**KHÓA CÔNG KHAI**

1. **Trao đổi khóa Diffie-Hellman**

Giả sử An và Ba muốn trao đổi khoá phiên, họ đồng ý chọn   
số nguyên tố q = 7159 và a = 3 (là căn nguyên thủy của q).   
An chọn khóa riêng xA = 371 Ba chọn khóa riêng xB = 476

Hãy cho biết

a) Cách An tính ra khóa công khai yA và khóa phiên K? yA =

b) Cách Ba tính ra khóa công khai yB và khóa phiên K? yB =

Tóm lược:

q=7159, a=3, xA=371, xB=476

1. yA=? K=?
2. yB=? K=?

Giải:

1. Ta có

***yA = mod q***

-> yA=3^371mod7159 = 6394 (Hạ bậc lũy thừa số modulo – Đi thi phải làm tuần tự)

***K = yA^(xB) mod q***

-> K = 6394^476 mod 7159 = 4506 (Hạ bậc lũy thừa số modulo)

1. Tương tự

***yB = mod q*** = 5689

***K = yA^(xB) mod q*** = 3199

1. **Thuật toán RSA - Bài toán 1**

Giả sử An chọn các giá trị p = 37 , q = 59 , e = 53 để tạo cặp khóa.

Hãy cho biết

a) Khóa công khai của An: PU = {e, n} =?

b) cách An tạo ra khóa riêng: PR = {d, n} =?

c) Cách An tạo bản mã hóa thông điệp M = 47: C =?

d) Hãy cho biết cách người nhận giải mã bản mã C?

e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

Giải:

1. PU = {e,n} =?  
   n = p\*q = 2183  
    \* = 2088  
   e = 53 thỏa mãn gcd (e,) = 1

* Khóa công khai của An là PU = {53,2088}

1. Ta có: d=e^(-1)mod -> 53^(-1)mod2088

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 2088 | 0 | 1 | 53 |
| 39 | 0 | 1 | 53 | 1 | -39 | 21 |
| 2 | 1 | -39 | 21 | -2 | 79 | 11 |
| 1 | -2 | 79 | 11 | 3 | -118 | 10 |
| 1 |  |  |  | -5 | 197 | 1 |

d = 197

* Khóa riêng của An là PR = {197,2088}

1. **C = M^d mod n** = 47^197 mod 2183  
   197 = 128 + 64 + 4 + 1

47^2 mod 2183 = 26 47^32mod 2183=1728  
47^4mod 2183 = 676 47^64mod 2183=1823  
47^8mod2183 = 729 47^128mod 2183=803  
47^16mod2183= 972

* C = (803\*1823\*676\*47) mod 2183 = 1839

1. **M = C^e mod n** = 1839^53 mod 2183
2. 32 + 16 + 4 + 1

1839^2 mod 2183 = 454 1839^16 mod 2183 = 2172   
1839^4 mod 2183 = 914 1839^32 mod 2183 = 121  
1839^8 mod 2183 = 1490 1839^64 mod 2183 = 1543

* M = (121\*2172\*914\*1839) mod 2183 = 47

1. **Thuật toán RSA - Bài toán 2:**

Giả sử An chọn các giá trị p = 37 , q = 59 , e = 53

Hãy cho biết

a) Khóa công khai của An: PU = {e, n} =?

b) Cách An tạo ra khóa riêng: PR = {d, n} =?

c) Cách người gửi (Ba) mã hóa thông điệp M = 47 để gửi cho An: C =?

d) Cách An giải mã bản mã C:

e) Việc mã hóa ở câu c) thực hiện nhiệm vụ chữ ký số hay bảo mật.

