Bài tập Mã cổ điển

Bài tập:

1. MẬT MÃ CAESAR

Input: M = NOROSEWITHOUTATH

Key: K = 8

Tìm Output: C =

Giải:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Gốc: | 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 |
|  | 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 |
| K=8 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |

Input: M = NOROSEWITHOUTATH

C = VWZWAMEQBPWCBIBP

1. MẬT MÃ VIGENERE – LẶP KHÓA

Input: M = MONEYMAKESTHE

Key: K = YOUREON

Tìm Output: C =

Giải:

M = MONEYMAKESTHE

K = YOUREONYOUREO

Tra bảng ta được:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | O | N | E | Y | M | A | K | E | S | T | H | E |
| Y | O | U | R | E | O | N | Y | O | U | R | E | O |
| K | C | H | V | C | A | N | I | S | M | K | L | S |

Ảnh có chứa văn bản

Mô tả được tạo tự động

C = KCHVCANISMKLS

1. MẬT MÃ VIGENERE – AUTOKEY

Input: M = MONEYMAKESTHE

Key: K = YOUREON

Tìm Output: C =

Giải:

M = MONEYMAKESTHE

K =YOUREONMONEYM

Tra bảng ta được:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | O | N | E | Y | M | A | K | E | S | T | H | E |
| Y | O | U | R | E | O | N | M | O | N | E | Y | M |
| K | C | H | V | C | A | N | W | S | F | X | F | Q |

Ảnh có chứa văn bản

Mô tả được tạo tự động

C = KCHVCANWSFXFQ

1. MÃ HÓA CHỮ ĐƠN

Input: M = AWOMANGIVESANDFO

Key: K = THLEYNPSXADWKFUBOGMQVJRCIZ

Tìm Output: C =

Giải:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| T | H | L | E | Y | N | P | S | X | A | D | W | K | F | U | B | O | G | M | Q | V | J | R | C | I | Z |

M = AWOMANGIVESANDFO

So theo bảng ta được kết quả

C = TRUKTFPXJYMTFENU

1. MẬT MÃ MA TRẬN KHÓA PLAYFAIR

Input: M = THETRUTHWILLOU

Key: K = THEDIEIS

Tìm Output: C =

Giải:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T | H | E | D | I |
| S | A | B | C | F |
| G | K | L | M | N |
| O | P | Q | R | U |
| V | W | X | Y | Z |

C = HEDHUOHEZHKBGQPF (Thêm chữ A)

1. MẬT MÃ HOÁN VỊ

Input: M = ABADBEGINNINGMAKES

Key: K = 9

Tìm Output: C =

Giải:

C = ANBIANDGBMEAGKIENS

Bài tập Modulo

1. TÍNH LŨY THỪA MODULO 𝒃 = 𝒂𝒎 𝒎𝒐𝒅 𝒏 BẰNG CÁCH HẠ BẬC LŨY THỪA

Input: a = 439; m = 760; n = 6269

Tìm Output: b =

Giải

b = 439760 mod 6269 = 2373

439760 mod 6269 = (439380 mod 6269)2 mod 6269 = 2373

439380 mod 6269 = (439190 mod 6269)2 mod 6269 = 5508

439190 mod 6269 = (43995 mod 6269)2 mod 6269 = 5815

43995 mod 6269 = [(43947 mod 6269)2 \* 439] mod 6269 = 755

43947 mod 6269 = [(43923 mod 6269)2 \* 439] mod 6269 = 6265

43923 mod 6269 = [(43911 mod 6269)2 \* 439] mod 6269 = 4509

43911 mod 6269 = [(4395 mod 6269)2 \* 439] mod 6269 = 2086

4395 mod 6269 = [(4392 mod 6269)2 \* 439] mod 6269 = 4211

4392 mod 6269 = (439 mod 6269)2 mod 6269 = 4651

439 mod 6269 = 439

2. TÌM NGHỊCH ĐẢO 𝒙 = 𝒂−𝟏 𝒎𝒐𝒅 𝒏 THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞ RỘNG

Input: a = 1885; n = 6563

Tìm Output: x =

Q = A3 div B3

(T1, T2, T3) = (A1 – Q\*B1, A2 – Q\*B2, A3 – Q\*B3)

(A1, A2, A3) = (B1, B2, B3)

(B1, B2, B3) = (T1, T2, T3)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 6563 | 0 | 1 | 1885 |
| 3 | 0 | 1 | 1885 | 1 | -3 | 908 |
| 2 | 1 | -3 | 908 | -2 | 7 | 69 |
| 13 | -2 | 7 | 69 | 27 | -94 | 11 |
| 6 | 27 | -94 | 11 | -164 | 571 | 3 |
| 3 | -164 | 571 | 3 | 519 | -1807 | 2 |
| 1 | 519 | -1807 | 2 | -683 | 2378 | 1 |

Giải

B3 = 1 => x = B2 = 2378 mod 6563 = 2378

3. SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO

𝒃 = 𝒂𝒎 𝒎𝒐𝒅 𝒏

Input: a = 397; m = 6329; n = 6329

Tìm Output: b =

Giải

b = 3976329  mod 6329

6329 là 1 số nguyên tố => 3976328 mod 6269 = 1

b = 3976329  mod 6329

= [(3976328  mod 6329) \* (397 mod 6329)] mod 6329

= (1 \* 397) mod 6329

b = 397

4. TÍNH GIÁ TRỊ HÀM EULER ɸ(n).

Input: n = 3992

Tìm Output: ɸ(n) =

Giải

ɸ(n) = ɸ(3992) = ɸ(23 \* 499) = (23 - 22).498 = 1992

5. SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO

𝒃 = 𝒂𝒎 𝒎𝒐𝒅 𝒏

Input: a = 23; m = 3885; n = 395

Tìm Output: b =

Giải

b = 233885  mod 395

Ta có 23 và 395 là 2 số nguyên tố cùng nhau:

=> 23ɸ(395) mod 395 = 1

ɸ(395) = ɸ(5\*79) =4\*78 = 312

b = 233885  mod 395 = 23312\*12+141  mod 395 = 23141 mod 395

Hạ bậc

b = 23141 mod 395 = [(2370 mod 395)2 \* 23] mod 395 = 238

b = 2370 mod 395 = (2335 mod 395)2 mod 395 = 339

b = 2335 mod 395 = [(2317 mod 395)2 \* 23] mod 395 = 292

b = 2317 mod 395 = [(238 mod 395)2 \* 23] mod 395 = 213

b = 238 mod 395 = (234 mod 395)2 mod 395 = 371

b = 234 mod 395 = (232 mod 395)2 mod 395 = 181

b = 232 mod 395 = (23 mod 395)2 mod 395 = 134

b = 23 mod 395 = 23

**= > b = 238**

6. SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo 𝒃 = 𝒂𝒌 𝒎𝒐𝒅 𝒏

Input: a = 227; k = 80; n = 60421

Tìm Output: b =

Giải:

