4. Mật mã ElGamal

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

q = 6827 là một số nguyên tố, a = 5 là căn nguyên thủy của q.

An chọn khóa riêng là (khoa rieng cua an)xA = 307

Hãy cho biết

1. Khóa công khai của An: PU = {q, a, YA} với yA = a^Xa mod q

Ya=5^307 mod 6827

5^307 mod 6827=[(5^158 mod 6827)^2\*5] mod 6827=2388

Vay Ya=2388

PU = {q, a, YA}={6827,5,2388}

1. Ba chọn số k = 919 để mã hóa bản tin M = 474 gửi cho An. Bản mã là (C1, C2) =

Tính K=(Ya)^k mod q=2388^919 mod 6827

2388^919 mod 6827=[(2388^459 mod 6827)^2\*2388] mod 6827=5072

2388^459 mod 6827=[(2388^229 mod 6827)^2\*2388] mod 6827=4642

2388^229 mod 6827=[(2388^114 mod 6827)^2\*2388] mod 6827=5154

2388^114 mod 6827=[(2388^57 mod 6827)^2] mod 6827=4920

2388^57 mod 6827=[(2388^28 mod 6827)^2\*2388] mod 6827=6583

2388^28 mod 6827=[(2388^14 mod 6827)^2] mod 6827=6235

2388^14 mod 6827=[(2388^7 mod 6827)^2] mod 6827=4987

2388^7 mod 6827=[(2388^3 mod 6827)^2\*2388] mod 6827=2015

2388^3 mod 6827=[(2388 mod 6827)^2\*2388] mod 6827=1539

2388^2 mod 6827=2388

Tính C1=a^k mod q=5^919 mod 6827 =4977

5^919 mod 6827=[(5^459 mod 6827)^2\*5] mod 6827=

5^459 mod 6827=[(5^229 mod 6827)^2\*5] mod 6827=

5^229 mod 6827=[(5^114 mod 6827)^2\*5] mod 6827=

5^114 mod 6827=[(5^57 mod 6827)^2] mod 6827=

5^57 mod 6827=[(5^28 mod 6827)^2\*5] mod 6827=

5^28 mod 6827=[(5^14 mod 6827)^2] mod 6827=1475

5^14 mod 6827=[(5^7 mod 6827)^2] mod 6827=123

5^7 mod 6827=[(5^3 mod 6827)^2\*5] mod 6827=3028

5^3 mod 6827=[(5mod 6827)^2\*5] mod 6827=125

5^2 mod 6827=5

Tính C2=KM mod q=474\*K mod 6827=1024

Vay (5072,1024)

1. Cách An giải bản mã (C1, C2)?

K=(C1)^Xa mod q=3200

M=(C2K^-1) mod q

=(1024\*3200^-1 )mod 6827

=[(1024 mod 6827)\* (3200^-1 )mod 6827] mod 6827

=1024\*(-401)

=-410624

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| q | A1 | A2 | A3 | B1 | B2 | B3 |  |  |
| - | 1 | 0 | 6827 | 0 | 1 | 3200 |  |  |
| 2 | 0 | 1 | 3200 | 1 | -2 | 427 |  |  |
| 7 | 1 | -2 | 427 | 7 | 15 | 211 |  |  |
| 2 | 7 | 15 | 211 | -13 | -32 | 5 |  |  |
| 42 | -13 | -32 | 5 |  | -401 | 1 |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |