###### Chương 1: Tổng quan về mật mã học

Tự ôn

###### Chương 2: Các hệ khóa bí mật

# 

A và B trao đổi tin nhắn bí mật với nhau sử dụng mã dịch vòng với khóa k= (2 số cuối của mã sinh viên) mod 6 +12. A có bản rõ như sau: Bản rõ = HOCCHAMCHISETHITOT

Hãy tìm bản mã A gửi cho B

B nhận được một trong các bản mã sau từ A.

Bản mã = DRMANTMFTMFT (Với k=19)

Bản mã = ESNBOUNGUNGU (Với k=20)

Bản mã = FTOCPVOHVOHV (Với k=21)

Biết A và B đã thống nhất sử dụng mã dịch vòng với khóa k=(2 số cuối của mã sinh viên) mod 3 +19

Biết A và B dùng hệ mật Affine để trao đổi thông tin bí mật với khóa k= (a,b), trong đó a= 5 và b=((2 số cuối của mã sinh viên) mod 4+ 5)\*a. Tìm bản mã của bản rõ: THIGIUAKY

Biết A và B dùng hệ mật Affine để trao đổi tin bí mật với khóa k=(11,2). Hãy tìm bản rõ của bản mã: DHOYDOGUP

Biết A và B dùng hệ mật Vigenere để trao đổi tin bí mật với khóa k=NOCOPY. Hãy mã hóa bản rõ: THIKHONGQUAYBAI

Biết A và B dùng hệ mật Vigenere để trao đổi tin bí mật với khóa k=TUGIAC. Hãy giải mã bản mã: THAWNIWCKCDQGAAVGJBXAVGIBI

Biết A và B dùng hệ mật Hill để trao đổi tin bí mật với khóa k=. Hãy mã hóa bản rõ: VIGENERE

Biết A và B dùng hệ mật Hill để trao đổi tin bí mật với khóa k=. Hãy giải mã bản mã: VCRC, biết bản mã được xếp theo hàng trước.

Biết A và B dùng hệ mật khóa chạy để trao đổi tin bí mật với khóa k= OCTOBER

Hãy mã hóa bản rõ: CRYPTOGRAPHYISINTERESTING

Biết A và B dùng hệ mật khóa chạy để trao đổi tin bí mật với khóa k=JULY

Hãy giải mã bản mã: FCYRAZVLGFUAPU

Biết A và B dùng hệ mật OTP: đơn giản là xor bit cả mã hóa và giải mã

Biết A và B dùng hệ mật hoán vị để trao đổi tin bí mật với khóa k (1,2,3,4,5,6,7,8)=(4, 1, 8, 2, 5, 7, 3, 6). Hãy mã hóa bản rõ: THISISTHEWAYICLEANMYFACE (THIS IS THE WAY I CLEAN MY FACE)

Biết A và B dùng hệ mật hoán vị để trao đổi tin bí mật với khóa k(1,2,3,4,5,6,7,8)=(2,7,4,8,1,5,3,6). Hãy giải mã bản mã: YDHRMICLNERREEAVSESTYWOE

Biết A và B muốn trao đổi tin bí mật. Đầu tiên A mã hóa bản rõ dùng hệ mật Affine với khóa k1=(17,3) sau đó tiếp tục mã hóa bản mã nhận được bằng hệ mật Vigenere với khóa k2=FRIDAY. Hãy tìm bản mã của bản rõ: WHATDIDYOUDOLASTMONDAY

Biết A mã hóa bản rõ theo hệ mật Hill với khóa k1= Sau đó A tiếp tục mã hóa với hệ mật khóa chạy với khóa k2= RULER, biết bản rõ xếp theo hàng trước. Hãy giải mã bản mã: YYFOEXNOUEOV

Giải mã bản mã: AFQRFSDLROFZ

Biết bản mã này thu được từ mã Affine và Q được mã hóa từ V, S được mã hóa từ N

PHẦN THÁM MÃ TỰ XEM LẠI VD VÀ TỰ ÔN

# DES qua IP, Ip-1. Hộp E, P

Cho xâu đầu vào

x=1101011111000110110001111000111000111100000001111111101111110000

1. Tìm đầu ra sau khi cho x đi qua IP
2. Tìm đầu ra sau khi cho x đi qua IP-1.
3. Tách x thành 2 nửa, tìm kết quả của mỗi nửa khi cho chúng đi qua hộp mở rộng E; hộp P

# DES qua hộp S

Tìm các kết quả sau:

