###### 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

###### Đáp án:

Bản rõ: 7 14 2 2 7 0 12 2 7 8 18 4 19 7 8 19 14 19

K=12: 19 0 14 14 19 12 24 14 19 20 4 16 5 19 20 5 0 5

Bản mã: TAOOTMYOTUEQFTUFAF

K=13: 20 1 15 15 20 13 25 15 20 21 5 17 6 20 21 6 1 6

Bản mã: UBPPUNZPUVFRGUVGBG

K=14: 21 2 16 16 21 14 0 16 21 22 6 18 7 21 22 7 2 7

Bản mã: VCQQVOAQVWGSHVWHCH

K=15: 22 3 17 17 22 15 1 17 22 23 7 19 8 22 23 8 3 8

Bản mã: WDRRWPBRWXHTIWXIDI

K=16: 23 4 18 18 23 16 2 18 23 24 8 20 9 23 24 9 4 9

Bản mã: XESSXQCSXYIUJXYJEJ

K=17: 24 5 19 19 24 17 3 19 24 25 9 21 10 24 25 10 5 10

Bản mã: YFTTYRDTYZJVKYZKFK

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

Đáp án: Cả 3 TH đều ra bản rõ: KYTHUATMATMA

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

Đáp án:

B=25: Khóa (5,25) 16 8 13 3 13 21 25 23 15

Bản mã: QINDNVZXP

B=30 khóa (5,30): 21 13 18 8 18 0 4 2 20

Bản mã:VNSISAECU

B=35, khóa (5, 35) : 0 18 23 13 23 5 9 7 25

Bản mã:ASXNXFJHZ

B=40, khóa (5,40): 5 23 2 18 2 10 14 12 4

Bản mã:FXCSCKOME

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

Đáp án:

Bản mã: 3 7 14 24 3 14 6 20 15

K=(19,2): giải mã: x= a-1(y-b)

Bản rõ: TRUCTUYEN

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

Đáp án:

Bản mã: 6 21 10 24 22 12 0 20 18 8 6 15 24 14 14 10

GVKYWMAUSIPWOOK

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

Đáp án

Bản mã: 19 7 0 22 13 8 22 2 10 2 3 16 6 0 0 21 6 9 1 23 0 21 6 8 1 8

Khóa= 19 20 6 8 0 2

Bản rõ: ANUONGDIEUDONGUNGHIDUNGGIO

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.

Đáp án: JUNE

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 (CRYPTOGRAPHY IS INTERESTING)

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

Đáp án:

Bản mã: 5 2 24 17 0 25 21 11 6 5 20 0 15 20

Khóa: 9 20 11 24

Bản rõ: WINTERISCOMING (WINTER IS COMING)

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)

ĐÁP ÁN:

BẢN RÕ: T H I S I S T H E W A Y I C L E A N M Y F A C E

Bản mã: S T H H I T I S Y E E W I L A C Y A E N F C M A

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

Đáp án:

k=(1,2,3,4,5,6,7,8)=(2,7,4,8,1,5,3,6). Do đó k-1(1,2,3,4,5,6,7,8)=(5,1,7,3,6,8,2,4)

Bản mã: YDHRMICL NERREEAV SESTYWOE

Bản rõ: MYCHILDR ENAREVER YSOSWEET (MY CHILDREN ARE VERY SO SWEET)

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

Đáp án:

Bản mã Affine: 13 18 3 14 2 9 2 21 7 5 2 7 8 3 23 14 25 7 16 2 3 21

Bản mã Vigen: 18 9 11 17 2 7 7 12 15 8 2 5 13 20 5 17 25 5 21 19 11 24

* SJLRCHHMPICFNUFRZFVTLY

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

Đáp án:

Bản mã: 24 24 5 14 4 23 13 14 20 4 14 21

Giải mã dùng hệ mật khóa chạy với k2=17 20 11 4 17

Bản rõ với hệ mật khóa chạy: 7 4 20 10 13 16 9 20 10 17 24 12

Giải mã dùng hệ mật Hill với khóa k1=, => khóa k1-1=11. =

Bản rõ (Bản rõ với hệ mật Hill): BEAUTIFUL DAY

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

Đáp án:

* Giải mã Affine với khóa k được bản rõ là HAVE A NICE DAY

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

đáp án:

1. i=1: đổi chỗ S[1] và S[12]
2. i=2: đổi chỗ S[2] và S[12]
3. i=3: đổi chỗ S[3] và S[53]

# 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

Đáp án

1. Đổi chỗ S[1] và S[17]
2. Đổi chỗ S[2] và S[15]
3. Đổi chỗ S[3] và S[9]

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

# Tính gcd theo euclide

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

Đáp án gcd(196425,5756)=1

gcd(3910164, 69072)=12

# Tính nghịch đảo theo euclide mở rộng

1. Tính 36545-1 mod 924163=?

Đáp án: 36545-1 mod 924163= 315801

1. Tính 635423-1mod 1865421=?

Đáp án: 635423-1mod 1865421=1372259

1. Tính 316116-1mod 4789305=?

Đáp án: không có do gcd= 9

# Tính phi(n)

Tính φ(n):

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

Đáp án:

1. φ(257)=257-1=256
2. φ(245025)= 118800
3. φ(319)= 280

# 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 22 trong Z35\*.

Đáp án:

ord(17)=12

* Tính cấp của 18: ord(18)=12
* Tính cấp của 19: ord(19)=6
* Tính cấp của 22: ord(22)=4

# 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\*

Đáp án:

Vậy các nhóm là cyclic là: Z50\*, Z4\*, Z97\*, Z54\*.

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

Những nhóm nào sau đây có phần tử sinh? Z9\*, Z143\*, Z44\*

Đáp án:

Vậy các nhóm có phần tử sinh là: Z9\*, Z143\*.

# Nhận biết nhóm có phần tử nguyên thủy

Những nhóm nào sau đây có phần tử nguyên thủy? Z121\*, Z39\*, Z84\*

Đáp án:

Vậy các nhóm có phần tử nguyên thủy là: Z121\*.

# Tìm phần tử sinh, số phần tử sinh

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

Đáp án:

Xét α =5 thuộc Z61\*.

Kiểm tra :

Nên α =5 ko phải là phần tử sinh

Xét α =6 Kiểm tra :

Vậy α =6 là một phần tử sinh của Z61\*.

* Tìm số phần tử sinh của Z61\*.

Số phần tử sinh là

# Tìm phần tử sinh, tìm số phần tử sinh

Tìm phần tử sinh của Z97\*. Biết có một phần tử sinh thuộc [3, 10]. Hãy tìm số phần tử sinh còn lại của Z97\*.

Đáp án:

* Tìm phần tử sinh của Z97\*. Biết có một phần tử sinh thuộc [3, 6]. (t/c 4)

Có **=25.3**

Do có 1 phần tử sinh thuộc [3,6] nên xét α =3

Kiểm tra :

Do vậy α =3 không là phần tử sinh

xét α =4

Kiểm tra :

Do vậy α =4 không là phần tử sinh

xét α =5

Kiểm tra :

Vậy α =5 là phần tử sinh của Z97\*.

* Tìm số phần tử sinh của Z97\*.(t/c 3)

Có số phần tử sinh là =32

# 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.

HD:

* Tìm phần tử sinh

(phi(31)=30 = 2.3.5 ,

Xét α =2 : Kiểm tra theo t/c 4

Thử α =3 là phần tử sinh vì 36 mod 31=16 khác 1; 310 mod 31 =25 khác 1; 315 mod 31 = 30 khác 1

Vậy α =3 là phần tử sinh của Z\*31.

* Tìm tất cả các phần tử sinh còn lại từ α =3

Theo tính chất 3 tính b = αi mod n **với** gcd(i, φ(n)) = 1

Suy ra i={ 7 11 13 17 19 23 29 }

b = 37 mod 31=17

b = 311 mod 31=13

b = 313 mod 31=24

b = 317 mod 31=22

b = 319 mod 31=12

b = 323 mod 31=11

b = 329 mod 31=21

# 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

đáp án:

Vậy x=7450 mod 7590

Thử lại thay x=7450 vào hệ ban đầu để kiểm tra

# 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

Đáp án:

x=155140 mod 220110

# Giải hệ đồng dư trung hoa trường hợp đặc biệt

Giải hệ PT đồng dư:

x ≡ 83 mod 91

x ≡ 83 mod 113

đáp án(trường hợp đặc biệt khi (n1 và n2 nguyên tố cùng nhau và hệ chỉ có 2 PT có cùng giá trị a): x= 83 mod (91.113)=83 mod 10283

# 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

đáp án:

1. do p =97 là nguyên tố nên =96/2=48
2. do p=37=5.7 là tích của 2 số nguyên tố nên **=((4.6)/4=6**

# tính kí hiệu legendre, jacobi

Tính các kí hiệu sau:

Đáp án

1. **=**=4696/2 mod 97=4648 mod 97=-1 mod 97
2. =315(7-1)/2 mod 7 =03 mod 7=0
3. ==512/2.1112/2.1912/2mod 13=(-1).(-1).(-1)=-1
4. =102112/2 mod 113=1
5. =189210/2 mod 211=1
6. ==(-1).(5714/2 mod 5). (-1).= =1416/2 mod 7=1

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
5. Tính các căn bậc 2 của 20 mod 31
6. Tính các căn bậc 2 của 7 mod 31

Đáp án:

1. căn bậc 2 của 28 mod 31
2. Vậy 2 căn bậc 2 của 28 mod 31 là 20 và -20 (=11) mod 31
3. các căn bậc 2 của 19 mod 31

* Vậy 2 căn bậc 2 của 19 mod 31 là 9 và -9 (=22) mod 31

1. Căn bậc 2 của 10 mod 31: 14 và 17
2. Căn bậc 2 của 8 mod 31: 16 và 15
3. Tính các căn bậc 2 của 20 mod 31: 19 và 12
4. Tính các căn bậc 2 của 7 mod 31: 10 và 21

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

Đáp án:

1. Căn bậc 2 của 28 mod 29 là r= 12 và –r = -12 (=17 ) mod 29
2. Tính các căn bậc 2 của 20 mod 29

* Căn bậc 2 của 28 mod 29 là r= 7 và –r = -7 (=22) mod 29

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

Đáp án:

1. Tính các căn bậc 2 của 16 mod n: 4, 433, 395 và 42
2. Tính các căn bậc 2 của 24 mod n: 47, 390, 162, 275
3. Tính các căn bậc 2 của 26 mod n: 315, 122, 407, 30

# 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

Đáp án:

1. Căn bậc 2 của 2 mod 17: 6 và 11
2. Căn bậc 2 của 8 mod 17: 5 và 12
3. Căn bậc 2 của 15 mod 17: 7 và 10
4. Căn bậc 2 của 13 mod 17: 8 và 9

# Nhân bình phương có lặp

Tính:

1. 26571524 mod 4624=?

Đáp án: 26571524 mod 4624=3345

1. 25641671 mod 3548=?

Đáp án: 25641671 mod 3548=76

1. 356481236842 mod 454654=?

Đáp án: 356481236842 mod 454654=127755

1. 165246524 mod 36845=?

Đáp án: 14901

# 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\*.

Đáp án: sử dụng tt bước nhỏ bước lớn

1. log1720 trên Z31\*:14
2. log178 trên Z31\*: 6
3. log1724 trên Z31\*: 19

# 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\*.

Đáp án: sử dụng tt bước nhỏ bước lớn

1. log3817 trên Z97\*.:35
2. log3822 trên Z97\*.:72
3. log3844 trên Z97\*.:94
4. log3884 trên Z97\*.:19

# 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\*.

Đáp án:

1. log5920 trên Z61\*.:24
2. log5954 trên Z61\*.:49
3. log5932 trên Z61\*.:35
4. log5948 trên Z61\*.:10

# 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.

Đáp án:

