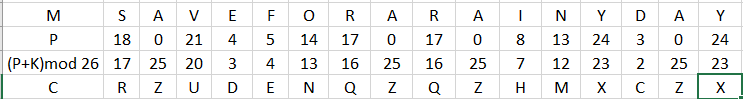
# Chương 1 : Mã hóa cổ điển

1. MẬT MÃ CAESARInput: M = SAVEFORARAINYDAY  
Key: K = 25  
Tìm Output: C =

****

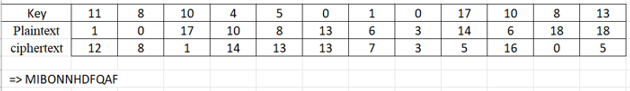
* **C : RZUDENQZQZHMXCZX**

**2. MẬT MÃ VIGENERE – LẶP KHÓA**Input: M = WHENINROMEDOKey: K = THETRUTHETRUTìm Output: C =

****

* **C:POIGZHKVQXUI**

3. MẬT MÃ VIGENERE – AUTOKEYInput: M = BARKINGDOGSS  
Key: K = LIKEFA  
Tìm Output: C =

****

=>**C:MIBONNHDFQAF**

4. MÃ HÓA CHỮ ĐƠNInput: M = PENNYWISEPOUNDFO  
Key: K = KGOXPMUHCAYTJQWZRIVESFLDNB  
Tìm Output: C =

Bảng giá trị tương ứng được xây dựng bởi bảng chữ cái và khóa K :

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

Bảng bản rõ : PENNYWISEPOUNDFO

Với từng kí tự trên bản rõ ta sẽ thay thế tương theo bảng trên :

* **C : ZPQQNLCVPZWSQXMW**

5. MẬT MÃ MA TRẬN KHÓA PLAYFAIRInput: M = STILLWATERSR  
Key: K = SAVEFORA  
Tìm Output: C =

Ta có ma trận khóa 5x5(với i,j chung giá trị)

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

Chia cặp cho bản rõ M ta đc :

M = ST IL LW AT ER SR

*Nguyên tắc mã hóa :*

1. *với các cặp nằm trên một hàng của ma trận thì mã hóa bằng cách dịch phải 1 cột với các chữ ở cuối khi dịch sẽ quay về cột đầu*
2. *các cặp nằm trên một cột của ma trận thì mã hóa bằng cách dịch xuống 1 hàng nếu ở hàng cốt thì quay về hàng đầu*
3. *các cặp ở khác hàng khác cột : thì đc mã hóa bằng chữ cái cùng hàng với chứ đó và cùng cột với chữ còn lại trong cặp.*

Áp dụng 3 nguyên tắc trên ta có các cặp đc mã hóa tương ứng là :

* + ST 🡪 FM (NT3)
  + IL 🡪 KG (NT1)
  + LW🡪 HZ(NT3)
  + AT🡪 FN(NT3)
  + ER🡪 AC (NT3)
  + SR🡪 AO (NT3)
* **C : FMKGHZFNACAO**

6. MẬT MÃ HOÁN VỊInput: M = TIMEISMONEYTIMEISM  
Key: K = 5  
Tìm Output: C =

Ta có k = 5

Có bảng mã hóa :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| T | I | M | E | I |
| S | M | O | N | E |
| Y | T | I | M | E |
| I | S | M |  |  |

Từ bảng trên ta có bảng mã bằng cách lấy theo dừng cột : **TSYIIMTSMOIMENMIEE**

# Chương 2: Modulo

**1.** TÍNH LŨY THỪA MODULO 𝒃 = 𝒂𝒎 𝒎𝒐𝒅 𝒏 BẰNG CÁCH HẠ BẬC LŨY THỪAInput: a = 281; m = 764; n = 6967  
Tìm Output: b =

281 764 mod 6967 = (281 382 mod 6967)2  mod 6967 =667

281 382 mod 6967 = (281 191 mod 6967)2  mod 6967 =4378

281 191 mod 6967 = [(281 95 mod 6967)2  .281] mod 6967 =6708

281 95 mod 6967 = [(281 47 mod 6967)2  . 281] mod 6967 =4715

281 47 mod 6967 = [(281 23 mod 6967)2  . 281] mod 6967 =995

281 23 mod 6967 = [(281 11 mod 6967)2  . 281] mod 6967 =6549

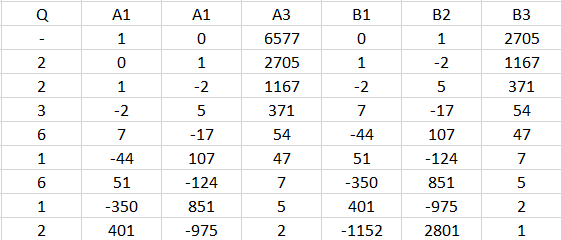
281 11 mod 6967 = [(281 5 mod 6967)2  . 281] mod 6967 =3499

281 5 mod 6967 = [(281 2 mod 6967)2  . 281] mod 6967 =3877

281 2 mod 6967 = 2324

**b=667**

**2.** TÌM NGHỊCH ĐẢO 𝒙 = 𝒂-𝟏 𝒎𝒐𝒅 𝒏 THEO ĐỊNH NGHĨA VÀ THUẬT TOÁN EUCLID – MỞRỘNGInput: a = 2705; n = 6577  
Tìm Output: x =



**b=2801**  
**3.** SỬ DỤNG ĐỊNH LÝ FERMAT ĐỂ TÍNH LŨY THỪA MODULO 𝒃 = 𝒂𝒎 𝒎𝒐𝒅 𝒏  
Input: a = 499; m = 6337; n = 6337  
Tìm Output: b =

Ta thấy : 6337 là số nguyên tố => 4996337mod 6337 = 499 mod 6337=499

4.TÍNH GIÁ TRỊ HÀM EULER φ(n).  
Input: n = 2863  
Tìm Output: φ(n) =

Output: φ(2863) = ø(409.7) = (409–1)×(7–1) =408×6 = 2448

5.SỬ DỤNG ĐỊNH LÝ EULER ĐỂ TÍNH LŨY THỪA MODULO 𝒃 = 𝒂𝒎 𝒎𝒐𝒅 𝒏  
Input: a = 27; m = 2201; n = 5400  
Tìm Output: b =

Ta có: φ(5400) = φ(23\*33\*52)

= φ(23)\* φ(33)\* φ(52)

= (23-22)\*(33-32)\*(52-5)

= 1440

=> 27 2201 mod 5400 = 271441+760 mod 5400

= 271441.27760 mod 5400

* 27 1441 mod 5400 = 27 mod 5400 = 27
* 27 760 mod 5400=4401

27 760 mod 5400 = (27 380 mod 5400)2 mod 5400 =4401

27 380 mod 5400 = (27 190 mod 5400)2 mod 5400 =4401

27 190 mod 5400 = (27 80 mod 5400)2 mod 5400 =4401

27 80 mod 5400 = (27 40 mod 5400)2  mod 5400 =4401

27 40 mod 5400 = (27 20 mod 5400)2 mod 5400 =4401

27 20 mod 5400 = (27 10 mod 5400)2  mod 5400 =4401

27 10 mod 5400 = (27 5 mod 5400)2 mod 5400 =5049

27 5 mod 5400 = [(27 2 mod 5400)2  .27]mod 5400 =1107

27 2 mod 5400 = 729

**b=27\*4401 mod 5400 = 27**

6. SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ TÍNH LŨY THỪA modulo 𝒃 = 𝒂𝒌 𝒎𝒐𝒅 𝒏  
Input: a = 101; k = 76; n = 49913  
Tìm Output: b =

A = 10176 ,

n=49913=19\*37\*71

m1 = 19, m2 = 37 ,m3=71

+) tính theo các Modul thành phần

A1=10176 mod19=(10172 mod 19\*1014mod19) mod 19

=4 mod 19

= 4

A2=10176 mod 37=(10172 mod 37\*1014mod37) mod 37

=10 mod 37

= 10

A3=10176mod 71=(10170 mod 71\*1016mod71) mod 71

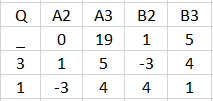
=45 mod 71

= 45

+) Tính kết quả A mod M

Khi đó M1=2627 ; M2= 1349 ; M3=703

M1-1=2627-1 mod 19 = 4



Tương tự: M2-1=1349-1 mod 37 =24

M3-1=703-1 mod 71 = 10

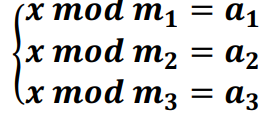
+)Tính ci =Mi\* (Mi-1 mod mi)

c1=19\*4=76

c2=37\*24=888

c3=71\*10=710

A = (76\*4 + 888\*10+710\*45) mod 49913=41134

**7. SỬ DỤNG ĐỊNH LÝ SỐ DƯ TRUNG HOA ĐỂ GIẢI HỆ PHƯƠNG TRÌNH MODULO.**  
  
Input: m1 = 11; m2 = 13; m3 = 17; a1 = 6; a2 = 2; a3 = 4;  
Tìm Output: x =

Ta có M = m1\*m2\*m3 = 11\*13\*17 = 2431

* M1 = M/m1 = 2431/11 = 221

M2 = 187

M3 = 143

Ta tính:

M1-1 mod m1 = 221-1 mod 11 = 1

M2-1 mod m2 = 187-1 mod 13 = 8

M3-1 mod m3 = 143-1 mod 17 = 5

Như vậy:

X = A = (a1\*c1 + a2\*c2 + a3\*c3) mod M

= (6\*221\*1 + 2\*187\*8 + 4\*143\*5) mod 2431

= 7178 mod 2431 = 2316

**8. KIỂM TRA SỐ NGUYÊN A CÓ LÀ MỘT CĂN NGUYÊN THỦY CỦA SỐ NGUYÊN N?**Input: a = 11; n = 293Tìm Output: a có là căn nguyên thủy của n không?

Ta có: ø(293) = 292

Áp dụng định lý Euler ta có: 11292 mod 293 = 1 vì GCD(11,293)=1

Ta có tập ước của 292 là m ={2,73,146}

+ xét 112 mod 293 = 121

+ xét 1173 mod 293 = 155

+ xét 11146 mod 293 = 292

A là căn nguyên thủy của 293

**9.** TÌM **LOGARITHM RỜI RẠC CỦA SỐ b VỚI CƠ SỐ 𝒂 (𝒎𝒐𝒅 𝒏), 𝒌 = 𝐥𝐨𝐠𝒂 𝒃 (𝒎𝒐𝒅 𝒏).**Input: a = 3; b = 8; n = 19Tìm Output: k =

k = log­38(mod19)

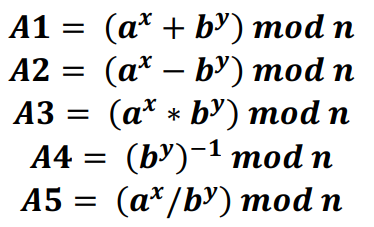
Ta có: 30 mod 19 = 1

31 mod 19 = 3

32 mod 19 = 9

33 mod 19 = 8

* K = log­38(mod19) = 3

10. TÍNH CÁC BIỂU THỨC MODULO CƠ BẢN  
Input: a = 83; b = 17; x = 354; y = 314; n = 241  
Tìm Output: A1 = ; A2 = ; A3 = ; A4 = ; A5 = ?

A1 = (ax + by) mod n

= (83354 + 17314) mod 241

= [(83354 mod 241) + (17314 mod 241)] mod 241

Ta có: 83 và 241 nguyên tố cùng nhau

Và 17 và 241 nguyên tố cùng nhau

Do đó ta có:

A1 = (83240+114 mod 241 + 17240+74 mod 241) mod 241

= (83114 mod 241 + 1774 mod 241) mod 241

Tính (1):

83114 mod 241 = (8357 mod 241)2 mod 241 = 143

8357 mod 241 = [(8328 mod 241)2 \*83] mod 241 = 25

8328 mod 241 = (8314 mod 241)2 mod 241 = 94

8314 mod 241 = (837 mod 241)2 mod 241 = 217

837 mod 241 = [(833 mod 241)2 \*83] mod 241 = 159

833 mod 241 = [(83mod 241)2 \*83] mod 241 = 135

Tính (2):

1774 mod 241 = (1737 mod 241)2 mod 241 = 116

1737 mod 241 = [(1718 mod 241)2 \*17] mod 241 = 57

1718 mod 241 = (179 mod 241)2 mod 241 = 79

179 mod 241 = [(174 mod 241)2 \*17] mod 241 = 140

174 mod 241 = (172 mod 241)2 mod 241 = 135

172 mod 241 = 48

* A1 = (143 + 116) mod 241 = 18

A2 = (ax - by) mod n

= (83354 - 17314) mod 241

= [(83354 mod 241) - (17314 mod 241)] mod 241

Tính như trên ta có :

83354 mod 241 = 143

17314 mod 241 = 116

* A2 = (143 - 116) mod 241 =27

A3 = (ax \* by) mod n

= (83354 \* 17314) mod 241

= [(83354 mod 241) \* (17314 mod 241)] mod 241

Tính như trên ta có :

83354 mod 241 = 143

17314 mod 241 = 116

* A3 = (143 \* 116) mod 241 =200

A4 = (by)-1 mod n

= (17314)-1 mod 241

= (17314 mod 241)-1 mod 241

Tính như trên ta có : 17314 mod 241 = 116

Do đó: A4 = 116-1 mod 241

Theo Euclid mở rộng ta có:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q** | **A2** | **A3** | **B2** | **B3** |
| ~ | 0 | 241 | 1 | 116 |
| 2 | 1 | 116 | -2 | 9 |
| 12 | -2 | 9 | 25 | 8 |
| 1 | 25 | 8 | -27 | 1 |

* A4 = -27 + 241 = 214

A5 = ( ) mod n

= () mod 241

= (83354 \* (17314)-1) mod 241

= [(83354 mod 241) \* ((17314)-1 mod 241))] mod 241

Tính như trên ta có :

83354 mod 241 = 143

(17314)-1 mod 241 = 214

* A5 = (143 \* 214) mod 241 =236

# Chương 3: DES

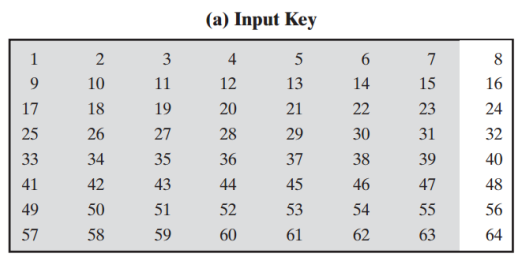
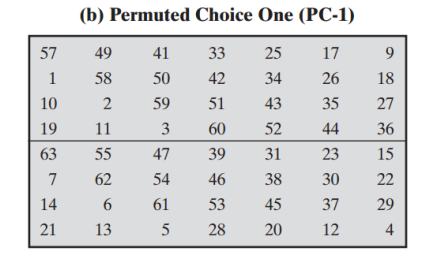
INPUT: K (là input bài 1) = 3FF81CDA5F417784;  
M (là input bài 4) = FF1C9CA3596B7D48;  
OUTPUT: Tìm C (kết quả bài 11) = C727541BBA49D95D

## **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 =

K = 3FF81CDA5F417784 = 0011 1111 1111 1000 0001 1100 1101 1010 0101 1111 0100 0001 0111 0111 1000 0100

|  |  |
| --- | --- |
| 0011 1111  1111 1000  0001 1100  1101 1010  0101 1111  0100 0001  0111 0111  1000 0100 | 1000 1010 0111 1010 0100 0011 0101  0101 1001 1101 0101 0001 1111 1111 |

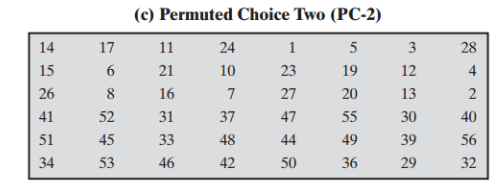
PC1=1000 1010 0111 1010 0100 0011 0101 0101 1001 1101 0101 0001 1111 1111

* C0 = 1000 1010 0111 1010 0100 0011 0101
* D0 = 0101 1001 1101 0101 0001 1111 1111

**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 =

|  |  |  |  |
| --- | --- | --- | --- |
| i | Si | PC1K | |
| Ci | Di |
| 0 |  | 1000101001111010010000110101 | 0101100111010101000111111111 |
| 1 | 1 | 0001010011110100100001101011 | 1011001110101010001111111110 |
| 2 | 1 | 0010100111101001000011010110 | 0110011101010100011111111101 |
| 3 | 2 | 1010011110100100001101011000 | 1001110101010001111111110101 |
| 4 | 2 | 1001111010010000110101100010 | 0111010101000111111111010110 |
| 5 | 2 | 0111101001000011010110001010 | 1101010100011111111101011001 |
| 6 | 2 | 1110100100001101011000101001 | 0101010001111111110101100111 |
| 7 | 2 | 1010010000110101100010100111 | 0101000111111111010110011101 |
| 8 | 2 | 1001000011010110001010011110 | 0100011111111101011001110101 |
| 9 | 1 | 0010000110101100010100111101 | 1000111111111010110011101010 |
| 10 | 2 | 1000011010110001010011110100 | 0011111111101011001110101010 |
| 11 | 2 | 0001101011000101001111010010 | 1111111110101100111010101000 |
| 12 | 2 | 0110101100010100111101001000 | 1111111010110011101010100011 |
| 13 | 2 | 1010110001010011110100100001 | 1111101011001110101010001111 |
| 14 | 2 | 1011000101001111010010000110 | 1110101100111010101000111111 |
| 15 | 2 | 1100010100111101001000011010 | 1010110011101010100011111111 |
| 16 | 1 | 1000101001111010010000110101 | 0101100111010101000111111111 |

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** = .

****

**K1 =** 1110 0001 0101 1011 0000 1000 1111 1100 1001 0110 0100 1111

## 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 =

M=FF1C9CA3596B7D48

=1111111100011100100111001010001101011001011010110111110101001000

IP(M) = 11110001010101110100011101111001 00001101011010011111011100101001

L0= F1574779

R0=0D69F729

**========== 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 =

R0= 0000 1101 0110 1001 1111 0111 0010 1001

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| R0 | 0000 | 1101 | 0110 | 1001 | 1111 | 0111 | 0010 | 1001 |
| ER0 | 100001 | 011010 | 101101 | 010011 | 111110 | 101110 | 100101 | 010010 |

ER0 = 100001 011010 101101 010011 111110 101110 100101 010010

**6. Thực hiên XOR ER0 với khóa K1  
Input:** ER0 (kết quả bài 5) , K1 (kết quả bài 3) **Output:** A =

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ER0 | 100001 | 011010 | 101101 | 010011 | 111110 | 101110 | 100101 | 010010 |
| K1 | 111000 | 010101 | 101100 | 001000 | 111111 | 001001 | 011001 | 001111 |
| A | 011001 | 001111 | 000001 | 011011 | 000001 | 100111 | 111110 | 011101 |

A= 64 F0 5B 06 7F 9D

**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) =

A= 64 F0 5B 06 7F 9D

= 01100100 11110000 01011011 00000110 01111111 10011101

• 6-bit input qua mỗi Si ->cho ra 4-bit output

(Hàng = bit đầu + bit cuối , Cột = 4 bit giữa)

* 6 bit đầu qua bảng S1 ta có:

011001 => lấy hàng 01 = 1 , lấy cột 1100 = 12

=> được 9 =1001

Tương tự ta có:

+ 14 =1110 (hàng 1 cột 7 bảng S2)

+ 13 =1101 (hàng 1 cột 0 bảng S3)

+ 10 =1010 (hàng 1 cột 13 bảng S4)

+ 14 =1110 (hàng 1 cột 0 bảng S5)

+ 12 =1100 (hàng 3 cột 3 bảng S6)

+ 2 =0010 (hàng 2 cột 15 bảng S7)

+ 9 =1001 (hàng 1 cột 14 bảng S8)

* B = 1001 1110 1101 1010 1110 1100 0010 1001 = 9E DA EC 29

**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 =

A picture containing text, electronics, telephone

Description automatically generated

B = 9E DA EC 29 =1001 1110 1101 1010 1110 1100 0010 1001

A picture containing text, white, light

Description automatically generated **========= 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 =

R0= 0D 69 F7 29 = 0000 1101 0110 1001 1111 0111 0010 1001

L0= F1 57 47 79 = 1111 0001 0101 0111 0100 0111 0111 1001

F = 5D CD 0D DA = 0101 1101 1100 1101 0000 1101 1101 1010

L1 = R0 = 0D 69 F7 29

R1 = L0 ⊕ F = 1010 1100 1001 1010 0100 1010 1010 0011 =AC9A4AA3

# Chương 4:AES

## **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) = CFD61D489E7C48BC46C9F875C1F04E1B, **Output:** w0 = , w1 = , w2 = , w3 = ,

|  |  |
| --- | --- |
| Các Word | 4btye(32bit) |
| W0 | CFD61D48 |
| W1 | 9E7C48BC |
| W2 | 46C9F875 |
| W3 | C1F04E1B |

