Lina Mi @01377283

Question 1. RSA Algorithm

Suppose Alice and Bob would like to use RSA encryption algorithm . Bob wants to send Alice a message (just number 3, may be they agreed that the number means meeting time)

Alice has the following keys:

p=5

q=7

e=11

Please explain all steps of encryption and decryption process

(Bonus: use RSA with digital signature, make up numbers for Bob)

Ans: encryption:

Step 1:

Bob needs to compute n=p*q=35

Step 2:

Encrypt the message (which is 3) with e and n;

$y = x^e \ mod \ n = 3^{11} mod \ 35 = 12$

Bob send y to Alice, encryption is done

Decryption:

Step 1:

Alice need to compute her private key d to decrypt the message Bob sent to her

$d = e^{-1} \ mod \ (p-1) \cdot (q-1)$ (1)

Multiplying equation (1) both sides with e, there is

$e \cdot d = e \cdot e^{-1} \ mod \ (p-1) * (q-1)$ since $e \cdot e^{-1} mod \ (p-1) \cdot (q-1) = 1$

According the definition of mod, then there is:

$e \cdot d = k \cdot (p-1) \cdot (q-1) + 1$

So $11d = k \cdot 4 \cdot 6 + 1 = 24k + 1$

To find d, Alice need to try different k, the equation above means that:

$(24k + 1) \ mod \ 11 = 0$

k	24k+1	(24k+1) mod11
0	1	1
1	25	3

2	49	5
3	73	7
4	97	9
5	121	0

So k=5, and d=(24k+1)/11=11

Step 2:
With d at hand , Alice decrypt the message received from Bob like following:

$x = y^d mod\ n = 12^{11} mod\ 35$

$= ((12^2)^5 mod 35 \cdot 12) mod\ 35$

$= ((12^2\ mod 35)^5 \cdot 12) mod 35 = (4^5 \cdot 12) mod\ 35 = 3$

Decryption is completed

Question 2

Please design Diffie-Hellman protocol for 4 people (pick up any numbers as private keys)

Ans: suppose there are four people named Alice, Bob, Carol and David separately, the Diffie-Hellman key exchange protocol is described as following:

All of four people agree on g=7 and n=13, the public function $7^k mod\ 13$

Round 1:

1) Alice randomly choose x=3 and sends Bob:
$X = 7^x mod\ 13 = 7^3 mod\ 13 = 5$
2) Bob randomly choose y=4 and sends Carol:
$Y = 7^y mod\ 13 = 7^4 mod\ 13 = 9$
3) Carol randomly choose z=5 and sends David:
$Z = 7^z mod\ 13 = 7^5 mod\ 13 = 11$
4) David randomly choose m=6 and sends Alice:
$M = 7^m mod\ 13 = 7^6 mod\ 13$ =12

Round2:

1) Alice sends Bob:
$M' = M^x mod\ 13 = 12^3 mod\ 13$=12
2) Bob sends Carol:
$X' = X^y mod\ 13 = 5^4 mod\ 13 = 1$
3) Carol sends David:
$Y' = Y^z mod\ 13 = 9^5 mod\ 13 = 3$
4) David sends Alice:
$Z' = Z^m mod\ 13 = 11^6 mod\ 13 = 12$

Round 3:

1) Alice sends Bob:
   $Z'' = Z'^{x} mod\ 13 = 12^3 mod\ 13 = 12$
2) Bob sends Carol:
   $M'' = M'^{y} mod\ 13 = 12^4 mod\ 13 = 1$
3) Carol sends David:
   $X'' = X'^{z} mod\ 13 = 1^5 mod\ 13 = 1$
4) David sends Alice:
   $Y'' = Y'^{m} mod\ 13 = 3^6 mod\ 13$=1

Round 4:

1) Alice computes:
   $k = Y''^{x} mod\ 13 = 1^3 mod\ 13 = 1$
2) Bob computes:
   $k' = Z''^{y} mod\ 13$=$12^4 mod\ 13$=1
3) Carol computes:
   $k'' = M''^{z} mod\ 13 = 1^5 mod\ 13 = 1$
4) David computes:
   $k''' = 1^6 mod\ 13 = 1$

   According to previous computation,
   $k = k' = k'' = k''' = g^{xyzm} mod\ n = 1$

Question 3.

