**ÔN TẬP CUỐI KỲ BẢO MẬT THÔNG TIN**

**Câu 1: Vận dụng các mã hoá cổ điển**

C1 = ?

C2 = ?

M

e2, k2

e1, k1

e2=Keyword-Ceasar

k2 = khongbiet

e1=play fair

k1 = bimat

M = hanhdonggiuadem

* Ma trận với từ khoá: BIMAT

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

* Mã hoá 2 chữ cái một lúc:

+ Nếu 2 chữ giống nhau, tách ra bởi 1 chữ điền thêm

+ Nếu 2 chữ cùng hàng, thay bởi các chữ bên phải

+ Nếu 2 chữ nằm cùng cột, thay bởi các chữ bên dưới

+ Các trường hợp khác, mỗi chữ cái được thay bởi chữ khác cùng hàng, trên cột chữ cái cùng cặp.

Ví dụ: Với M = hanhdonggiuadem thì:

HA NH DO NG XG IU AD EM

Tiến hành mã hoá:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| HA | NH | DO | NG | XG | IU | AD | EM |
| NB | OK | GK | OF | ZE | TQ | IF | LE |

Vậy C1 = NBOKGKOFZETQIFLE

* Mã hoá Keyword-Ceasar:

+ Khoá: khongbiet → Z26(10, 7, 14, 13, 6, 1, 8, 4, 19)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bản rõ | N | B | O | K | G | K | G | K | O | F | Z | E | T | Q | I | F | L | E |
| Số hoá | 13 | 1 | 14 | 10 | 6 | 10 | 6 | 10 | 14 | 5 | 25 | 4 | 19 | 16 | 8 | 5 | 11 | 4 |
| Khoá | 10 | 7 | 14 | 13 | 6 | 1 | 8 | 4 | 19 | 10 | 7 | 14 | 13 | 6 | 1 | 8 | 4 | 19 |
| MOD(SH+K, 26) | 23 | 8 | 2 | 23 | 12 | 11 | 14 | 14 | 7 | 15 | 6 | 18 | 6 | 22 | 9 | 13 | 15 | 23 |
| Chuyển chữ | X | I | C | X | M | L | O | O | H | P | G | S | G | W | J | N | P | X |

**Câu 2: Mã hoá DES**

110101

111111

4 bit

1111

8 bit

00001111

Hoán vị

54827631

M

10100110

R1

L1

0000

Hoán vị

331244

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S1 | 0 | 1 | 2 | 3 |
| 0 | 3 | 0 | 1 | 2 |
| 1 | 2 | 1 | 3 | 0 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S2 | 0 | 1 | 2 | 3 |
| 0 | 1 | 0 | 3 | 2 |
| 1 | 1 | 3 | 0 | 2 |

⊕

K: 001010

Chỉ số cột

B3 B2 B1

101

110

Chỉ số dòng

1111

**Câu 3: Các phương thức mã hoá khối:**

**M = 11010101 (P1 = 1101 | P2 = 0101)**

1. **N = 1011, K=1100**

**Các bước thực hiện:**

* Lấy P1 ⊕ N (1)
* (1) ⊕ K → C1
* Lấy C1 ⊕ P2  (2)
* (2) ⊕ K → C2
* Kết quả cuối cùng: C1C2

**Ví dụ:**

P1 1 1 0 1

⊕

N 1 0 1 1

0 1 1 0

⊕

K 1 1 0 0

C1 1 0 1 0

⊕

P2 0 1 0 1

1 1 1 1

⊕

K 1 1 0 0

C2 0 0 1 1

**Kết quả:** 1010011

1. **N = 110101, K=110001**

**Các bước thực hiện:**

* Đề cho S4 → dịch 4 bit, giữa lại 2 bit (1)
* Lấy N ⊕ K (2)
* (1) (2) ⊕ P1 → C1
* 2bit(giữ)|C1 ⊕ K (3)
* (3) → dịch 4 bit, giữa lại 2 bit (4)
* (4) ⊕ P2 → C2
* Kết quả cuối cùng: C1C2