1. Xâu x= 100110 đi qua hộp S1
2. Xâu x= 010110 đi qua hộp S2
3. Xâu x= 101111 đi qua hộp S3
4. Xâu x= 101010 đi qua hộp S4
5. Xâu x= 001101 đi qua hộp S5
6. Xâu x= 010110 đi qua hộp S6
7. Xâu x= 010110 đi qua hộp S7
8. Xâu x= 100111 đi qua hộp S8

# DES qua hộp S

Xâu x thu được bằng cách lấy MSV mod 64 rồi chuyển sang 6 bit nhị phân, cho xâu x qua hộp Si, với i=(MSV mod 8) +1, với MSV là 3 số cuối của mã sinh viên. Tìm kết quả nhận được.

# DES khóa k qua PC-1

Giả sử có xâu khóa 64 bit key=1101011111000110110001111000111000111100000001111111101111110000

Tìm kết quả khi cho key qua hộp PC-1

Cho xâu Ci-1Di-1 (56 bit) =11110000111100001111000011111000111111110000111110001111

Giả sử đang tính khóa cho vòng thứ i=(MSV mod 16)+1. Trong đó MSV=3 số cuối của mã sinh viên

1. Tính CiDi.
2. Tính Ki (cho đi qua PC-2)

# DES hoàn chỉnh

Cho bản rõ ở dạng hexa: AC256789AB34CDEF và khóa ở dạng hexa K= 35A29370DB21FE38.

1. Thực hiện mã hóa DES
2. Giải mã bản mã nhận được ở câu a)

# Xtime

Tính các giá trị sau:

1. xtime(A5)
2. xtime(4B)
3. xtime(79)
4. xtime(52)
5. xtime(EB)

# subbyte

Tìm kết quả khi cho các dữ liệu sau qua hộp S-Box, Inv-Sbox của AES

1. (AF, 14, 2C, 58)
2. (BC, 04, 9C, 18)
3. (0F, 47, C3, 45)

# Shiftrow

Tìm kết quả khi thực hiện shiftrow các dữ liệu sau của AES với số hàng của mỗi dữ liệu lần lượt là 3, 2, 4, 1

1. (AF, 14, 2C, 58)
2. (BC, 04, 9C, 18)
3. (0F, 47, C3, 45)

# Mixcolum

Cho mỗi cột trạng thái dữ liệu sau, hãy thực hiện mixcolum và Inv-Mixcolum

|  |
| --- |
| 0D |
| 4E |
| 38 |
| 95 |

b)

|  |
| --- |
| 24 |
| 61 |
| 50 |
| 87 |

# Mixcolum

Cho trạng thái dữ liệu sau, hãy thực hiện mixcolum và Inv-Mixcolum

|  |  |  |  |
| --- | --- | --- | --- |
| 32 | 0B | FE | 25 |
| 31 | 29 | 64 | 70 |
| 83 | CD | FA | 9B |
| 5A | B3 | 10 | 34 |

# Mở rộng khóa AES

Cho khóa AES dưới dạng hexa: key=0B 56 30 ED FA 45 23 41 57 90 83 A0 3C 4F 28 94

Hãy thực hiện mở rộng khóa

Cho khóa AES dưới dạng hexa: key=0B 56 30 ED FA 45 23 41 57 90 83 A0 3C 4F 28 94. Hãy mã hóa bản rõ dưới dạng hexa: 54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F

# Mã dòng RC4

Giả sử T[0]=17; T[1]=250; T[2]=254; T[3]=38. Hãy tìm các vị trí của S để thực hiện hoán đổi trong câu lệnh 7 của thuật toán KSA trong RC4 với các giá trị i sau:

1. i=1
2. i=2
3. i=3

# Mã dòng RC4

Giả sử S[1]=17; S[2]=254; S[3]=250. Hãy tìm các vị trí của S để thực hiện hoán đổi trong câu lệnh 6 của thuật toán PRGA trong RC4 với vòng lặp while lặp số lần như sau:

1. 1 lần
2. 2 lần
3. 3 lần

###### Chương 3: Các hệ mật khóa công khai.

# Tính gcd theo euclide

Tính gcd(196425,5756); gcd(3910164, 69072);

# Tính nghịch đảo theo euclide mở rộng

1. Tính 36545-1 mod 924163=?
2. Tính 635423-1mod 1865421=?
3. Tính 316116-1mod 4789305=?

# Tính φ(n)

Tính φ(n):

1. Với n=257
2. Với n= 245025
3. Với n =319

# Liệt kê các phần tử và tính cấp các phần tử

Liệt kê các phần tử trong nhóm Z35\* và tính cấp của các phần tử 17, 18, 19 và 22trong Z35\*.

# Nhận biết nhóm cyclic (nhóm có phần tử sinh)

Những nhóm nào sau đây là nhóm cyclic (có phần tử sinh, phần tử nguyên thủy)? Z15\*, Z50\*, Z4\*, Z97\*, Z54\*, Z28\*, Z9\*, Z143\*, Z44\*, Z121\*, Z39\*, Z84\*

Tìm phần tử sinh của Z61\*, biết có 1 phần tử sinh thuộc [5,10]. Tìm số phần tử sinh của Z61\*.

# Tìm phần tử sinh, tìm số phần tử sinh, khó, kiểm tra đến lần thứ 3 từ nhỏ tới lớn mới đc

Tìm phần tử sinh của Z97\*. Biết có một phần tử sinh thuộc [3, 10]. Từ phần tử sinh vừa tìm được hãy tìm tất cả các phần tử sinh còn lại của Z97\*.

# Tìm phần tử sinh, tìm tất cả các phần tử sinh còn lại (thử từ giá trị nhỏ tới lớn 2 trường hợp mới đc)

Tìm phần tử sinh của Z\*31. Từ phần tử sinh vừa tìm được tìm tất cả các phần tử sinh còn lại.

# Giải hệ đồng dư trung hoa

Giải hệ phương trình đồng dư sau: (nên thử lại)

x ≡ 10 mod 15

x ≡ 14 mod 22

x ≡ 21 mod 23

# Giải hệ đồng dư trung hoa

Giải hệ phương trình đồng dư sau:

7x ≡ 10 mod 15

13x ≡ 14 mod 22

18x ≡ 21 mod 23

24x ≡ 21 mod 29

# Giải hệ đồng dư trung hoa trường hợp đặc biệt

Giải hệ PT đồng dư:

x ≡ 83 mod 91

x ≡ 83 mod 113

# Tính số các giá trị thặng dư bậc 2 của 1 nhóm

Tính số các giá trị thặng dư bậc 2 của **Zp\***. Với:

1. p=97
2. p=35

# tính kí hiệu legendre, jacobi

Tính các kí hiệu sau:

Cho p=31, tính căn bậc 2 của các số sau:

1. Tính các căn bậc 2 của 28 mod 31
2. Tính các căn bậc 2 của 19 mod 31
3. Tính các căn bậc 2 của 10 mod 31
4. Tính các căn bậc 2 của 8 mod 31

# Thuật toán 2 tính căn bậc 2

Cho p=29, tính căn bậc 2 của các số sau:

1. Tính các căn bậc 2 của 28 mod 29
2. Tính các căn bậc 2 của 20 mod 29

# Thuật toán 3 tính căn bậc 2

Cho p=19, q= 23, n=p.q, tính căn bậc 2 của các số sau:

1. Tính các căn bậc 2 của 16 mod n
2. Tính các căn bậc 2 của 24 mod n
3. Tính các căn bậc 2 của 26 mod n

# Thuật toán 4 tính căn bậc 2

Cho p=17. Tính các căn bậc 2 sau:

1. Căn bậc 2 của 2 mod 17
2. Căn bậc 2 của 8 mod 17
3. Căn bậc 2 của 15 mod 17
4. Căn bậc 2 của 13 mod 17

# Nhân bình phương có lặp

Tính:

1. 26571524 mod 4624=?
2. 356481236842 mod 454654=?
3. 165246524 mod 36845=?

# Bài toán tìm logarit rời rạc trên Zn\*,

Cho α = 17 là phần tử sinh của Z31\*. Hãy tìm: (nhớ thử lại)

1. log1720 trên Z31\*.
2. log178 trên Z31\*.
3. log1724 trên Z31\*.

# Bài toán tìm logarit rời rạc trên Zn\*,

Cho α = 38 là phần tử sinh của Z97\*. Hãy tìm: (nhớ thử lại αx =beta?)

1. log3817 trên Z97\*.
2. log3822 trên Z97\*.
3. log3844 trên Z97\*.
4. log3884 trên Z97\*.

# Bài toán tìm logarit rời rạc trên Zn\*,

Cho α = 59 là phần tử sinh của Z61\*. Hãy tìm: (nhớ thử lại αx =beta?)

1. log5920 trên Z61\*.
2. log5954 trên Z61\*.
3. log5932 trên Z61\*.
4. log5948 trên Z61\*.