Phân tích thừa số nguyên tố :

m1, m2, m3 = 23, 37, 71

Mi = n / mi

M1,M2,M3 = 2627, 1633, 851

M1-1 mod m1 = 2627 mod 23

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 23 | 0 | 1 | 2627 |
| 0 | 0 | 1 | 2627 | 1 | 0 | 23 |
| 114 | 1 | 0 | 23 | -114 | 1 | 5 |
| 4 | -114 | 1 | 5 | 457 | -4 | 3 |
| 1 | 457 | -4 | 3 | -571 | 5 | 2 |
| 1 | -571 | 5 | 2 | 1028 | -9 | 1 |

B3 = 1 => B2 = 2627 mod 23 = -9 mod 23 = 14

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 37 | 0 | 1 | 1633 |
| 0 | 0 | 1 | 1633 | 1 | 0 | 37 |
| 44 | 1 | 0 | 37 | -44 | 1 | 5 |
| 7 | -44 | 1 | 5 | 309 | -7 | 2 |
| 2 | 309 | -7 | 2 | -662 | 15 | 1 |

B3 = 1 => B2 = 1633 mod 37 = 15 mod 37 = 15

M3-1 mod m3 = 851 mod 71

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 71 | 0 | 1 | 851 |
| 0 | 0 | 1 | 851 | 1 | 0 | 71 |
| 11 | 1 | 0 | 71 | -11 | 1 | 70 |
| 1 | -11 | 1 | 70 | 12 | -1 | 1 |

B3 = 1 => B2 = 851 mod 71 = -1 mod 71 = 70

ci = (Mi-1 mod mi) \* Mi

c1, c2, c3 = 36778, 24495, 59570

ai = ak mod mi

a1 = 22780 mod 23

22780 mod 23 = 4

22780 mod 23 = (22740 mod 23)2 mod 23 = 4

22740 mod 23 = (22720 mod 23)2 mod 23 = 2

22720 mod 23 = (22710 mod 23)2 mod 23 = 18

22710 mod 23 = (2275 mod 23)2 mod 23 = 8

2275 mod 23 = [(2272 mod 23)2 \* 227] mod 23 = 10

2272 mod 23 = (227 mod 23)2 mod 23 = 9

227 mod 23 = 20

a1 = 4

a2 = 22780 mod 37

22780 mod 37 = 16

22780 mod 37 = (22740 mod 37)2 mod 37 = 16

22740 mod 37 = (22720 mod 37)2 mod 37 = 33

22720 mod 37 = (22710 mod 37)2 mod 37 = 12

22710 mod 37 = (2275 mod 37)2 mod 37 = 30

2275 mod 37 = [(2272 mod 37)2 \* 227] mod 37 = 17

2272 mod 37 = (227 mod 37)2 mod 37 = 25

227 mod 37 = 5

a2 = 16

a3 = 22780 mod 71

22780 mod 71 = 1

22780 mod 71 = (22740 mod 71)2 mod 71 = 1

22740 mod 71 = (22720 mod 71)2 mod 71 = 1

22720 mod 71 = (22710 mod 71)2 mod 71 = 1

22710 mod 71 = (2275 mod 71)2 mod 71 = 1

2275 mod 71 = [(2272 mod 71)2 \* 227] mod 71 = 70

2272 mod 71 = (227 mod 71)2 mod 71 = 54

227 mod 71 = 14

a3 = 1

c1, c2, c3 = 36778, 24495, 59570

a1, a2, a3 = 4, 16, 1

b = (a1c1 + a2c2+ a3c3) mod (m1\*m2\*m3)

= (4\*36778 + 16\* 24495+ 1\*59570) mod(60421)

= 598602 mod 60421 = 54813

7. SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.

{

𝒙 𝒎𝒐𝒅 𝒎𝟏 = 𝒂𝟏

𝒙 𝒎𝒐𝒅 𝒎𝟐 = 𝒂𝟐

𝒙 𝒎𝒐𝒅 𝒎𝟑 = 𝒂𝟑

Input: m1 = 17; m2 = 19; m3 = 11; a1 = 5; a2 = 16; a3 = 3;

Tìm Output: x =

Giải:

Ta có x mod 17 = 5; x mod 19 = 16; x mod 11 = 3

Áp dụng định lý phần dư Trung Hoa:

m1 = 17, m2 = 19, m3 = 11, a1 = 5, a2 = 16, a3 = 3,

M1 = 209, M2 = 187, M3 = 323

Ta tính:

M1-1  mod m1 = 209-1 mod 17= 7

M2-1 mod m2 = 187-1 mod 19= 6

M3-1 mod m3 = 323-1 mod 11= 3

c1 = (M1-1 mod m1)\* M1 = 7 \* 209

c2 = (M2-1 mod m2)\* M2 = 6 \* 187

c3 = (M3-1 mod m3)\* M3 = 3 \* 323

Như vậy x = A = (a1\*c1 + a2\*c2 + a3\*c3) mod (11\*17\*19)

= (5\*7\*209 + 16 \*6\*187 + 3\*3\*323) mod 3553

= 28174 mod 3553

= 3303

x = 3303

8. KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?

Input: a = 5; n = 463

Tìm Output: a có là căn nguyên thủy của n không?

Giải:

Gcd(5, 463) = 1

Ước ɸ463 = {1, 2, 3, 6, 7, 11, 14, 21, 22, 33, 42, 66, 77, 154, 231, 462}

51 mod 463 = 5

52 mod 463 = 25

53 mod 463 = 125

56 mod 463 = 346

57 mod 463 = 341

511 mod 463 = 145

514 mod 463 = 68

521 mod 463 = 38

522 mod 463 = 190

533 mod 463 = 233

542 mod 463 = 55

566 mod 463 = 118

577 mod 463 = 442

5154 mod 463 = 441

5231 mod 463 = 462

5462 mod 463 = 1

Phải

9. TÌM LOGARITHM RỜI RẠC CỦA SỐ b VỚI CƠ SỐ 𝒂 (𝒎𝒐𝒅 𝒏), 𝒌 = 𝐥𝐨𝐠𝒂 𝒃 (𝒎𝒐𝒅 𝒏).

Input: a = 3; b = 5; n = 19

Tìm Output: k =

Giải:

k = 𝐥𝐨𝐠35(𝒎𝒐𝒅 19).