Please answer the following questions:

- Is f(x)=x+2 one way function?

  Ans: f(x)=x+2 is not one way function, because it is easy to find the f^{-1}(x): x=f(x)-2

- Is f(x)=x^3 one way function?

  Ans: function f(x)=y=x^3 is not one way function, since once we know y, we can get $x = \sqrt[3]{y}$ easily.

- Is f(x)=x mod 3 one way function?

  Ans: f(x)=y=x mod 3 is one way function as even we know the value of y, x=3k+y, k=0,1,2…..N, it is hard to get the value of x without knowing k.

- Is f(x)=x^3 mod 3 one way function?

  Ans: f(x)=y=x^3 mod 3 is one way function because even we know the value of y, $x = \sqrt[3]{(3k + y)}$, k=0,1,2…..N, it is hard to get the exact value of x without knowing k.

- What is the difference between public and private key Cryptography?

  Ans: public key cryptography uses public key to encrypt message, the key is published and everyone know it, the receiver uses his or her private key to decrypt received message; in private key cryptography, message sender and receiver have agreed on a private key in advance, the sender uses this private key to encrypt message and receiver uses it to decrypt received message, the key must be secret, nobody else except sender and receiver should know it.

Question 4

Please prove that the set of natural numbers N has the same size as a set of all even natural numbers and the same size as the size of all odd numbers

Ans: the set of all even numbers can be expressed as A={2n, $n \in N$}, so for each member of set N, $n, n \in N$, there is one and only one number 2n in the set of A corresponding to it; on the other side, for every number m $(m = 2n, n \in N)$ of set A, , there is one and only one number n in set N corresponding to it, therefore set A and N has a relationship of one-to-one matching, so the set of natural numbers N has the same size as the set of all even numbers A;

Similarly, the set of all odd numbers can be expressed as $B = \{2n + 1, n \in N\}$, for each number n in set N, there is one and only one number $2n + 1, n \in N$ in set B to match it; on the other side, for each number m $(m = 2n + 1, n \in N)$ in set B, there is one and only one number n in set N corresponding to it. Since the member of set B and N are one-to-one matching, so the set of natural numbers N has the same size of the set of all odd numbers B.

Please provide your own example of sets A and B such that A is subset of B, but they have the same size

Ans: for example, the set of natural numbers N and the set of all natural numbers that are divisible by 5 M. Namely $M = \{5n, n \in N\}$, set M is subset of set N, but it has the same size of set N, since for every number $n\ in\ set\ N$, there is one and only one number $5n, n \in N$ in set M to match it, so set N and M have same size.

Prove that the set of numbers divisible by 3 has the same size as a set of numbers divisible by 7

Ans: the set of number divisible by 3 can be expressed as $\mathrm{A} = \{3\mathrm{n}, \mathrm{n} \in \mathrm{N}\}$, and the set of number divisible by 7 can be expressed as $B = \{7n, n \in N\}$,

Question 5

Take the number all parties arrive at as a result of Diffie-Hellman protocol for Question2.Make this number an encryption key and encrypt a shorter version of your first name using XOR encryption.

Ans: since the encryption key I get in question2 is 1, which is expressed as 000001 in form of six digits of binary number, my first name is lina, using 000001 as encryption key to do XOR encryption as following:

1) encrypt letter 'l':
   001100
   XOR 000001
   001101 letter 'm'
2) encrypt letter 'i':
   001001
   XOR 000001
   001000 letter 'h'
3) encrypt letter 'n'
   001110
   XOR000001
   001111 letter 'o'
4) encrypt letter 'a'
   000001
   XOR000001
   000000 symbol space

   The encryption result is 'mho '

Question 6

How would you enumerate the set of all rational numbers. (Bonus: connect this problem with Infinite Hotel 3 problem)

Ans: the set of all rational numbers can be expressed as

$$\begin{Bmatrix} \frac{1}{m}, \frac{2}{m-1}, \frac{3}{m-2}, \cdots \frac{m}{1} \quad m = 2n-1, n = 1,2,3 \cdots N \\ \frac{m}{1}, \frac{m-1}{2}, \frac{m-2}{3}, \cdots \frac{1}{m} \quad m = 2n, \qquad n = 1,2,3 \cdots N \end{Bmatrix}$$