CHƯƠNG 1

MẬT MÃ CỔ ĐIỂN

* 1. MỞ ĐẦU - MỘT SỐ HỆ MẬT ĐƠN GIẢN

Đối tượng cơ bản của mật mã là tạo ra khả năng liên lạc trên một kênh không mật cho hai người sử dụng (tạm gọi là Alice và Bob) sao cho đối phương (Oscar) không thể hiểu được thông tin được truyền đi. Kênh này có thể là một đường dây điện thoại hoặc một mạng máy tính. Thông tin mà Alice muốn gửi cho Bob (bản rõ) có thể là một văn bản tiếng Anh, các dữ liệu bằng số hoặc bất cứ tài liệu nào có cấu trúc tuỳ ý. Alice sẽ mã hoá bản rõ bằng một kháo đã được xacs định trước và gửi bản mã kết quả trên kênh. Oscar có bản mã thu trộm được trên kênh song không thể xác định nội dung của bản rõ, nhưng Bob (người đã biết khoá mã) có thể giải mã và thu được bản rõ.

Ta sẽ mô tả hình thức hoá nội dung bằng cách dung khái niệm toán học như sau:

***Định nghĩa 1.1***

*Một hệ mật là một bộ 5 (P,C,K,E,D) thoả mãn các điều kiện sau:*

1. *P là một tập hữu hạn các bản rõ có thể.*
2. *C là một tập hữu hạn các bản mã có thể.*
3. *K (không gian khoá) là tập hữu hạn các khoá có thể.*
4. *Đối với mỗi k∈ K có một quy tắc mã ek: P → C và một quy tắcv giải mã tương ứng dk ∈ D. Mỗi ek:* *P → C và dk: C → P là những hàm mà:*

*dk(ek (x)) = x với mọi bản rõ x ∈ P.*

Trong tính chất 4 là tính chất chủ yếu ở đây. Nội dung của nó là nếu một bản rõ x được mã hoá bằng *ek* và bản mã nhận được sau đó được giải mã bằng *dk* thì ta phải thu được bản rõ ban đầu x. Alice và Bob sẽ áp dụng thủ tục sau dùng hệ mật khoá riêng. Trước tiên họ chọn một khoá ngẫu nhiên K *∈ K* . Điều này được thực hiện khi họ ở cùng một chỗ và không bị Oscar theo dõi hoặc khi họ có một kênh mật trong trường hợp họ ở xa nhau. Sau đó giả sử Alice muốn gửi một thông baó cho Bob trên một kênh không mật và ta xem thông báo này là một chuỗi:

x = x1,x2 ,. . .,xn

với số nguyên n ≥ 1 nào đó. Ở đây mỗi ký hiệu của mỗi bản rõ xi *∈ P* , 1 ≤ i ≤ n. Mỗi xi sẽ được mã hoá bằng quy tắc mã ek với khoá K xác định trước đó. Bởi vậy Alice sẽ tính yi = ek(xi), 1 ≤ i ≤ n và chuỗi bản mã nhận được:

y = y1,y2 ,. . .,yn

sẽ được gửi trên kênh. Khi Bob nhận đươc y1,y2 ,. . .,yn anh ta sẽ giải mã bằng hàm giải mã dk và thu được bản rõ gốc x1,x2 ,. . .,xn. Hình 1.1 là một ví dụ về một kênh liên lạc

***Hình 1.1. Kênh liên lạc***

Oscar

Bộ giải mã

Bộ mã hoá

Bob

Alice

Kênh an toàn

Nguồn khoá

Rõ ràng là trong trường hợp này hàm mã hoá phải là hàm đơn ánh ( tức là ánh xạ 1-1), nếu không việc giải mã sẽ không thực hiện được một cách tường minh. Ví dụ

y = ek(x1) = ek(x2)

trong đó x1 ≠ x2 , thì Bob sẽ không có cách nào để biết liệu sẽ phải giải mã thành x1 hay x2 . Chú ý rằng nếu *P = C* thì mỗi hàm mã hoá ize="2">Bản quyền Công ty Phát ttập các bản mã và tập các bản rõ là đồng nhất thì mỗi một hàm mã sẽ là một sự sắp xếp lại (hay hoán vị ) các phần tử của tập này.

***1.1.1 Mã dịch vòng ( shift cipher)***

Phần này sẽ mô tả mã dịch (MD) dựa trên số học theo modulo. Trước tiên sẽ điểm qua một số định nghĩa cơ bản của số học này.

***Định nghĩa 1.2***

*Giả sử a và b là các số nguyên và m là một số nguyên dương. Khi đó ta viết a ≡ b (mod m) nếu m chia hết cho b-a. Mệnh đề a ≡ b (mod m) được gọi là " a đồng dư với b theo modulo m". Số nguyên m được gọi là mudulus.*

Giả sử chia a và b cho m và ta thu được thương nguyên và phần dư, các phần dư nằm giữa 0 và m-1, nghĩa là a = q1m + r1 và b = q2m + r2 trong đó 0 ≤ r1 ≤ m-1 và 0 ≤ r2 ≤ m-1. Khi đó có thể dễ dàng thấy rằng a ≡ b (mod m) khi và chỉ khi r1 = r2 . Ta sẽ dùng ký hiệu a mod m (không dùng các dấu ngoặc) để xác định phần dư khi a được chia cho m (chính là giá trị r1 ở trên). Như vậy: a ≡ b (mod m) khi và chỉ khi a mod m = b mod m. Nếu thay a bằng a mod m thì ta nói rằng a được rút gọn theo modulo m.

*Nhận xét:* Nhiều ngôn ngữ lập trình của máy tính xác định a mod m là phần dư trong dải - m+1,.. ., m-1 có cùng dấu với a. Ví dụ -18 mod 7 sẽ là -4, giá trị này khác với giá trị 3 là giá trị được xác định theo công thức trên. Tuy nhiên, để thuận tiện ta sẽ xác định a mod m luôn là một số không âm.

Bây giờ ta có thể định nghĩa số học modulo m: Zm được coi là tập hợp {0,1,. . .,m-1} có trang bị hai phép toán cộng và nhân. Việc cộng và nhân trong Zm được thực hiện giống như cộng và nhân các số thực ngoài trừ một điểm làcác kết quả được rút gọn theo modulo m.

Ví dụ tính 11× 13 trong Z16 . Tương tự như với các số nguyên ta có 11 ×13 = 143. Để rút gọn 143 theo modulo 16, ta thực hiện phép chia bình thường: 143 = 8 × 16 + 15, bởi vậy 143 mod 16 = 15 trong Z16 .

Các định nghĩa trên phép cộng và phép nhân Zm thảo mãn hầu hết các quy tắc quyen thuộc trong số học. Sau đây ta sẽ liệt kê mà không chứng minh các tính chất này:

1. Phép cộng là đóng, tức với bất kì a,b ∈ Zm ,a +b ∈ Zm
2. Phép cộng là giao hoán, tức là với a,b bất kì ∈ Zm

a+b = b+a

1. Phép cộng là kết hợp, tức là với bất kì a,b,c ∈ Zm

(a+b)+c = a+(b+c)

1. 0 là phần tử đơn vị của phép cộng, có nghĩa là với a bất kì ∈ Zm

a+0 = 0+a = a

1. Phần tử nghịch đảo của phép cộngcủa phần tử bất kì (a ∈ Zm ) là m-a, nghĩa là a+(m-a) = (m-a)+a = 0 với bất kì a ∈ Zm .
2. Phép nhân là đóng , tức là với a,b bất kì ∈ Zm , ab ∈ Zm .
3. Phép nhân là gioa hoán , nghĩa là với a,b bất kì ∈ Zm , ab = ba
4. Phép nhân là kết hợp, nghĩa là với a,b,c ∈ Zm , (ab)c = a(cb)
5. 1 là phần tử đơn vị của phép nhân, tức là với bất kỳ a ∈ Zm

a×1 = 1×a = a

1. Phép nhân có tính chất phân phối đối với phép cộng, tức là đối với a,b,c ∈ Zm , (a+b)c = (ac)+(bc) và a(b+c) = (ab) + (ac)

Các tính chất 1,3-5 nói lên rằng Zm lâp nên một cấu trúc đại số được gọi là một nhóm theo phép cộng. Vì có thêm tính chất 4 nhóm được gọi là nhóm Aben (hay nhóm gioa hoán).