Ta có:

3k mod 19 = 5

Xét:

k = 0: 30 mod 19 = 1

k = 1: 31 mod 19 = 3

k = 2: 32 mod 19 = 9

k = 3: 33 mod 19 = 8

k = 4: 34 mod 19 = 5

=> k = 4

10. TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN

𝑨𝟏 = (𝒂𝒙 + 𝒃𝒚) 𝒎𝒐𝒅 𝒏

𝑨𝟐 = (𝒂𝒙 − 𝒃𝒚) 𝒎𝒐𝒅 𝒏

𝑨𝟑 = (𝒂𝒙  \* 𝒃𝒚) 𝒎𝒐𝒅 𝒏

𝑨𝟒 = (𝒃𝒚)−𝟏 𝒎𝒐𝒅 𝒏

𝑨𝟓 = (𝒂𝒙/𝒃𝒚) 𝒎𝒐𝒅 𝒏

Input: a = 37; b = 97; x = 581; y = 364; n = 127

Tìm Output: A1 = ; A2 = ; A3 = ; A4 = ; A5 = ?

Giải:

A1 = (37581 + 97364) 𝒎𝒐𝒅 127

= (37581 𝒎𝒐𝒅 127 + 97364 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

GCD(37, 127) = 1 => là 2 số nguyên tố cùng nhau:

* 37ɸ127  𝒎𝒐𝒅 127= 37126 𝒎𝒐𝒅 127 = 1

GCD(97, 127) = 1 => là 2 số nguyên tố cùng nhau:

* 97ɸ127  𝒎𝒐𝒅 127= 97126 𝒎𝒐𝒅 127 = 1

A1 = (374x126+77 𝒎𝒐𝒅 127 + 972x126+112 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

= (3777 𝒎𝒐𝒅 127 + 97112 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

X1 = 3777 𝒎𝒐𝒅 127

X2 = 97112 𝒎𝒐𝒅 127

Hạ bậc:

X1 = 3777 mod 127 = 52

3777 mod 127 = [(3738 mod 127)2 \* 37] mod 127 = 52

3738 mod 127 = (3719 mod 127)2 mod 127 = 99

3719 mod 127 = [(379 mod 127)2 \* 37] mod 127 = 37

379 mod 127 = [(374 mod 127)2 \* 37] mod 127 = 1

374 mod 127 = (372 mod 127)2 mod 127 = 22

372 mod 127 = (37 mod 127)2 mod 127 = 99

37 mod 127 = 37

X2 = 97112 mod 127 = 103

97112 mod 127 = (9756 mod 127)2 mod 127 = 103

9756 mod 127 = (9728 mod 127)2 mod 127 = 22

9728 mod 127 = (9714 mod 127)2 mod 127 = 99

9714 mod 127 = (977 mod 127)2 mod 127 = 37

977 mod 127 = [(973 mod 127)2 \* 97] mod 127 = 75

973 mod 127 = [(97 mod 127)2 \* 97] mod 127 = 51

97 mod 127 = 97

A1 = (52 + 103) 𝒎𝒐𝒅 127 = 155 𝒎𝒐𝒅 127

A1 = 28

A2 = (37581 - 97364) 𝒎𝒐𝒅 127

= (37581 𝒎𝒐𝒅 127 - 97364 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

GCD(37, 127) = 1 => là 2 số nguyên tố cùng nhau:

* 37ɸ127  𝒎𝒐𝒅 127= 37126 𝒎𝒐𝒅 127 = 1

GCD(97, 127) = 1 => là 2 số nguyên tố cùng nhau:

* 97ɸ127  𝒎𝒐𝒅 127= 97126 𝒎𝒐𝒅 127 = 1

A2 = (374x126+77 𝒎𝒐𝒅 127 - 972x126+112 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

= (3777 𝒎𝒐𝒅 127 - 97112 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

X1 = 3777 𝒎𝒐𝒅 127

X2 = 97112 𝒎𝒐𝒅 127

Hạ bậc:

X1 = 3777 mod 127 = 52

3777 mod 127 = [(3738 mod 127)2 \* 37] mod 127 = 52

3738 mod 127 = (3719 mod 127)2 mod 127 = 99

3719 mod 127 = [(379 mod 127)2 \* 37] mod 127 = 37

379 mod 127 = [(374 mod 127)2 \* 37] mod 127 = 1

374 mod 127 = (372 mod 127)2 mod 127 = 22

372 mod 127 = (37 mod 127)2 mod 127 = 99

37 mod 127 = 37

X2 = 97112 mod 127 = 103

97112 mod 127 = (9756 mod 127)2 mod 127 = 103

9756 mod 127 = (9728 mod 127)2 mod 127 = 22

9728 mod 127 = (9714 mod 127)2 mod 127 = 99

9714 mod 127 = (977 mod 127)2 mod 127 = 37

977 mod 127 = [(973 mod 127)2 \* 97] mod 127 = 75

973 mod 127 = [(97 mod 127)2 \* 97] mod 127 = 51

97 mod 127 = 97

A2 = (52 - 103) 𝒎𝒐𝒅 127 = 155 𝒎𝒐𝒅 127

A2 = 76

A3 = (37581 x 97364) 𝒎𝒐𝒅 127

= (37581 𝒎𝒐𝒅 127 x 97364 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

GCD(37, 127) = 1 => là 2 số nguyên tố cùng nhau:

* 37ɸ127  𝒎𝒐𝒅 127= 37126 𝒎𝒐𝒅 127 = 1

GCD(97, 127) = 1 => là 2 số nguyên tố cùng nhau:

* 97ɸ127  𝒎𝒐𝒅 127= 97126 𝒎𝒐𝒅 127 = 1

A3 = (374x126+77 𝒎𝒐𝒅 127 x 972x126+112 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

= (3777 𝒎𝒐𝒅 127 x 97112 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

X1 = 3777 𝒎𝒐𝒅 127

X2 = 97112 𝒎𝒐𝒅 127

Hạ bậc:

X1 = 3777 mod 127 = 52

3777 mod 127 = [(3738 mod 127)2 \* 37] mod 127 = 52

3738 mod 127 = (3719 mod 127)2 mod 127 = 99

3719 mod 127 = [(379 mod 127)2 \* 37] mod 127 = 37

379 mod 127 = [(374 mod 127)2 \* 37] mod 127 = 1

374 mod 127 = (372 mod 127)2 mod 127 = 22

372 mod 127 = (37 mod 127)2 mod 127 = 99

37 mod 127 = 37

X2 = 97112 mod 127 = 103

97112 mod 127 = (9756 mod 127)2 mod 127 = 103

9756 mod 127 = (9728 mod 127)2 mod 127 = 22

9728 mod 127 = (9714 mod 127)2 mod 127 = 99

9714 mod 127 = (977 mod 127)2 mod 127 = 37

977 mod 127 = [(973 mod 127)2 \* 97] mod 127 = 75

973 mod 127 = [(97 mod 127)2 \* 97] mod 127 = 51

97 mod 127 = 97

A3 = (52 x 103) 𝒎𝒐𝒅 127 = 155 𝒎𝒐𝒅 127

A3 = 22

A4 = (97364)-1 𝒎𝒐𝒅 127

GCD(97, 127) = 1 => là 2 số nguyên tố cùng nhau:

* 97ɸ127  𝒎𝒐𝒅 127= 97126 𝒎𝒐𝒅 127 = 1

A4 = (972x126+112 𝒎𝒐𝒅 127)-1 𝒎𝒐𝒅 127

= (97112 𝒎𝒐𝒅 127)-1 𝒎𝒐𝒅 127

Hạ bậc:

X = 97112 mod 127

X = 97112 mod 127 = 103

97112 mod 127 = (9756 mod 127)2 mod 127 = 103

9756 mod 127 = (9728 mod 127)2 mod 127 = 22

9728 mod 127 = (9714 mod 127)2 mod 127 = 99

9714 mod 127 = (977 mod 127)2 mod 127 = 37

977 mod 127 = [(973 mod 127)2 \* 97] mod 127 = 75

973 mod 127 = [(97 mod 127)2 \* 97] mod 127 = 51

97 mod 127 = 97

A4 = 103-1 𝒎𝒐𝒅 127

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 127 | 0 | 1 | 103 |
| 1 | 0 | 1 | 103 | 1 | -1 | 24 |
| 4 | 1 | -1 | 24 | -4 | 5 | 7 |
| 3 | -4 | 5 | 7 | 13 | -16 | 3 |
| 2 | 13 | -16 | 3 | -30 | 37 | 1 |

B3 = 1 => x = B2 = 37 mod 127 = 37

A4 = 37

A5 = (37581 / 97364) 𝒎𝒐𝒅 127

= (37581 𝒎𝒐𝒅 127 \* (97364)-1 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

GCD(37, 127) = 1 => là 2 số nguyên tố cùng nhau:

* 37ɸ127  𝒎𝒐𝒅 127= 37126 𝒎𝒐𝒅 127 = 1

GCD(97, 127) = 1 => là 2 số nguyên tố cùng nhau:

* 97ɸ127  𝒎𝒐𝒅 127= 97126 𝒎𝒐𝒅 127 = 1

A5 = (374x126+77 𝒎𝒐𝒅 127 \* (972x126+112)-1 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

= (3777 𝒎𝒐𝒅 127 \* (97112)-1 𝒎𝒐𝒅 127) 𝒎𝒐𝒅 127

X1 = 3777 𝒎𝒐𝒅 127

X2 = 97112 𝒎𝒐𝒅 127

Hạ bậc:

X1 = 3777 mod 127 = 52

3777 mod 127 = [(3738 mod 127)2 \* 37] mod 127 = 52

3738 mod 127 = (3719 mod 127)2 mod 127 = 99

3719 mod 127 = [(379 mod 127)2 \* 37] mod 127 = 37

379 mod 127 = [(374 mod 127)2 \* 37] mod 127 = 1

374 mod 127 = (372 mod 127)2 mod 127 = 22

372 mod 127 = (37 mod 127)2 mod 127 = 99

37 mod 127 = 37

X2 = 97112 mod 127 = 103

97112 mod 127 = (9756 mod 127)2 mod 127 = 103

9756 mod 127 = (9728 mod 127)2 mod 127 = 22

9728 mod 127 = (9714 mod 127)2 mod 127 = 99

9714 mod 127 = (977 mod 127)2 mod 127 = 37

977 mod 127 = [(973 mod 127)2 \* 97] mod 127 = 75

973 mod 127 = [(97 mod 127)2 \* 97] mod 127 = 51

97 mod 127 = 97

A5 = (52 \* 103-1) 𝒎𝒐𝒅 127 = 155 𝒎𝒐𝒅 127

X = 103-1 𝒎𝒐𝒅 127

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 127 | 0 | 1 | 103 |
| 1 | 0 | 1 | 103 | 1 | -1 | 24 |
| 4 | 1 | -1 | 24 | -4 | 5 | 7 |
| 3 | -4 | 5 | 7 | 13 | -16 | 3 |
| 2 | 13 | -16 | 3 | -30 | 37 | 1 |

B3 = 1 => x = B2 = 37 mod 127 = 37

X = 37

A5 = (52 \* 37) 𝒎𝒐𝒅 127

A5 = 19

Bài tập DES

BÀI TẬP MÃ HÓA DES

INPUT: K (là input bài 1) = B35F59255E3BCB54;

M (là input bài 4) = 32D604E6C4504149;

OUTPUT: Tìm C (kết quả bài 11) = 056546D954490960

HÃY THỰC HIỆN CÁC BÀI TOÁN CHI TIẾT TỪ Bài 1 đến Bài 9, và Bài 11

(XEM THÊM YÊU CẦU PHẦN THỰC HÀNH)

PHẦN 1: SINH KHÓA Ki từ khóa K (input)

1. Tính hoán vị PC1 đối với khóa K:

Input: K = (input) = , PC1 (xem tài liệu mục 3.2 DES)

Output: C0 = , D0 =

Giải:

Input:

K = B35F59255E3BCB54

= 1011001101011111010110010010010101011110001110111100101101010100

PC1 = 41D629B739A767

= 01000001110101100010100110110111001110011010011101100111

Output:

C0: 0100000111010110001010011011

D0: 0111001110011010011101100111

C0: 41D6290B

D0: 739A7607

2. Tính các giá trị dịch vòng Ci, Di:

Input: C0 = , D0 = (kết quả bài 1), si(xem tài liệu mục 3.2 DES)

Output: Ci = , Di =

Giải:

Input:

C0: 0100000111010110001010011011

D0: 0111001110011010011101100111

C0: 41D6290B

D0: 739A7607

SHIFT = 1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1

Output:

C1: 1000001110101100010100110110

D1: 1110011100110100111011001110

C1: 83AC5306

D1: E734EC0E

C2: 0000011101011000101001101101

D2: 1100111001101001110110011101

C2: 0758A60D

D2: CE69D90D

C3: 0001110101100010100110110100

D3: 0011100110100111011001110111

C3: 1D629B04

D3: 39A76707

C4: 0111010110001010011011010000

D4: 1110011010011101100111011100

C4: 758A6D00

D4: E69D9D0C

C5: 1101011000101001101101000001

D5: 1001101001110110011101110011

C5: D629B401

D5: 9A767703

C6: 0101100010100110110100000111

D6: 0110100111011001110111001110

C6: 58A6D007

D6: 69D9DC0E

C7: 0110001010011011010000011101

D7: 1010011101100111011100111001

C7: 629B410D

D7: A7677309

C8: 1000101001101101000001110101

D8: 1001110110011101110011100110

C8: 8A6D0705

D8: 9D9DCE06

C9: 0001010011011010000011101011

D9: 0011101100111011100111001101

C9: 14DA0E0B

D9: 3B3B9C0D

C10: 0101001101101000001110101100

D10: 1110110011101110011100110100

C10: 53683A0C

D10: ECEE7304

C11: 0100110110100000111010110001

D11: 1011001110111001110011010011

C11: 4DA0EB01

D11: B3B9CD03

C12: 0011011010000011101011000101

D12: 1100111011100111001101001110

C12: 3683AC05

D12: CEE7340E

C13: 1101101000001110101100010100

D13: 0011101110011100110100111011

C13: DA0EB104

D13: 3B9CD30B

C14: 0110100000111010110001010011

D14: 1110111001110011010011101100

C14: 683AC503

D14: EE734E0C

C15: 1010000011101011000101001101

D15: 1011100111001101001110110011

C15: A0EB140D

D15: B9CD3B03

C16: 0100000111010110001010011011

D16: 0111001110011010011101100111

C16: 41D6290B

D16: 739A7607

3. Tính khóa Ki cho vòng lặp thứ i

Input: Ci = , Di = (kết quả bài 2), PC2 (xem tài liệu mục 3.2 DES)

Output: Ki = .

Giải

K1 : 101110000000100011011110001011110100011011111110

K1 : B808DE2F46FE

K2 : 010000010101111011010010110000100111111111100010

K2 : 415ED2C27FE2

K3 : 011101001111100111000100011111001010101100111101

K3 : 74F9C47CAB3D

K4 : 000100101110010101000011111100110101110011011010

K4 : 12E543F35CDA

K5 : 011010010100010100110111010011011011001100111011

K5 : 6945374DB33B

K6 : 111001011000000110001101101101110111110001101100

K6 : E5818DB77C6C

K7 : 000100111000001010110011011010001001101111110110

K7 : 1382B3689BF6

K8 : 101111010001100010110010100101011110110010111111

K8 : BD18B295ECBF

K9 : 000000011111101100001010101000010111111101001101

K9 : 01FB0AA17F4D

K10 : 001000000011110111010111111110101011001010110010

K10 : 203DD7FAB2B2

K11 : 011101010110110001000001111101010100111100101111

K11 : 756C41F54F2F

K12 : 010000111110010110110000000111100011101011011010

K12 : 43E5B01E3ADA

K13 : 110111001000010110010111111101011111000101110101

K13 : DC8597F5F175

K14 : 011101111000001000001011001000111010111011101010

K14 : 77820B23AEEA

K15 : 001010111001000010100110111111001011110100010111

K15 : 2B90A6FCBD17

K16 : 100100011011011001001001101111111001000100101101

K16 : 91B649BF912D

PHẦN 2: MÃ HÓA

4. Tính hoán vị IP đối với bản tin M

Input: M = (input) = , IP (xem tài liệu mục 3.2 DES)

Output: L0 = , R0 =

Giải:

32D604E6C4504149

0011001011010110000001001110011011000100010100000100000101001001

1111101000100011000111101100000000011010000010011000000000001011

M sau khi hoán vị IP = FA231EC01A09800B

L0 = FA231EC0

R0 = 1A09800B

========== CHI TIẾT VÒNG LẶP THỨ NHẤT ==============

5. Tính hàm mở rộng nửa phải E[R0]

Input: R0 = (kết quả bài 4), E (xem tài liệu mục 3.2 DES)

Output: ER0 =

Giải:

ER0: 100011110100000001010011110000000000000001010110

ER0: 8F4053C00056

6. Thực hiên XOR ER0 với khóa K1

Input: ER0 (kết quả bài 5) , K1 (kết quả bài 3)

Output: A =

Giải:

A: 001101110100100010001101111011110100011010101000

A: 37488DEF46A8

7. Thực hiện phép thế S-box đối với B

Input: A (kết quả bài 6), 8 bảng Si, i = 1, 2, ..., 8; (xem tài liệu mục 3.2 DES)

Output: B = S(A) =

Giải:

B: 11011100011000000100010010101001

B: DC6044A9

8. Thực hiện hoán vị P đối với SB

Input: B (kết quả bài 7), P (xem tài liệu mục 3.2 DES)

Output: F =

F: 00001000100011011000110000011111

F: 088D8C1F

========= THỰC HIỆN VÒNG LẶP THỨ NHẤT =================

9. Thực hiện vòng lặp thứ nhất

Input: L0 = ; R0 = , (kết quả bài 4), F (kết quả bài 8)

Output: L1 = R0 = ; R1 = L0  F =

L1= 1A09800B

R1= F2AE92DF

========= THỰC HIỆN VÒNG LẶP THỨ i, i = 2, 3, ..., 16 ==========

10. Thực hiện vòng lặp thứ i, i = 2, 3, ..., 16

Input: Li-1 = ; Ri-1 = , (kết quả bài 9 hoặc bài 10)

Output: Li = Ri-1 = ; Ri = Li-1  f(Ri-1,Ki) =

L2 = F2AE92DF

R2 = 90C9EE98

L3 = 90C9EE98

R3 = EE9DCA10

L4 = EE9DCA10

R4 = 5248F727

L5 = 5248F727

R5 = C3082107

L6 = C3082107

R6 = 3210CB66

L7 = 3210CB66

R7 = F24BE993

L8 = F24BE993

R8 = 4784A056

L9 = 4784A056

R9 = E071AFDE

L10 = E071AFDE

R10 = E1C863EB

L11 = E1C863EB

R11 = EAE65579

L12 = EAE65579

R12 = 84E40795

L13 = 84E40795

R13 = 0CF0991C

L14 = 0CF0991C

R14 = 3BBD6FC1

L15 = 3BBD6FC1

R15 = 2CD7A82B

L16 = 2CD7A82B

R16 = 2DAC07E4

========= KẾT THÚC VÒNG LẶP THỨ 16 ======================

11. Thực hiện hoán vị cuối cùng IP-1

Input: L16 = ; R16 = , (kết quả bài 10); IP-1

(xem tài liệu mục 3.2 DES)

Output: C = ;(bản mã cần tìm)

Giải:

R16+L16 = 2DAC07E42CD7A82B

0010110110101100000001111110010000101100110101111010100000101011

C: 6626F5DA20DB2139

============ KẾT QUẢ MÃ HÓA

AES:

Input M = 4AEB5D62EC3B55DBF5D5A87708E2FF1E là input bài 6

K = 6704C20E086B3F537AE5721F486DC559 là input bài 1, 6

output C =

PHẦN 1: SINH 10 KHÓA Ki từ khóa K (input), i = 1, 2, ..., 10. (Mục 5.4)

1. Chia khóa K (128 bit) thành 4 word (32 bit)

Input: K (input) = 6704C20E086B3F537AE5721F486DC559,

Output: w0 = , w1 = , w2 = , w3 = ,

Giải:

W0 = 6704C20E,

W1= 086B3F53,

W2=7AE5721F,

W3=486DC559

2. Dịch vòng trái 1 byte đối với w3 (32 bit)

Input: w3 (kết quả bài 1) =

Output: rw = RotWord(w3) =

Giải:

W3=486DC559

rw = 6DC55948

3. Thay thế từng byte trong rw bằng bảng S-box SubWord

Input: rw (kết quả bài 2) = ; Sbox (tài liệu mục 5.3, Table 5.2, trang 157)

Output: sw = SubWord(rw) =

Giải:

rw = 6DC55948

sw = SubWord(rw) = 3CA6CB52

4. sw XORbit với Rcon[j]

Input: sw (kết quả bài 3) = ; RC[i] (xem tài liệu mục 5.4 Key Expansion)

Output: xcsw = XorRcon(sw, RC[i]) =

Giải:

sw = 3CA6CB52

xcsw = XorRcon(sw, RC[1]) = 3DA6CB52

5. Tính khóa K1 = (w4, w5, w6, w7)

Input: xcsw (kết quả bài 4) = ; w0, w1, w2, w3 (kết quả bài 1);

Output: w4 = XORbit(xcsw, w0) =

w5 = XORbit(w4, w1) =

w6 = XORbit(w5, w2) =

w7 = XORbit(w6, w3) =

Giải:

w4 = XORbit(xcsw, w0) = 5AA2095C

w5 = XORbit(w4, w1) = 52C9360F

w6 = XORbit(w5, w2) = 282C4410

w7 = XORbit(w6, w3) = 60418149

K1 = 5AA2095C52C9360F282C441060418149

LẶP LẠI từ Bài 2 đến Bài 5 để tạo các khóa K2, K3, ..., K10

K2 = DB89A1C1AE674B0A320440C18C8393DA

K3 = B8319051D6B1FAF0656121E0F477E43E

K4 = 3C0D9DCC37867C8CD7B697772552B688

K5 = 4845D814C24438B413A532456E3C8A02

K6 = E5A0786CACE8D06464C1F3B694A82220

K7 = E6463E52E20ADABED312E157C46C4E6E

K8 = C88EB0E2B9B369D74C5EBFE8C4A8E688

K9 = DD53E3012291F82F88D669815CF4129A

K10 = FEAD4E4F2EBF476830E68F0E20D4C65C

PHẦN 2: MÃ HÓA (mục 5.2, sơ đồ hình 5.3)

6. Tính kết quả AddRoundKey (tài liệu mục 5.3, trang 165)

Input: M (input) = 4AEB5D62EC3B55DBF5D5A87708E2FF1E,

K (input) = 6704C20E086B3F537AE5721F486DC559

Output: state = AddRoundKey(M, K)

Giải:

state = 2D6E468F640EF65063068F9F66A6DA63A6C688668647

======================== VÒNG LẶP THỨ i, i = 1, 2, ..., 9 ===========

7. Thay thế từng byte trong state bằng bảng S-box SubByte (tài liệu mục 5.3, trang 156)

Input: state (kết quả bài 6 cho lần lặp 1 hoặc kết quả bài 10 cho lần lặp kế tiếp) = ,

Sbox (tài liệu mục 5.3, Table 5.2, trang 157)

Output: state = SubByte (state)

Giải:

|  |  |  |  |
| --- | --- | --- | --- |
| D8 | 69 | 73 | 09 |
| DF | 53 | 04 | 73 |
| DB | 02 | 57 | 80 |
| 50 | C4 | 45 | A0 |

Vòng 1:

|  |  |  |  |
| --- | --- | --- | --- |
| 2D | E4 | 8F | 40 |
| EF | 50 | 30 | 8F |
| 9F | 6A | DA | 3A |
| 6C | 88 | 68 | 47 |

SubBytes

=>

8. Dịch vòng trái các byte trong state ShiftRows (tài liệu mục 5.3, trang 161)

Input: state (kết quả bài 7) = ,

Output: state = ShiftRows (state)

Giải:

Vòng 1:

|  |  |  |  |
| --- | --- | --- | --- |
| D8 | 69 | 73 | 09 |
| DF | 53 | 04 | 73 |
| DB | 02 | 57 | 80 |
| 50 | C4 | 45 | A0 |

|  |  |  |  |
| --- | --- | --- | --- |
| D8 | 69 | 73 | 09 |
| 53 | 04 | 73 | DF |
| 57 | 80 | DB | 02 |
| A0 | 50 | C4 | 45 |

ShiftRows

=>

9. Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)

Input: state (kết quả bài 8) = ,

Output: state = MixColumns (state)

Giải:

Vòng1

|  |  |  |  |
| --- | --- | --- | --- |
| D8 | 69 | 73 | 09 |
| 53 | 04 | 73 | DF |
| 57 | 80 | DB | 02 |
| A0 | 50 | C4 | 45 |

|  |  |  |  |
| --- | --- | --- | --- |
| A9 | 0E | 6C | 2F |
| 27 | AA | 27 | EF |
| DE | 86 | FA | 1D |
| 2C | 9F | AE | 4C |

MixColumns =>

10. Dịch vòng trái các byte trong state AddRoundKey (tài liệu mục 5.3, trang 165)

Input: state (kết quả bài 9) = ,

Ki (kết quả bài 5) =

Output: state = AddRoundKey (state, Ki)

Giải:

Vòng 1:

|  |  |  |  |
| --- | --- | --- | --- |
| F3 | 5C | 44 | 4F |
| 85 | 63 | 0B | AE |
| D7 | B0 | BE | 9C |
| 70 | 90 | BE | 05 |

|  |  |  |  |
| --- | --- | --- | --- |
| A9 | 0E | 6C | 2F |
| 27 | AA | 27 | EF |
| DE | 86 | FA | 1D |
| 2C | 9F | AE | 4C |

AddRoundKey(state, K1) =>

===================== VÒNG LẶP THỨ 10 ===========

11. Vòng lặp cuối (lần lặp 10) (tài liệu mục 5.3, trang 165)

Input: state (kết quả bài 10) = ,

K10 (kết quả bài 5) =

Output: C = state = AddRoundKey (ShiftRows(SubByte (state)), Ki

76D5686D9D45301738669B64DD76E0A7

Bài tập Mã 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 = 6947

và a = 5 (là căn nguyên thủy của q).