# RSA

Giả sử A và B muốn trao thông tin bí mật với nhau bằng cách sử dụng hệ mật RSA. A chọn 2 số nguyên tố p1= 73 và q1=37 và số mũ bí mật d1=1013 còn B chọn 2 số nguyên tố p2= 41 và q2=59 và số mũ bí mật d2=531

1. Hãy mã bản rõ A muốn gửi B là m1=557
2. B nhận được bản mã c1= 1624 từ A. Hãy tìm bản rõ.

# RSA

Giả sử A và B muốn trao thông tin bí mật với nhau bằng cách sử dụng hệ mật RSA. A chọn 2 số nguyên tố p1= 73 và q1=37 và số mũ bí mật d1= 1013 còn B chọn 2 số nguyên tố p2= 41 và q2=59 và số mũ bí mật d2=531

1. Hãy mã bản rõ B muốn gửi A là m2=2310
2. A nhận được bản mã c2= 1624 từ B. Hãy tìm bản rõ.

# Rabin

Giả sử A và B muốn trao thông tin bí mật với nhau bằng cách sử dụng hệ mật Rabin. A chọn 2 số nguyên tố p1= 47 và q1=43 còn B chọn 2 số nguyên tố p2= 83 và q2=103. A và B thống nhất khi mã hóa sẽ lặp lại 3 bit cuối

1. Hãy mã bản rõ A muốn gửi B là m1=224
2. B nhận được bản mã nhận được ở câu a) từ A. Hãy tìm bản rõ.
3. A nhận được bản mã c2= 354 từ B. Hãy tìm bản rõ biết B thông báo đã lặp 3 bit cuối của bản rõ trước khi mã hóa và 2 bit cuối không giống nhau.

# Elgamal

Giả sử A và B muốn trao thông tin bí mật với nhau bằng cách sử dụng hệ mật Elgamal. A chọn số nguyên tố p1= 61, phần tử sinh của Z61\* là =7 và số bí mật a1= 33 còn B chọn số nguyên tố p2= 97, phần tử sinh của Z97\* là =10 và số bí mật a2=77. Khi mã hóa, A và B chọn thêm số ngẫu nhiên lần lượt là k1=56 và k2=62

1. Hãy mã bản rõ B muốn gửi A là m2=15
2. Hãy thực hiện việc giải mã của A đối với bản mã nhận được ở câu a) từ B.
3. B nhận được bản mã c2= (16, 82) từ A. Hãy tìm bản rõ.

# Giải bài toán dãy siêu tăng

A chuẩn bị đồ đi du lịch với trọng lượng của các đồ dùng như sau: M1=21, M2=30, M3=59, M4=117, M5=233, M6=465, M7= 929, M8=1857, M9=3713, M10=7425 và tổng trọng lượng ba lô của A chứa được là S=10127. Hãy giúp A lựa chọn các đồ vật có thể mang đi.

# Merkle-Hellman

Giả sử A và B muốn trao thông tin bí mật với nhau bằng cách sử dụng hệ mật Merkle-Hellman. A chọn các tham số sau:

* n1= 7
* Dãy siêu tăng M1i=(M11, M12, M13, ..., M 17)=( 15 21 41 81 161 321 641)
* Số modulo M1=1301
* Số ngẫu nhiên W1=211
* Phép hoán vị π1(1,2, …, 7)=(3, 2, 4, 1, 7, 5, 6)

Còn B chọn các tham số sau:

* n2= 7
* Dãy siêu tăng M2i=(M21, M22, M23, ..., M27)=( 9 15 29 57 113 225 449)
* Số modulo M2=901
* Số ngẫu nhiên W2=101
* Phép hoán vị π2(1,2, …, 7)=(2, 4, 5, 1, 7, 3, 6)

1. Hãy mã bản rõ B muốn gửi A là x2=1011101
2. Giải mã bản mã A nhận được từ B ở câu a)
3. B nhận được bản mã y1= 1326 từ A. Hãy tìm bản rõ.