Các tính chất 1-10 sẽ thiết lập nên một vành Zm . Ta sẽ còn thấy nhiều ví dụ khác về các nhóm và các vành trong cuốn sách này. Một số ví dụ quên thuộc của vành là các số nguyên Z, các số thực R và các số phức C. Tuy nhiên các vành này đều vô hạn, còn mối quan tâm của chúng ta chỉ giới hạn trên các vành hữu hạn.

Vì phần tử ngược của phép cộng tồn tại trong Zm nên cũng có thể trừ các phần tử trong Zm . Ta định nghĩa a-b trong Zm là a+m-b mod m. Một cách tương có thể tính số nguyên a-b rồi rút gon theo modulo m.

Ví dụ : Để tính 11-18 trong Z31, ta tính 11+13 mod 31 = 24. Ngược lại, có thể lấy 11-18 được -7 rồid sau đó tính -7 mod 31 = 24.

Ta sẽ mô tả mã dịch vòng trên hình 1.2. Nó được xác định trên Z26 (do có 26 chữ cái trên bảng chữ cái tiếng Anh) mặc dù có thể xác định nó trên Zm với modulus m tuỳ ý. Dễ dàng thấy rằng, MDV sẽ tạo nên một hệ mật như đã xác định ở trên, tức là dK (eK(x)) = x với mọi x∈ Z26 .

***Hình 1.2: Mã dịch vòng***

Giả sử *P = C = K =* Z26 với 0 ≤ k ≤ 25 , định nghĩa:

eK(x) = x +K mod 26

và dK(x) = y -K mod 26

(x,y ∈ Z26)

*Nhận xét:* Trong trường hợp K = 3, hệ mật thường được gọi là mã Caesar đã từng được Julius Caesar sử dụng.

Ta sẽ sử dụng MDV (với modulo 26) để mã hoá một văn bản tiếng Anh thông thường bằng cách thiết lập sự tương ứnggiữa các kí tự và các thặng dư theo modulo 26 như sau: A ↔ 0,B ↔ 1, . . ., Z ↔ 25. Vì phép tương ứng này còn dùng trong một vài ví dụ nên ta sẽ ghi lại để còn tiện dùng sau này:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Sau đây là một ví dụ nhỏ để minh hoạ

*Ví dụ 1.1:*

Giả sử khoá cho MDV là K = 11 và bản rõ là:

*wewillmeetatmidnight*

Trước tiên biến đổi bản rõ thành dãy các số nguyên nhờ dùng phép tương ứng trên. Ta có:

22 4 22 8 11 11 12 4 4 19

0 19 12 8 3 13 8 6 7 19

sau đó cộng 11 vào mỗi giá trị rồi rút gọn tổng theo modulo 26

7 15 7 19 22 22 23 15 15 4

11 4 23 19 14 24 19 17 18 4

Cuối cùng biến đổi dãy số nguyên này thành các kí tự thu được bản mã sau:

HPHTWWXPPELEXTOYTRSE

Để giả mã bản mã này, trước tiên, Bob sẽ biến đổi bản mã thành dãy các số nguyên rồi trừ đi giá trịcho 11 ( rút gọn theo modulo 26) và cuối cùng biến đổi lại dãy nàythành các ký tự.

Nhận xét: Trong ví dụ trên , ta đã dùng các chữ in hoa ch o bản mã, các chữ thường cho bản rõ đêr tiện phân biệt. Quy tắc này còn tiếp tục sử dụng sau này.