An chọn khóa riêng xA = 395

Ba chọn khóa riêng xB = 338

Hãy cho biết

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

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

Giải:

a)

xA = 395, yA = a xA mod q = 5395 mod 6947 = 4267

K = yA xB mod q = 4267338 mod 6947

K = 4267338 mod 6947 = 5944

4267338 mod 6947 = (4267169 mod 6947)2 mod 6947 = 5944

4267169 mod 6947 = [(426784 mod 6947)2 \* 4267] mod 6947 = 6441

426784 mod 6947 = (426742 mod 6947)2 mod 6947 = 4745

426742 mod 6947 = (426721 mod 6947)2 mod 6947 = 5969

426721 mod 6947 = [(426710 mod 6947)2 \* 4267] mod 6947 = 5823

426710 mod 6947 = (42675 mod 6947)2 mod 6947 = 1225

42675 mod 6947 = [(42672 mod 6947)2 \* 4267] mod 6947 = 35

42672 mod 6947 = (4267 mod 6947)2 mod 6947 = 6149

4267 mod 6947 = 4267

b)

xB = 338, yB = a xB mod q = 5338 mod 6947 = 256

K = yB xA mod q = 256395 mod 6947 = 5944

K = 256395 mod 6947 = 5944

256395 mod 6947 = [(256197 mod 6947)2 \* 256] mod 6947 = 5944

256197 mod 6947 = [(25698 mod 6947)2 \* 256] mod 6947 = 900

25698 mod 6947 = (25649 mod 6947)2 mod 6947 = 2607

25649 mod 6947 = [(25624 mod 6947)2 \* 256] mod 6947 = 3444

25624 mod 6947 = (25612 mod 6947)2 mod 6947 = 3747

25612 mod 6947 = (2566 mod 6947)2 mod 6947 = 1401

2566 mod 6947 = (2563 mod 6947)2 mod 6947 = 2839

2563 mod 6947 = [(256 mod 6947)2 \* 256] mod 6947 = 211

256 mod 6947 = 256

2. Thuật toán RSA - Bài toán 1

Giả sử An chọn các giá trị p = 43 , q = 47 , e = 67 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 = 59: 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:

a)

n = p\*q = 43\*47 = 2021

PU = {e, n} = {67,2021}

b)

ɸ(n) = ɸ(43\*47) = (43 -1)\*(47 -1) = 1932

d = e-1 (mod ɸ(n)) = 67-1 (mod 1932)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 1932 | 0 | 1 | 67 |
| 28 | 0 | 1 | 67 | 1 | -28 | 56 |
| 1 | 1 | -28 | 56 | -1 | 29 | 11 |
| 5 | -1 | 29 | 11 | 6 | -173 | 1 |

B3 = 1 => d = B2 = -173 mod 1932 = 1759

PR = {d, n} = {1759, 2021}

c)

C = Md mod n = 591759 mod 2021 = 1976

C = 591759 mod 2021 = 1976

591759 mod 2021 = [(59879 mod 2021)2 \* 59] mod 2021 = 1976

59879 mod 2021 = [(59439 mod 2021)2 \* 59] mod 2021 = 907

59439 mod 2021 = [(59219 mod 2021)2 \* 59] mod 2021 = 1225

59219 mod 2021 = [(59109 mod 2021)2 \* 59] mod 2021 = 729

59109 mod 2021 = [(5954 mod 2021)2 \* 59] mod 2021 = 477

5954 mod 2021 = (5927 mod 2021)2 mod 2021 = 1397

5927 mod 2021 = [(5913 mod 2021)2 \* 59] mod 2021 = 1325

5913 mod 2021 = [(596 mod 2021)2 \* 59] mod 2021 = 852

596 mod 2021 = (593 mod 2021)2 mod 2021 = 121

593 mod 2021 = [(59 mod 2021)2 \* 59] mod 2021 = 1258

59 mod 2021 = 59

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

M = Ce mod n = 197667 mod 2021 = 59

Hạ bậc

197667 mod 2021 = [(197633 mod 2021)2 \* 1976] mod 2021 = 59

197633 mod 2021 = [(197616 mod 2021)2 \* 1976] mod 2021 = 742

197616 mod 2021 = (19768 mod 2021)2 mod 2021 = 864

19768 mod 2021 = (19764 mod 2021)2 mod 2021 = 256

19764 mod 2021 = (19762 mod 2021)2 mod 2021 = 16

19762 mod 2021 = (1976 mod 2021)2 mod 2021 = 4

1976 mod 2021 = 1976

e)

Thực hiện nhiệm vụ chữ ký số

3. Thuật toán RSA - Bài toán 2:

Giả sử An chọn các giá trị p = 43 , q = 47 , e = 67 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 người gửi (Ba) mã hóa thông điệp M = 59 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:

a)

n = p\*q = 43\*47 = 2021

PU = {e, n} = {67,2021}

b)

ɸ(n) = ɸ(43\*47) = (43 -1)\*(47 -1) = 1932

d = e-1 (mod ɸ(n)) = 67-1 (mod 1932)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 1932 | 0 | 1 | 67 |
| 28 | 0 | 1 | 67 | 1 | -28 | 56 |
| 1 | 1 | -28 | 56 | -1 | 29 | 11 |
| 5 | -1 | 29 | 11 | 6 | -173 | 1 |

B3 = 1 => d = B2 = -173 mod 1932 = 1759

PR = {d, n} = {67,2021}

c)

C = Me mod n = 5967 mod 2021 = 1896

C = 5967 mod 2021 = 1896

5967 mod 2021 = [(5933 mod 2021)2 \* 59] mod 2021 = 1896

5933 mod 2021 = [(5916 mod 2021)2 \* 59] mod 2021 = 666

5916 mod 2021 = (598 mod 2021)2 mod 2021 = 686

598 mod 2021 = (594 mod 2021)2 mod 2021 = 833

594 mod 2021 = (592 mod 2021)2 mod 2021 = 1466

592 mod 2021 = (59 mod 2021)2 mod 2021 = 1460

59 mod 2021 = 59

d):

M = Cd mod n = 18961759 mod 2021 = 59

Hạ bậc

18961759 mod 2021 = 59

18961759 mod 2021 = [(1896879 mod 2021)2 \* 1896] mod 2021 = 59

1896879 mod 2021 = [(1896439 mod 2021)2 \* 1896] mod 2021 = 1933

1896439 mod 2021 = [(1896219 mod 2021)2 \* 1896] mod 2021 = 1196

1896219 mod 2021 = [(1896109 mod 2021)2 \* 1896] mod 2021 = 145

1896109 mod 2021 = [(189654 mod 2021)2 \* 1896] mod 2021 = 729

189654 mod 2021 = (189627 mod 2021)2 mod 2021 = 465

189627 mod 2021 = [(189613 mod 2021)2 \* 1896] mod 2021 = 441

189613 mod 2021 = [(18966 mod 2021)2 \* 1896] mod 2021 = 957

18966 mod 2021 = (18963 mod 2021)2 mod 2021 = 613

18963 mod 2021 = [(1896 mod 2021)2 \* 1896] mod 2021 = 1182

1896 mod 2021 = 1896

e)

Thực hiện nhiệm vụ bảo mật

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 xA = 307

Hãy cho biết

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

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

c) Cách An giải bản mã (C1, C2)?