Giải:

1. Giống phần a) Bài toán số 1 RSA
2. Giống phần b) Bài toán số 1 RSA

**C = M^e mod n** = 47^53 mod 2183

53 = 2^5 + 2^4 + 2^2 + 2^0 (110101) = 32 + 16 + 4 + 1

47^2 mod 2183 = 26 47^16mod2183=729^2mod2183= 972  
47^4mod 2183 = 26^2 mod 2183 =676 47^32mod 2183=972^2mod2183=1728  
47^8mod2183 = 676^2mod 2183 =729

* C = (1728\*972\*676\*47) mod 2183= 1654

**M = C^d mod 2183** = 1654^197 mod 2183

197 = 128 + 64 + 4 + 1

1654 ^2 mod 2183 = 417 1654 ^32 mod 2183 = 1231  
1654 ^4 mod 2183 = 1432 1654 ^64 mod 2183 = 359  
1654 ^8 mod 2183 = 787 1654 ^128 mod 2183 = 84  
1654 ^16 mod 2183 = 1580

* M = (84\*359\*1432\*1654) mod 2183 = 47

1. **Mật mã ElGamal**

Giả sử An và Ba trao đổi bằng hệ mật mã ElGamal, có các giá trị chung là

q = 6571 là một số nguyên tố, a = 3 là căn nguyên thủy của q.

An chọn khóa riêng là xA = 436

Hãy cho biết

a) Khóa công khai của An: PU = {q, a, YA} với yA =?

b) Ba chọn số k = 979 để mã hóa bản tin M = 459 gửi cho An. Bản mã là (C1, C2) =?

c) Cách An giải bản mã (C1, C2)?

Giải:

1. **yA= a^xA mod n** = 3^436 mod 6571 =

436=256+128+32+16+4

3^2mod6571=9 3^32mod6571=3429  
 3^4mod6571=81 3^64mod6571=2522  
 3^8mod6571=6561 3^128mod6571=6327  
 3^16mod6571=100 3^256mod6571=397  
 => yA=(397\*6327\*3429\*100\*81) mod6571=5457

1. **K = yA^k mod n** = 5457^979 mod 6571 = 1186

979 = 512 + 256 + 128 + 64 + 16 + 2 + 1

5457^2mod6571=5648 5457^64mod6571=175  
5457^4mod6571=4270 5457^128mod6571=4341  
5457^8mod6571=4946 5457^256mod6571=5224  
5457^16mod6571=5654 5457^512mod6571=813  
5457^32mod6571=6372

* K = (813\*5224\*4341\*175\*5654\*5648\*5457) mod 6571 = 1186

**C1 = a^k mod n** = 3^979 mod 6571 = 4722 (Hạ bậc lũy thừa)

**C2 = K\*M mod n** = 1186\*459 mod6571=5552

* (C1;C2) = (4722;5552)

1. **K = C1^xA mod n = a^(k\*xA) mod n**

4722^436 mod 6571 = 3^(979\*436) = 1186 (Hạ bậc lũy thừa - nên lấy phép tính đầu tiên cho dễ tính )

**M = C2\*K^(-1) mod n** = 5552\*1186^(-1) mod 6571 = (5552\*4449)mod6571 = 459

1. **CHỮ KÝ ĐIỆN TỬ DSA**

Giả sử An cần gửi cho Ba một bản tin M kèm chữ ký số, bản tin M có mã băm là H(M) = 1

An và Ba thống nhất các giá trị: p = 59, q = 29, h = 3

và An chọn xA = 19, k = 25

Hãy cho biết

a) Khóa công khai của An: yA =?

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

c) Cách Ba xác minh chữ ký số được đính kèm với bản tin M?

Giải:

1. **yA = h^xA mod q** = 3^19 mod 59 = 53
2. **r = (h^k mod p) mod q = (**3^25 mod 59) mod 29 =22

**s = [k^(-1)\*(H(M) + xA\*r)] mod q =** [25^(-1)\*(1 +19\*22)] mod 29

= (7 \* 429) mod 29 = 4

* M: (r,s) = (22,4)

1. w = s^(-1)(mod q) = 4^(-1) mod 29 = -7 mod 29 = 22

u1 = (H(M)\*w)(mod q) = (1\*22) mod 29 = 22

u2 = (r\*w)(mod q) = (22\*22) mod 29 = 20

v = (h^u1\*yA^u2(mod p)) (mod q) = [(3^22\*53^20) mod 59] mod 29 = 51 mod 29 = 22

v = r => chữ ký điện tử đúng