Nếu một hệ mật có thể sử dụng được trong thực tế thì nó phảo thoả mãn một số tính chất nhất định. Ngay sau đây sé nêu ra hai trong số đó:

1. Mỗi hàm mã hoá eK và mỗi hàm giải mã dK phải có khả năng tính toán được một cách hiệu quả.

2. Đối phương dựa trên xâu bản mã phải không có khả năng xác định khoá K đã dùng hoặc không có khả năng xác định được xâu bản rõ x.

Tính chất thứ hai xác định (theo cách khá mập mờ) ý tưởng ý tưởng "bảo mật". Quá trình thử tính khoá K (khi đã biết bản mã y) được gọi là mã thám (sau này khái niệm này sẽ đực làm chính xác hơn). Cần chú ý rằng, nếu Oscar có thể xác định được K thì anh ta có thể giải mã được y như Bob bằng cách dùng dK. Bởi vậy, việc xác định K chí ít cũng khó như việc xác định bản rõ x.

Nhận xét rằng, MDV (theo modulo 26) là không an toàn vì nó có thể bị thám theo phương pháp vét cạn. Do chỉ có 26 khoá nên dễ dàng thử mọi khoá dK có thể cho tới khi nhận được bản rõ có nghĩa. Điều này được minh hoạ theo ví dụ sau:

Ví du 1.2

Cho bản mã

JBCRCLQRWCRVNBJENBWRWN

ta sẽ thử liên tiếp các khoá giải mã d0 ,d1 .. . và y thu được:

j b c r c l q r w c r v n b j e n b w r w n

i a b q b k p q v b q u m a i d m a v q v m

h z a p a j o p u a p t l z h c l z u p u l

g y z o z i n o t z o s k y g b k y t o t k

j x y n y h m n s y n r j e x f a j x s n s j

e w x m x g l m r x m q i w e z i w r m r i

d v w l w f k l q w l p h v o d y h v q l q h

c u v k v e j k p v k o g u c x g u p k p g

b t u j u d i j o u j n f t b w f o j o f

a s t i t c h i n t i m e s a v e s n i n e

Tới đây ta đã xác định được bản rõ và dừng lại. Khoá tương ứng K = 9.

Trung bình có thể tính được bản rõ sau khi thử 26/2 = 13 quy tắc giải mã.

Như đã chỉ ra trong ví dụ trên , điều kiện để một hệ mật an toàn là phép tìm khoá vét cạn phải không thể thực hiện được; tức không gian khoá phải rất lớn. Tuy nhiên, một không gian khoá lớn vẫn chưa đủ đảm bảo độ mật.

***1.1.2 Mã thay thế***

Một hệ mật nổi tiếng khác là hệ mã thay thế. Hệ mật này đã được sử dụng hàng trăm năm. Trò chơi đố chữ "*cryptogram*" trong các bài báo là những ví dụ về MTT. Hệ mật này được nếu trên hình 1.3.

Trên thực tế MTT có thể lấy cả *P* và *C* đều là bộ chữ cái tiếng anh, gồm 26 chữ cái. Ta dùng Z26 trong MDV vì các phép mã và giải mã đều là các phép toán đại số. Tuy nhiên, trong MTT, thích hợp hơn là xem phép mã và giải mã như các hoán vị của các kí tự.

***Hình 1.3 Mã thay thế***

Cho *P* =*C* = Z26 . *K* chứa mọi hoán vị có thể của 26 kí hiệu 0,1, . . . ,25

Với mỗi phép hoán vị π ∈*K* , ta định nghĩa:

eπ(x) = π(x)

và

dπ(y) = π-1(y)

trong đó π-1 là hoán vị ngược của π.

Sau đây là một ví dụ về phép hoán vị ngẫu nhiên π tạo nên một hàm mã hoá (cũng nhưb trước, các kí hiệu của bản rõ được viết bằng chữ thường còn các kí hiệu của bản mã là chữ in hoa).