# Merkle-Hellman

Giả sử A và B muốn trao thông tin bí mật với nhau bằng cách sử dụng hệ mật Merkle-Hellman. A chọn các tham số sau:

* n1= 9
* Dãy siêu tăng M1i=(M11, M12, M13, ..., M 19)=( 201 209 417 833 1665 3329 6657 13313 26625)
* Số modulo M1= 53251
* Số ngẫu nhiên W1=213
* Phép hoán vị π1(1,2, …, 9)=(3, 2, 9, 4, 1, 7, 5, 6,8)

Còn B chọn các tham số sau:

* n2= 9
* Dãy siêu tăng M2i=(M21, M22, M23, ..., M29)=( 135 143 285 569 1137 2273 4545 9089 18177)
* Số modulo M2=36357
* Số ngẫu nhiên W2=103
* Phép hoán vị π2(1,2, …, 9)=(9, 2, 4, 8, 5, 1, 7, 3, 6)

1. Hãy mã bản rõ B muốn gửi A là x2=0 1 1 0 1 1 1 0 1
2. Giải mã bản mã A nhận được từ B ở câu a)
3. B nhận được bản mã y1= 106752 từ A. Hãy tìm bản rõ.

# elliptic

Cho đường cong E: y2=x3 + 2x + 2 trên Z17. Xác định các điểm trên E

Cho E17(2,2); G=(5,1). Khóa riêng của A và B lần lượt là nA = 7; nB = 15. Tính KCK của A, B.

Giả sử người A cần gửi tin cho B, hãy mô phỏng quá trình mã hóa bản tin PM = (7,6) và giải mã bản mã thu được. Cho trước giá trị ngẫu nhiên k = 12

Cho E11(1, 6); G = (2,7). Biết khóa riêng của B nB = 9. Tính KCK của B.

Giả sử người A cần gửi tin cho B, hãy mô phỏng quá trình mã hóa bản tin PM = (7,9) và giải mã bản mã thu được. Cho trước giá trị ngẫu nhiên k = 11

###### Chương 4: Hàm băm, xác thực và chữ kí số (xong)

# Tấn công ngày sinh nhật

Giả sử độ dài của hàm băm là 80 bit. Tính số văn bản cần lựa chọn một cách ngẫu nhiên để tồn tại va chạm mạnh (làm cho hàm băm không còn an toàn) với xác suất epsilon=0.5

Giả thiết A cần kí vào văn bản M=9345 dùng chữ kí số RSA và gửi văn bản M cùng với chữ kí s cho B. A chọn 2 số nguyên tố p=113, q = 97 và khóa riêng của A là 1373. A tính khóa công khai của mình và gửi cho B.

1. Hãy thực hiện cách kí của A.
2. Hãy thực hiện cách B kiểm tra chữ kí
3. Giả sử trên đường truyền C đã thay đổi thông báo M thành M’=9346. Hãy thực hiện cách B kiểm tra chữ kí.
4. Giả sử trên đường truyền C đã chặn được khóa công khai mà A gửi cho B. C chọn khóa riêng là dC= 1331, sau đó C chuyển khóa công khai của C là (n, eC) (trong đó n=p.q) cho B. C đồng thời chặn được chữ kí và văn bản M mà A cần gửi cho B. C giả mạo thông báo M thành M1=8953 và dùng khóa riêng của mình để kí lên văn bản M1 rồi gửi M1 cùng chữ kí s1 cho B. Hãy thực hiện cách B kiểm tra chữ kí trong trường hợp này.
5. Có nhận xét gì về kết quả kiểm tra chữ kí của phần b, c và d.

Giả thiết A dùng chữ kí số Elgamal với p= 467, và phần tử sinh của Zp\* là α **=**32, khóa riêng của A là a= 359. A chọn số ngẫu nhiên k=119 rồi kí vào văn bản M=285 sau đó A gửi văn bản M cùng với chữ kí s cho B. Hãy thực hiện cách kí của A và cách B kiểm tra chữ kí.

###### Chương 5: Vấn đề phân phối và thỏa thuận khóa (xong)

Giả sử có 5 người sử dụng là A, B, C, D và E cần trao đổi khóa bí mật dùng sơ đồ phân phối khóa Blom với số nguyên tố công khai p = 113

A, B, C, D và E chọn phần tử công khai của mình lần lượt là rA=100, rB=47, rC= 34, rD= 29 và rE= 56

TA chọn 3 phần tử ngẫu nhiên a= 51, b= 14 và c= 79

1. Tính khóa bí mật lần lượt dành riêng cho A, B, C, D và E
2. Tính khóa bí mật dùng chung cho cả A và B; B và C; A và E; D và E

Giả sử A và B muốn trao đổi khóa bí mật dùng phương thức trao đổi khóa Diffie-Hellman với các tham số an toàn là p= 211 và α = 57 là một phần tử nguyên thủy của Zp\*. A chọn một số bí mật x = 186, B chọn một số bí mật y = 203. Tính các thông báo công khai mà A và B gửi cho nhau để tính khóa bí mật chung giữa họ. Từ đó tính khóa bí mật chung này.