1. Hãy mã bản rõ A muốn gửi B là m1=557

c1=m1e2 mod n2=557651 mod 2419 = 2367

1. B nhận được bản mã c1= 1624 từ A. Hãy tìm bản rõ.

m1=c1d2 mod n2=1624531 mod 2419=1760

# 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.

Đáp án:

1. Hãy mã bản rõ B muốn gửi A là m2=2310

c2=m2e1 mod n1=2310893 mod 2701 = 2365

1. A nhận được bản mã c2= 1624 từ B. Hãy tìm bản rõ.

m2=c2d1 mod n1=16241013 mod 2701=1788

# 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.

Đáp án:

1. Hãy mã bản rõ A muốn gửi B là m1=224

Bản mã c1=m1’2 mod n2=17922 mod 8549 = 5389

1. B nhận được bản mã từ A. Hãy tìm bản rõ.

B tính căn bậc 2 của bản mã c1=5389 được 4 căn bậc 2: 1792; 6757; 3852 và 4697

chuyển các giá trị căn bậc 2 thành nhị phân:

1792=11100000000

6757=1101001100101

3852=111100001100

4697=1001001011001

Do chỉ có 1792=11100000000 đáp ứng yêu cầu có 3 bit cuối lặp lại nên bản rõ A gửi cho B là m1’=1792 và bản rõ thực sự là 11100000=224

1. 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.

Tính căn bậc 2 của bản mã c1=354 được 4 căn bậc 2: 230; 1791; 1133 và 888

chuyển các giá trị căn bậc 2 thành nhị phân:

230=11100110

1791=11011111111

1133=10001101101

888=1101111000

Do chỉ có 1133=10001101101 đáp ứng yêu cầu có 3 bit cuối lặp lại và 2 bit cuối của bản rõ ban đầu không giốn nhau nên bản rõ A gửi cho B là m1’=1133 và bản rõ thực sự là 10001101=141

# 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.

Đáp án:

1. Hãy mã bản rõ B muốn gửi A là m2=15

vậy B gửi cho A bản mã c2=(49,5)

1. Hãy thực hiện việc giải mã của A đối với bản mã nhận được ở câu a) từ B.

m2=15

1. B nhận được bản mã c2= (16,82) từ A. Hãy tìm bản rõ.

m1=46

# 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.

Đáp án:

Trọng lượng của các đồ vật của A tuân theo dãy siêu tăng, gọi v=vi với i=1:10 là dãy nhị phân, nếu vi=1 là đồ được mang theo, ngược lại không mang theo.

Dùng thuật toán giải với Ba lô siêu tăng đc v=0101110101

# 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.

Đáp án:

1. Hãy mã bản rõ B muốn gửi A là x2=1011101

B mã hóa: y=**2913**

1. Giải mã bản mã A nhận được từ B ở câu a)

Bản rõ x

1 0 1 1 1 0 1

1. B nhận được bản mã y1= 1326 từ A. Hãy tìm bản rõ.

Do vậy bản rõ x= 0 0 1 0 1 1 1

# 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.

Đáp án:

1. Hãy mã bản rõ B muốn gửi A là x2=0 1 1 0 1 1 1 0 1

B mã hóa: y==**195769**

1. Giải mã bản mã A nhận được từ B ở câu a)

Bản rõ x

0 1 1 0 1 1 1 0 1

1. B nhận được bản mã y1= 106752 từ A. Hãy tìm bản rõ.

Do vậy bản rõ x= 0 1 1 0 1 1 1 0 1

# 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

Đáp án:

Mã hóa:

C=[P1,P2] =[(0,11) ; (7,11)]

Giải mã:

B tính: P2-nB.P1=(7,6)

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

Đáp án:

C=[P1,P2]=[(5,9) ; (2,7)]

Giải mã:

B tính: P2-nB.P1= (7,9)

###### 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

Đáp án:

Vậy 240

# Chữ kí số

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.

Đáp án:

A kí như sau: s=Md mod n=93451373 mod 10961=6951

1. B biết khóa công khai của A là (n,e)=(10961, 7925)

B kiểm tra chữ kí như sau: se mod n = 69517925 mod 10961 = 9345=M

Vậy B xác nhận chữ kí là đúng.