Giải:

a)

yA = a xA mod q = 5307 mod 6827

Hạ bậc:

5307 mod 6827 = 2388

5307 mod 6827 = [(5153 mod 6827)2 \* 5] mod 6827 = 2388

5153 mod 6827 = [(576 mod 6827)2 \* 5] mod 6827 = 1607

576 mod 6827 = (538 mod 6827)2 mod 6827 = 842

538 mod 6827 = (519 mod 6827)2 mod 6827 = 2748

519 mod 6827 = [(59 mod 6827)2 \* 5] mod 6827 = 2063

59 mod 6827 = [(54 mod 6827)2 \* 5] mod 6827 = 603

54 mod 6827 = (52 mod 6827)2 mod 6827 = 625

52 mod 6827 = (5 mod 6827)2 mod 6827 = 25

5 mod 6827 = 5

yA = 2388

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

b)

K = (yA)k mod q = 2388919 mod 6827

Hạ bậc:

2388919 mod 6827 = 5072

2388919 mod 6827 = [(2388459 mod 6827)2 \* 2388] mod 6827 = 5072

2388459 mod 6827 = [(2388229 mod 6827)2 \* 2388] mod 6827 = 4642

2388229 mod 6827 = [(2388114 mod 6827)2 \* 2388] mod 6827 = 5154

2388114 mod 6827 = (238857 mod 6827)2 mod 6827 = 4920

238857 mod 6827 = [(238828 mod 6827)2 \* 2388] mod 6827 = 6583

238828 mod 6827 = (238814 mod 6827)2 mod 6827 = 6235

238814 mod 6827 = (23887 mod 6827)2 mod 6827 = 4987

23887 mod 6827 = [(23883 mod 6827)2 \* 2388] mod 6827 = 2015

23883 mod 6827 = [(2388 mod 6827)2 \* 2388] mod 6827 = 1539

2388 mod 6827 = 2388

K = 5072

C1 = ak mod q = 5919 mod 6827

Hạ bậc:

5919 mod 6827 = 4977

5919 mod 6827 = [(5459 mod 6827)2 \* 5] mod 6827 = 4977

5459 mod 6827 = [(5229 mod 6827)2 \* 5] mod 6827 = 5610

5229 mod 6827 = [(5114 mod 6827)2 \* 5] mod 6827 = 1348

5114 mod 6827 = (557 mod 6827)2 mod 6827 = 6290

557 mod 6827 = [(528 mod 6827)2 \* 5] mod 6827 = 2714

528 mod 6827 = (514 mod 6827)2 mod 6827 = 1475

514 mod 6827 = (57 mod 6827)2 mod 6827 = 123

57 mod 6827 = [(53 mod 6827)2 \* 5] mod 6827 = 3028

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

5 mod 6827 = 5

C1 = 4977

C2 = KM mod q = 5072\*474 mod 6827 = 1024

(C1, C2) = (4977, 1024)

c)

K = (C1)xA mod q = 4977307 mod 6827

Hạ bậc:

4977307 mod 6827 = 5072

4977307 mod 6827 = [(4977153 mod 6827)2 \* 4977] mod 6827 = 5072

4977153 mod 6827 = [(497776 mod 6827)2 \* 4977] mod 6827 = 6122

497776 mod 6827 = (497738 mod 6827)2 mod 6827 = 826

497738 mod 6827 = (497719 mod 6827)2 mod 6827 = 1368

497719 mod 6827 = [(49779 mod 6827)2 \* 4977] mod 6827 = 3955

49779 mod 6827 = [(49774 mod 6827)2 \* 4977] mod 6827 = 1856

49774 mod 6827 = (49772 mod 6827)2 mod 6827 = 4472

49772 mod 6827 = (4977 mod 6827)2 mod 6827 = 2173

4977 mod 6827 = 4977

K = 5072

K-1 mod q = 5072-1 mod 6827 = 4174

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 6827 | 0 | 1 | 5072 |
| 1 | 0 | 1 | 5072 | 1 | -1 | 1755 |
| 2 | 1 | -1 | 1755 | -2 | 3 | 1562 |
| 1 | -2 | 3 | 1562 | 3 | -4 | 193 |
| 8 | 3 | -4 | 193 | -26 | 35 | 18 |
| 10 | -26 | 35 | 18 | 263 | -354 | 13 |
| 1 | 263 | -354 | 13 | -289 | 389 | 5 |
| 2 | -289 | 389 | 5 | 841 | -1132 | 3 |
| 1 | 841 | -1132 | 3 | -1130 | 1521 | 2 |
| 1 | -1130 | 1521 | 2 | 1971 | -2653 | 1 |

B3 = 1 => B2 = -2653 mod 6827 = 4174

K-1 mod q = 4174

M = (C2K-1) mod q = 4977\*4174 mod 6827 = 474

5. 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) = 9

An và Ba thống nhất các giá trị: p = 47, q = 23, h = 25

và An chọn xA = 2, k = 3

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

Giải:

a)

g = h(p-1)/q mod p = 25(47-1)/23 mod 47 = 252 mod 47 = 14

yA = gxA mod p = 142 mod 47 = 8

b)

r = (gk mod p) mod q = (143 mod 47) mod 23 = 18 mod 23 = 18

s = (k-1(H(M) + xA\*r)) mod q = (3-1(9 + 2\*18)) mod 23

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | A1 | A2 | A3 | B1 | B2 | B3 |
| - | 1 | 0 | 23 | 0 | 1 | 3 |
| 7 | 0 | 1 | 3 | 1 | -7 | 2 |
| 1 | 1 | -7 | 2 | -1 | 8 | 1 |

B3 = 1 => B2 = 8 mod 23 = 8

3-1 = 8

s = (8(9 + 36)) mod 23

s = (8\*45) mod 23

s = 360 mod 23 = 15

(r, s) = (18, 15)

c)

w = s-1(mod q)

w = 15-1 mod 23 = 20

u1= (H(M).w)(mod q)

u1 = (9 \* 20) mod 23 = 19

u2= (r.w)(mod q)

u2 = (18\*20) mod 23 = 15

v = (gu1.yu2(mod p)) (mod q)

gu1 mod p = 1419 mod 47

Hạ bậc:

1419 mod 47 = 36

1419 mod 47 = [(149 mod 47)2 \* 14] mod 47 = 36

149 mod 47 = [(144 mod 47)2 \* 14] mod 47 = 4

144 mod 47 = (142 mod 47)2 mod 47 = 17

142 mod 47 = (14 mod 47)2 mod 47 = 8

14 mod 47 = 14

yAu2 mod p = 815 mod 47

Hạ bậc:

815 mod 47 = 24

815 mod 47 = [(87 mod 47)2 \* 8] mod 47 = 24

87 mod 47 = [(83 mod 47)2 \* 8] mod 47 = 12

83 mod 47 = [(8 mod 47)2 \* 8] mod 47 = 42

8 mod 47 = 8

v = (36.24(mod 47)) (mod 23) = 18 mod 23 = 18

Ta thấy v = r :

=> Đúng