**RSA**

**1, Diffie Hellman**

* **q là số nguyên tố**
* **a là căn nguyên thủy của q và a < q**
* **a và q là cái đề bài đã cho**

|  |  |
| --- | --- |
| YA = aXa mod q | * Cứ có X thì cho nên trên đầu * ­K tính bên A phải bằng K tính bên B |
| YB = aXb mod q |
| K = YAXb mod q  K = YBXa mod q |

2, RSA

+ Lần này khóa riêng và khóa công khai không còn là 1 số nữa mà là

PU = {e, n} khóa công khai (public)

PR = {d, n} khóa riêng (private)

2 cái cuối đều là n

Cho e, p, q

Bước 1: tính n = p.q (tìm được public)

Bước 2: ϕ(n) = ϕ(p)\*ϕ(q) = (p-1)(q-1)

Bước 3: d = e-1 mod ϕ(n)

(tìm được private) PR = {d,n}

Bước 4: đến đoạn này cho M là bản ghi

Nó có 2 cách mã hóa đó là

A, Dùng khoá riêng của người sở hữu bản ghi M để mã hóa bản rõ M và dùng Dùng và phải giải mã bằng mã công khai của người mã hóa cái bản ghi M này (Bản ghi số vì bất kì ai có được mã công khai của người sở hữu bản ghi M đều có thể lấy được bản ghi M)

C = Me mod n

M = Cd mod n

B, Dùng mã công khai của người định gửi tới để mã hóa bản ghi M sau khi người nhận nhận được thì sẽ mã hóa lại bằng mã riêng của người nhận để có thể giải mã bản ghi M (Bảo mật vì chỉ có người nhận mới có thể giải mã được bản ghi M)

C = Md mod n

M = Ce mod n

Thuật toán Alganma

(mục đích tạo chữ kí số cho 2 bên)

Nó sẽ cho mã riêng của An (XA)

Giá trị trung là q = 7919 và a = 7

Bắt tính

Câu 1:

Bước 1: Ya = aXa mod q

Câu 2:

Cho thêm k(nhỏ) và M

Bước 2: K = (Ya)k mod q

Bước 3: C1= ak mod q

Bước 4: C2 = M\*K mod q

Câu 3: Để giải mã

K = (C1)Xa mod q

M = (C2\*K-1) mod q

DSA (Tạo chữ kí điện tử cho 2 bên)

H(M) = 9 , p = 47, q = 23, h = 25

Câu 1: YA = gxA mod q

Với g = h(p-1)/q mod p

Câu 2 : tạo chữ kí số cho An

r = ( gk mod p ) mod q

s = [ k-1 \* ( H(M) + xA\*r) ] mod q

* Chữ ký số của An cho bản tin M : (r,s) =

Câu 3: Ba xác minh chữ kí

w = (s’)-1 mod q

u1 = [H(M’)w] mod q

u2 = (r’)w mod q

v = [(gu1yu2) mod p] mod q

ktra v = r’ (tính ở trên)