
$M\{14\}= 14^5 \bmod 39= 14$ -> O
$M\{27\}= 27^5 \bmod 39= 27$ -> ‘ ‘
$M\{28\}= 28^5 \bmod 39= 19$ -> T
$M\{10\}= 10^5 \bmod 39= 4$ -> E
$M\{13\}= 13^5 \bmod 39= 13$ -> N
$M\{15\}= 15^5 \bmod 39= 6$ -> G
$M\{14\}= 14^5 \bmod 39= 6$ -> O
M{26}= 265 mod 39= 26 -> .
MA = NO TENGO.