1. Do C đã thay đổi thông báo M thành M’=9346 nên B sẽ nhận được (M,s)=(9346, 6951)

B kiểm tra chữ kí như sau: se mod n = 69517925 mod 10961 = 9345M

Vậy B xác nhận chữ kí là sai.

1. Khóa công khai mà C chuyển cho B là: (n, eC),

B kiểm tra chữ kí:

S1ec mod n = 95510235 mod 10961= 8953=M1

Vậy B xác nhận chữ kí là đúng

1. - Kết quả xác nhận chữ kí phần b là đúng, kết quả này chính xác vì trên đường truyền văn bản và chữ kí của A không bị thay đổi hoặc giả mạo

* Kết quả xác nhận chữ kí phần c là sai, kết quả này chính xác vì trên đường truyền văn bản M đã bị thay đổi nhưng chữ kí của A không bị thay đổi hoặc giả mạo
* Kết quả xác nhận chữ kí phần c là đúng, kết quả này chính xác nhưng có thể thấy trên đường truyền văn bản và chữ kí của A đã bị C giả mạo. Do vậy giao thức kí RSA bị tấn công kẻ ở giữa

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.

Đáp án:

* **A kí như sau:**

Vậy chữ kí trên văn bản M=285 của A là (gama, sigma)=(61, 22)

* **B xác nhận chữ kí như sau:**

Hai vế bằng nhau vậy B xác thực chữ kí là đúng

###### 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

Đáp án:

1. Tính khóa bí mật lần lượt dành riêng cho A, B, C, D và E

=> Khóa bí mật dành riêng cho A là (aA, bA)=(95,4); B là (aB, bB)=(31,111); C là (aC, bC)=(75,101); D là (aD, bD)=(5,45) và E là (aE, bE)=(44,31)

b) Tính khóa bí mật dùng chung cho cả A và B; B và C; A và E; D và E

- khóa bí mật dùng chung cho A và B với rA=100, rB=47:

+) A tính gA(rB)= **95 + 4x** mod 113=95+4.47 mod 113=57

+) B tính gB(rA) = **31 + 111x** mod 113=31 + 111.100 mod 113=57

Vậy khóa bí mật dùng chung của A và B là 57

- khóa bí mật dùng chung cho B và C với rB=47, rC= 34:

+) B tính gB(rC) = **31 + 111x** mod 113=31 + 111.34 mod 113=76

+) C tính gC(rB) = 75 + 101x mod 113= 75 + 101.47 mod 113=76

Vậy khóa bí mật dùng chung của B và C là 76

- khóa bí mật dùng chung cho A và E với rA=100, và rE= 56:

+) A tính gA(rE)= **95 + 4x** mod 113=95+4.56 mod 113=93

+) E tính gE(rA)= 44 + 31x mod 113= 44 + 31.100 mod 113=93

Vậy khóa bí mật dùng chung của A và E là 93

- khóa bí mật dùng chung cho D và E với rD= 29 và rE= 56:

+) D tính gD(rE)= 5 + 45x mod 113= 5 + 45.56 mod 113=39

+) E tính gE(rD)= 44 + 31x mod 113= 44 + 31.29 mod 113=39

Vậy khóa bí mật dùng chung của D và E là 39

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.

Đáp án:

* Tính các thông báo công khai mà A và B gửi cho nhau:
  + A tính βA = αx  mod p=57186 mod 211=79, công khai giá trị này cho B
  + B tính βB = αy  mod p=57203 mod 211=77, công khai giá trị này cho A
* Tính khóa bí mật chung của A và B:
  + A nhận đc βB =77, dùng khóa riêng x=186 để tính khóa chung: k = (βB)x = mod p=77186 mod 211=188
  + B nhận đc βA =79, dùng khóa riêng x=203 để tính khóa chung:k = (βA)y= mod p=79203 mod 211=188
* Vậy khóa bí mật chung của A và B được trao đổi là 188