2. **Dịch vòng trái 1 byte đối với w3 (32 bit)  
Input:** w3 (kết quả bài 1) = **Output:** rw = RotWord(w3) =

|  |  |
| --- | --- |
| Word | RotWord |
| C1F04E1B | F04E1BC1 |

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) =

|  |  |  |
| --- | --- | --- |
| Word | RotWord | SubWord |
| C1F04E1B | F04E1BC1 | 8C2FAF78 |

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]) =

|  |  |  |
| --- | --- | --- |
| SubWord | Rc[1] | xcsw |
| 8C2FAF78 | 01 | 8C2FAF78 |

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**) =**

|  |  |
| --- | --- |
| W4 | 43F9B230 |
| W5 | DD85FA8C |
| W6 | D9E9650B |
| W7 | 18192B10 |

## **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)**

A screenshot of a computer

Description automatically generated with medium confidence **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)**

Table

Description automatically generated8. **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)**

Table

Description automatically generated9. **Trộn các byte trong state MixColumns (tài liệu mục 5.3, trang 162)  
Input:** state (kết quả bài 8) = , **Output:** state = **MixColumns (state)**

Table

Description automatically generatedA picture containing text

Description automatically generated

Kết quả cột 1

{02}.{0E} + {03}{85} + {01}.{42} + {01}.{4E}

{02}.{0E} : {0E} = 0000 1110 =>{02}.{0E} = 0001 1100

{03}{85} = {85} + {85}{02}

{85} = 1000 0101 => {85}{02} = 1 0000 1010 + 1 0001 1011 = 0001 0001

{03}{85} = 1000 0101 + 0001 0001 = 1001 0100

{01}.{42} = {42} = 0100 0010

{01} {4E} = {4E} = 0010 1110

{02}.{0E} + {03}{85} + {01}.{42} + {01}.{4E}

= 0001 1100 + 1001 0100 + 0100 0010 + 0010 1110 = 11100100 = {E4}

{01}.{0E} + {02}{85} + {03}.{42} + {01}.{4E} :

{01}.{0E} ={ 0E} = 0000 1110

{02}{85} = 0001 0001 (theo ý trên)

{03}.{42} = {42} + {02}{42}

{42} = 0100 0010 => {42}{02} = 1000 0100

=> {03}.{42} = = 0100 0010 + 1000 0100 = 1100 0110

{01}.{4E} = 0010 1110 (theo ý trên)

{01}.{0E} + {02}{85} + {03}.{42} + {01}.{4E} = 1111 0111 = {F7}

{01}.{0E} + {01}{85} + {02}.{42} + {03}.{4E} :

{01}.{0E} = 0000 1110

{01}{85} = 1000 0101

{02}.{42} = 1000 0100

{03}.{4E} = {4E} + {02}{4E} = 0100 1110 + 1001 1100 = 1101 0010

{01}.{0E} + {01}{85} + {02}.{42} + {03}.{4E} = 1101 1101 = {DD}

{03}.{0E} + {01}{85} + {01}.{42} + {02}.{4E} :

{03}.{0E} = {0E} + {0E}{02} = 0000 1110 + 0001 1100 = 0001 0010

{01}{85} = 1000 0101 1001 0111

{01}.{42} = 0100 0010 1101 1110

{02}.{4E} : {4E} = 0100 1110 =>{02}.{4E} = 1001 1100

{03}.{0E} + {01}{85} + {01}.{42} + {02}.{4E} = 0100 1001 = {47}

Kết quả cột 2

{02}.{67} + {03}{85} + {01}{21} + {01}{FB} :

{67} = 0110 0111 => {67}{02} = 1100 1110

{03}{85} = 1001 0100 (Theo ý trên)

{01}{21} = 0010 0001

{01}{ FB } = 1111 1010

{02}.{67} + {03}{85} + {01}{21} + {01}{FB}= 1000 0001 = {81}

{01}.{67} + {02}{85} + {03}{21} + {01}{FB} :

{01}.{67} = 0110 0111

{02}{85} = 0001 0001 (ý trên)

{03}{21} = {21} + {21}{02}

{21} = 0010 0001 => {21}{02} = 0100 0010

{03}{21} = {21} + {21}{02} = 0010 0001 + 0100 0010 = 0110 0011

{01}{FB} = 1111 1011

{01}.{67} + {02}{85} + {03}{21} + {01}{FB} = 1110 1110 = {EE}

{01}.{67} + {01}{85} + {02}{21} + {03}{FB} :

{01}.{67} = 0110 0111

{01}{85} = 1000 0101

{02}{21} = 0100 0010 (ý trên)

{03}{FB} :

{FB} = 1111 1011 => {FB}{02} = 1 1111 0110 + 1 0001 1011 = 1110 1101

{03}{FB} = {FB} + {FB}{02} = 1111 1011 + 1110 1101 = 0001 0110

{01}.{67} + {01}{85} + {02}{21} + {03}{FB} = 1011 0110 = {B6}

{03}.{67} + {01}{85} + {01}{21} + {02}{FB} :

{03}.{67} = {67} + {67}{02} = 0110 0111 + 1100 1110(cmt) = 1010 1001

{01}{85} = 1000 0101

{01}{21} = 0010 0001

{02}{FB} = 1110 1101 (cmt)

{03}.{67} + {01}{85} + {01}{21} + {02}{FB} = 1110 0000 = {E0}

Kết quả cột 3

{02}.{5D} + {03}{3C} + {01}{96 } + {01}{A7} :

{02}.{5D} : {5D} = 0101 1101=>{02}.{5D} = 1011 1010

{03}{3C}:

{3C} = 0011 1100 =>{02}{3C} = 0111 1000

{03}{3C} = {3C} +{02}{3C} = 0011 1100 + 0111 1000 = 0100 0100

{01}{96 } = 1001 0110

{01}{A7} = 1010 0111

{02}.{5D} + {03}{3C} + {01}{96 } + {01}{A7} = 1100 1111 = {CF}

{01}.{5D} + {02}{3C} + {03}{96} + {01}{A7} :

{01}.{5D} = 0101 1101

{02}{3C} = 0111 1000 (cmt)

{03}{96} :

{96} = 1001 0110 => {02}{96} = 1 0010 1100 + 1 0001 1011 = 0011 0111

{03}{96} = {96} + {02}{96} = 1001 0110 + 0011 0111 = 1001 0001

{01}{A7} = 1010 0111

{01}.{5D} + {02}{3C} + {03}{96} + {01}{A7} = 0001 0011 = {13}

{01}{5D} + {01}{3C} + {02}{96} + {03}{A7} :

{01}{5D} = 0101 1101

{01}{3C} = 0011 1100

{02}{96} = 0011 0111(cmt)

{03}{A7}

{A7} = 1010 0111 => {02}{A7} = 1 0100 1110 + 1 0001 1011 = 0101 0101

{03}{A7} = {A7} + {02}{A7} = 1010 0111 + 0101 0101 = 1111 0010

{01}{5D} + {01}{3C} + {02}{96} + {03}{A7} = 1010 0100 = {A6}

{03}{5D} + {01}{3C} + {01}{96} + {02}{A7} :

{03}{5D} = {5D} + {02}{5D} = 0101 1101 + 1011 1010 = 1110 0111

{01}{3C} = 0011 1100

{01}{96} = 1001 0110

{02}{A7} = 0101 0101 (cmt)

{03}{5D} + {01}{3C} + {01}{96} + {02}{A7} = 0001 1000 = {18}

Kết quả cột 4

{02}.{C1} + {03}{F6} + {01}{87} + {01}{73} :

{02}.{C1} :

{C1} = 1100 0001 =>{02}{C1} = 1 1000 0010 + 1 0001 1011 = 1001 1001

{03}{F6} :

{F6} = 1111 0110 =>{02}{F6} = 1 1110 1100 + 1 0001 1011 =1111 0111

{03}{F6} = {F6} + {02}{F6} = 1111 0110 + 1111 0111 = 0000 0001

{01}{87} = 1000 0111

{01}{73} = 0111 0011

{02}.{C1} + {03}{F6} + {01}{87} + {01}{73} = 0110 1100 = {6C}

{01}.{C1} + {02}{F6} + {03}{87} + {01}{73} :

{01}.{C1} = 1100 0001

{02}{F6} = 1111 0111 (cmt)

{03}{87}

{87} = 1000 0111 =>{02}{87} = 1 0000 1110 + 1 0001 1011 = 0001 0101

{03}{87} = {87} + {02}{87} = 1000 0111 + 0001 0101 = 1001 0010

{01}{73} = 0111 0011

{01}.{C1} + {02}{F6} + {03}{87} + {01}{73} = 1101 0111 = {D7}

{01}{C1} + {01}{F6} + {02}{87} + {03}{73} :

{01}{C1} = 1100 0001

{01}{F6} = 1111 0110

{02}{87} = 0001 0101 (cmt)

{03}{73} : {73} = 0111 0011 =>{02}{73} = 1110 0110

{03}{73} = {73} + {02}{73} = 0111 0011 + 1110 0110 = 1001 0101

{01}{C1} + {01}{F6} + {02}{87} + {03}{73} = {B7}

{03}.{ C1} + {01}{ F6} + {01}{87} + {02}{73} = 1011 0111 :

{03}.{ C1} = {C1} + {02}{C1} = 1100 0001 + 1001 1001(cmt) = 0101 1000

{01}{ F6} = 1111 0110 1010 1110

{01}{87} = 1000 0111 0110 0001

{02}{73} = 1110 0110(cmt)

{03}.{ C1} + {01}{ F6} + {01}{87} + {02}{73} = 1100 1111 = {CF}

MixColumns(state)

|  |  |  |  |
| --- | --- | --- | --- |
| E4 | 81 | CF | 6C |
| F7 | EE | 13 | D7 |
| DD | B6 | A6 | B7 |
| 47 | E0 | 18 | CF |

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)**===================== VÒNG LẶP THỨ 10 ===========

|  |  |  |  |
| --- | --- | --- | --- |
| E4 | 81 | CF | 6C |
| F7 | EE | 13 | D7 |
| DD | B6 | A6 | B7 |
| 47 | E0 | 18 | CF |

**+**

|  |  |  |  |
| --- | --- | --- | --- |
| CF | D6 | 1D | 48 |
| 9E | 7C | 48 | BC |
| 46 | C9 | F8 | 75 |
| C1 | F0 | 4E | 1B |

* STATE

|  |  |  |  |
| --- | --- | --- | --- |
| 81 | 57 | D3 | 24 |
| 69 | 92 | 5B | 6B |
| 9B | 7F | 4E | C2 |
| 96 | 10 | 56 | D5 |

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)**

# **Chương 5. Mã hóa 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 = 7523** **và a = 5 (là căn nguyên thủy của q).** **An chọn khóa riêng xA = 387** **Ba chọn khóa riêng xB = 247** Hãy cho biết **a) Cách An tính ra khóa công khai yA và khóa phiên K? yA = K =**

q=7523 **,** a=5

xA=387

yA=5387mod7523

5387mod7523 = [(5193 mod 7523)2.5] mod 7523 =2221

5193mod7523 = [(596 mod 7523)2.5] mod 7523 =1558

596mod7523 = (548 mod 7523)2 mod 7523 =5657

548mod7523 = (524 mod 7523)2mod 7523 =7168

524mod7523 = (512 mod 7523)2 mod 7523 =2270

512mod7523 = (56 mod 7523)2 mod 7523 =4229

56mod7523 = (53 mod 7523)2 mod 7523 =579

53 mod 7523 =125

* yA=2221

**K = yA xB mod q = 2221247 mod 7523**

2221247mod7523 = [(2221123 mod 7523)2. 2221] mod 7523 =7466

2221123mod7523 = [(222161 mod 7523)2. 2221] mod 7523 =6520

222161mod7523 = [(222130 mod 7523)2. 2221] mod 7523 =5219

222130mod7523 = (222115 mod 7523)2 mod 7523 =6605

222115mod7523 = [(22217 mod 7523)2. 2221] mod 7523 =6141

22217mod7523 = [(22213 mod 7523)2. 2221] mod 7523 =650

22213 mod 7523 =4685

* **K=7466**

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

q=7523 **,** a=5

xB=247

yB=5247mod7523

5247mod7523 = [(5123 mod 7523)2.5] mod 7523 =7477

5123mod7523 = [(561 mod 7523)2.5] mod 7523 =6286

561mod7523 = [(530 mod 7523)2.5] mod 7523 =1479

530mod7523 = (515 mod 7523)2 mod 7523 =5328

515mod7523 = [(57 mod 7523)2.5] mod 7523 =2015

57mod7523 = [(53 mod 7523)2.5] mod 7523 =2895

53 mod 7523 =125

* yB=7477

**K = yB xA mod q = 7477387 mod 7523=7466**

7477387mod7523 = [(7477193 mod 7523)2. 7477] mod 7523 =7466

7477193mod7523 = [(596 mod 7523)2. 7477] mod 7523 =4371

747796mod7523 = (747748 mod 7523)2 mod 7523 =189

747748mod7523 = (747724 mod 7523)2mod 7523 =6941

747724mod7523 = (747712 mod 7523)2 mod 7523 =1813

747712mod7523 = (74776 mod 7523)2 mod 7523 =3213

74776mod7523 = (74773 mod 7523)2 mod 7523 =3725

74773 mod 7523 =463

2. Thuật toán RSA - Bài toán 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Giả sử An chọn các giá trị p = 47** Hãy cho biết | **, q = 71** | **, e = 61** | **để tạo cặp khóa.** |

1. **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.**

Giả sử An chọn các giá trị p = 47 , q = 71 , e = 61

1. Khóa công khai của An: PU = {e, n} =
2. b) cách An tạo ra khóa riêng: PR = {d, n} =

p=47 && q=71

n=p\*q=47\*71=3337

ø(n)=46\*70=3220

e=61 thỏa mãn gcd(e,3220)=1

d=2481 bởi

2481\*61= 3220\*47+1=1

PU={61,3337 }

PR={2481,3337}

C ) M = 59: C =

M=59

C=Me mod n = 5961 mod 3337=3026

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

C=3026

M=Cd mod n = 30262481 mod 3337=59

3. Thuật toán RSA - Bài toán 2:

|  |  |  |  |
| --- | --- | --- | --- |
| **Giả sử An chọn các giá trị p = 47** Hãy cho biết | **, q = 71** | **, e = 61** | **để tạo cặp khóa.** |

1. **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.**

Ta có: n = p.q = 47 . 71 = 3337

Ø(n) = Ø(3337) =Ø(47) . Ø(71) = 46 . 70 = 3220

Có d = e-1 mod Ø(n) =61-1 mod 3220

Table

Description automatically generated

* d = 3220 – 739 = 2481

a,b, Khi đó PU={e,n} = {61,3337} , PR ={d,n} = {2481,3337}

c, Ba sử dụng mã công khai để giải mã:

C = Me mod n = 5961 mod 3337 = 3026



Hạ bậc: ((5930 mod 3337)2.59) mod 3337 = 3026

(5915 mod 3337)2  mod 3337 = 747

((597 mod 3337)2.59) mod 3337 = 2227

((593 mod 3337)2.59) mod 3337 = 2815

593 mod 3337 = 1822

d, An sẽ dùng mã riêng để giải bản mã

M = Cd mod n = 30262481 mod 3337 = 59

Hạ bậc:

((30261240 mod 3337)2 . 3026) mod 3337 = 59

((3026620 mod 3337)2 ) mod 3337 = 545

((3026310 mod 3337)2 ) mod 3337 = 598

((3026155 mod 3337)2 ) mod 3337 = 103

((302677 mod 3337)2 . 3026) mod 3337 = 520

((302638 mod 3337)2 . 3026) mod 3337 = 2176

((302619 mod 3337)2 ) mod 3337 = 2998

((30269 mod 3337)2 . 3026) mod 3337 = 1771

((30264 mod 3337)2 . 3026) mod 3337 = 2649

((30262 mod 3337)2 ) mod 3337 = 2704

(30262 mod 3337) = 3285

Vậy M =59

e, Việc mã hóa ở câu c) là thông điệp 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 = 7433 là một số nguyên tố, a = 3 là căn nguyên thủy của q.  
An chọn khóa riêng là xA = 341**Hãy cho biết **a) Khóa công khai của An: PU = {q, a, YA} với yA =  
b) Ba chọn số k = 872 để mã hóa bản tin M = 403 gửi cho An. Bản mã là (C1, C2) =  
c) Cách An giải bản mã (C1, C2)?**

a, yA=3341 mod 7433

3341 mod 7433 = [(3170 mod 7433)2.3] mod 7433 = 2124

3170 mod 7433 = (385 mod 7433)2mod 7433 = 757

385 mod 7433 = [(342 mod 7433)2.3] mod 7433 = 1347

342 mod 7433 = (321 mod 7433)2 mod 7433 = 4784

321 mod 7433 = [(310 mod 7433)2.3] mod 7433 = 3798

310 mod 7433 = (35 mod 7433)2 mod 7433 = 7018

35 mod 7433 = [(32 mod 7433)2.3] mod 7433 =243

32 mod 7433 = 9

* yA=2124

b,

K=(yA)k mod q = 2124872 mod 7433

2124872 mod 7433 = (2124436 mod 7433)2 mod 7433 =3190

2124436 mod 7433 = (2124218 mod 7433)2 mod 7433 =5747

2124218 mod 7433 = (2124109 mod 7433)2 mod 7433 =5096

2124109 mod 7433 = [(212454 mod 7433)2.2124] mod 7433 =4817

212454 mod 7433 = (212427 mod 7433)2 mod 7433 =6559

212427 mod 7433 = [(212413 mod 7433)2.2124] mod 7433 =3503

212413 mod 7433 = [(21246 mod 7433)2.2124] mod 7433 =4445

21246 mod 7433 = (21243 mod 7433)2 mod 7433 =2034

21243 mod 7433 =7303

* K = 3190

C1 = ak mod q = 3872 mod 7433

3872 mod 7433 = (3436 mod 7433)2 mod 7433 =2235

3436 mod 7433 = (3218 mod 7433)2 mod 7433 =5934

3218 mod 7433 = (3109 mod 7433)2 mod 7433 =4379

3109 mod 7433 = [(354 mod 7433)2.3] mod 7433 =2023

354 mod 7433 = (327 mod 7433)2 mod 7433 =692

327 mod 7433 = [(313 mod 7433)2.3] mod 7433 =3666

313 mod 7433 = [(36 mod 7433)2.3] mod 7433 =3661

36 mod 7433 = (33 mod 7433)2 mod 7433 =729

33 mod 7433 =27

* C1=2235

C2 = K.M mod q = 3190.403 mod 7433 = 7094

* Bản mã (2230,7094)

c , Bản mã (2230,7094)

Ta có : K = C1yA mod q = 2235341 mod 7433

2235341 mod 7433 = [(2235170 mod 7433)2. 2235] mod 7433 = 3190

2235170 mod 7433 = (223585 mod 7433)2mod 7433 = 5411

223585 mod 7433 = [(223542 mod 7433)2. 2235] mod 7433 = 1556

223542 mod 7433 = (223521 mod 7433)2 mod 7433 = 304

223521 mod 7433 = [(223510 mod 7433)2. 2235] mod 7433 = 3670

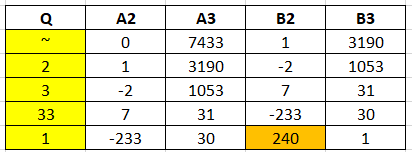
223510 mod 7433 = (22355 mod 7433)2 mod 7433 = 4452

22355 mod 7433 = [(22352 mod 7433)2. 2235] mod 7433 = 6249

22352 mod 7433 = 249

* K = 3190

Ta có : K-1 mod 7433 = 3190-1 mod 7433



* 3190-1 mod 7433 = 240

Bản gốc M = (C2.K-1)mod q

= (C2 mod q.K-1mod q) mod q

=(7094 mod 7433 .240) mod 7433

=(7094.240) mod 7433

=403

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) =  
An và Ba thống nhất các giá trị: p = 47, q = 23, h = 34  
và An chọn xA = 2, k = 10**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?**

a , xA = 2, K =10

yA = gxA mod p = 282 mod 47 = 32

b ,

r = (gkmod p)mod q

=(2810 mod 47) mod 23 (1)

Ta có :

2810 mod 47 = (285 mod 47)2mod 47 =4(2)

285 mod 47 = [(285 mod 47)2 .28]mod 47 =2

282 mod 47 = 32

Từ 1 và 2 => r = 4 mod 23 = 4

Chọn H(M) = 3

S = [K-1(H(M)+r)] mod q

= (10-1(3+2.4)) mod 23 = 8

* Chữ kí điện tử M(4,8)

C ,

W=s-1 mod q = 8-1mod 23 = 3

U1= (H(M).w)mod q = 3.3 mod 23 = 9

U2 = (r.w) mod q = 4.3 mod 23 = 12

V=[(yu1.yu2(mod q)] mod q = [(289.3212)mod 47]mod 23 = 4 mod 23 = 4

* Chữ kí đúng r = v