**Ví dụ:**

N(4bit|2bit) 1 1 0 1|0 1

⊕

K 1 1 0 0 0 1

0 0 0 1 0 1

4bit 0 0 0 1

⊕

P1 1 1 0 1

C1 1 1 0 0

2bit(giữ)|C1  0 1|1 1 0 0

⊕

K 1 1 0 0 0 1

4bit 1 0 1 1|0 1

⊕

P2 0 1 0 1

C2 1 1 1 0

**Kết quả:** 11001110

1. **N = 11010, K=11001**

**Các bước thực hiện:** Tương tự như CFB tuy nhiên không sử dụng lại cùng khoá và IV

**Ví dụ:**

N(4bit|1bit) 1 1 0 1|0

⊕

K 1 1 0 0 1

0 0 0 1 1

K1 0 0 0 1

⊕

P1 1 1 0 1

C1 1 1 0 0

1bit(giữ)|K1  0|0 0 0 1

⊕

K 1 1 0 0 1

4bit 1 1 0 0|0

⊕

P2 0 1 0 1

C2 1 0 0 1

**Kết quả:** 11001001

1. **K=1001**

**Các bước thực hiện:**

* Đề cho Count 10 → 1010 (1)
* (1) ⊕ K (2)
* (2) ⊕ P1 → C1
* Tiếp tục tăng biến đếm + 1 → 1011 (3)
* (3) ⊕ K (4)
* (4) ⊕ P2 → C2

**Ví dụ:**

Cout 1:

10 1 0 1 0

⊕

K 1 0 0 1

0 0 1 1

⊕

P1 1 1 0 1

C1 1 1 1 0

Cout 2:

10+1 1 0 1 1

⊕

K 1 0 0 1

0 0 1 0

⊕

P2 0 1 0 1

C2 0 1 1 1

**Kết quả:** 11100111

**Câu 4: Áp dụng định lý Trung Hoa: Tính toán theo modulo số lớn**

**Cách giải:**

Để tính A mod M, với M khá lớn và A là biểu thức số học nào đó. Trước hết ta cần tính tất cả ai = A mod mi. Sau đó sử dụng công thức:

Trong đó: Mi = M/mi

**Ví dụ: Tính** **178 mod 77.**

Áp dụng định lý phần dư Trung hoa, ta coi:

A = 178 m1 = 7 m2 = 11

Khi đó: M1 = 11 M2 = 7

11-1 mod 7 = 6-1 mod 7 = 2 → c1 = 11 2= 22

7-1 mod 11 = 8 → c2 = 7 8= 56

a1  = 178 mod 7 = (17 mod 7)8 mod 7

= 38 mod 7 = (32)4 mod 7

= 24 mod 7 = 2

a2  = 178 mod 11 = (17 mod 11)8 mod 11

= 68 mod 11 = (62)4 mod 11

= 34 mod 11 = 4

Vậy A = 178 mod 77 = (a1 c1 + a2 c2) mod 77

= (222 + 4 56) mod 77

= 268 mod 77 = 37

**Câu 5: Thuật toán SHA – 1**

Cho M = 101001110000. Tính h(M) = ?

**Thuật toán h:**

* h = h1h2h3 ( h1 = 001, h2 = 011, h3 = 110)
* a = h1, b = h2, c = h3,

foreach(Mi ∈ M, Mi 6 bit)

{

foreach(wk ∈ Mi , wk 3bit , w3 = w1 ⊕ w2)

{

t = a « 1 + b ⊕ c + w1

c = b, b = a « 1, a = t

}

h1 = h1 + a , h2 = h2 + b , h3 = h3 + c

}

h = h1h2h3

**Bài giải:**

* a = 001, b = 011, c = 110
* M1 = 101001

+ w1 = 101

. t = 010 + (011 ⊕ 110) + 101 = 12 mod 8 = 4 = 100

. c = 011, b = 010, a = 100

+ w2 = 001

. t = 000 + (010 ⊕ 011) + 001 = 110

. c = 010, b = 000, a = 110

+ w3 = w1 ⊕ w2  = 101⊕ 001 = 100

. t = 101 + (000 ⊕ 010) + 100 = 011

. c = 000, b = 101, a = 011

+ h1 = 001+ 011 = 100,

h2 = 011+ 101 = 000,

h3 = 110+ 000 = 110.

* M2 = 110000

+ w1 = 110

. t = 110 + (101 ⊕ 000) + 110 = 001

. c = 101, b = 110, a = 001

+ w2 = 000

. t = 010 + (110 ⊕ 101) + 000 = 101

. c = 110, b = 010, a = 101

+ w3 = w1 ⊕ w2  = 110⊕ 000 = 110

. t = 010 + (010 ⊕ 110) + 110 = 100

. c = 010, b = 010, a = 100

+ h1 = 100+ 100 = 000,

h2 = 000+ 010 = 010,

h3 = 110+ 010 = 000.

* h = 000010000