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | c | d | e | f | g | h | i | j | k | l | M |
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n | o | p | q | r | s | t | u | v | w | x | y | Z |
| S | F | L | R | C | V | M | U | E | K | J | D | I |

Như vậy, eπ(a) = X, eπ(b) = N,. . . . Hàm giải mã là phép hoán vị ngược. Điều này được thực hiện bằng cách viết hàng thứ hai lên trước rồi sắp xếp theo thứ tự chữ cái. Ta nhận được:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| d | l | r | y | v | o | h | e | z | x | w | p | T |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| b | g | f | j | q | n | m | u | s | k | a | c | I |

Bởi vậy dπ(A) = d, dπ(B) = 1, . . .

Để làm bài tập, bạn đọc có giải mã bản mã sau bằng cách dùng hàm giải mã đơn giản:

M G Z V Y Z L G H C M H J M Y X S S E M N H A H Y C D L M H A.

Mỗĩ khoá của MTT là một phép hoán vị của 26 kí tự. Số các hoán vị này là 26!, lớn hơn 4 ×1026 là một số rất lớn. Bởi vậy, phép tìm khoá vét cạn không thể thực hiện được, thậm chí bằng máy tính. Tuy nhiên, sau này sẽ thấy rằng MTT có thể dễ dàng bị thám bằng các phương pháp khác.

* + 1. ***Mã Affine***

MDV là một trường hợp đặc biệt của MTT chỉ gồm 26 trong số 26! các hoán vị có thể của 26 phần tử. Một trường hợp đặc biệt khác của MTT là mã Affine được mô tả dưới đây. trong mã Affine, ta giới hạn chỉ xét các hàm mã có dạng:

e(x) = ax + b mod 26,

a,b ∈ Z26 . Các hàm này được gọi là các hàm Affine (chú ý rằng khi a = 1, ta có MDV).

Để việc giải mã có thể thực hiện được, yêu cầu cần thiết là hàm Affine phải là đơn ánh. Nói cách khác, với bất kỳ y ∈ Z26, ta muốn có đồng nhất thức sau:

ax + b ≡ y (mod 26)

phải có nghiệm x duy nhất. Đồng dư thức này tương đương với:

ax ≡ y-b (mod 26)

Vì y thay đổi trên Z26 nên y-b cũng thay đổi trên Z26 . Bởi vậy, ta chỉ cần nghiên cứu phương trình đồng dư:

ax ≡ y (mod 26) (y∈ Z26 ).

Ta biết rằng, phương tfình này có một nghiệm duy nhất đối với mỗi y khi và chỉ khi UCLN(a,26) = 1 (ở đây hàm UCLN là ước chung lớn nhất của các biến của nó). Trước tiên ta giả sử rằng, UCLN(a,26) = d >1. Khi đó, đồng dư thức ax ≡ 0 (mod 26) sẽ có ít nhất hai nghiệm phân biệt trong Z26 là x = 0 và x = 26/d. Trong trường hợp này, e(x) = ax + b mod 26 không phải là một hàm đơn ánh và bởi vậy nó không thể là hàm mã hoá hợp lệ.

Ví dụ, do UCLN(4,26) = 2 nên 4x +7 không là hàm mã hoá hợp lệ: x và x+13 sẽ mã hoá thành cùng một giá trị đối với bất kì x ∈ Z26 .

Ta giả thiết UCLN(a,26) = 1. Giả sử với x1 và x2 nào đó thảo mãn:

ax1 ≡ ax2 (mod 26)

Khi đó

a(x1- x2) ≡ 0(mod 26)

bởi vậy

26 | a(x1- x2)

Bây giờ ta sẽ sử dụng một tính chất của phép chia sau: Nếu USLN(a,b)=1 và a ⏐bc thì a ⏐c. Vì 26 ⏐ a(x1- x2) và USLN(a,26) = 1 nên ta có:

26⏐(x1- x2)

tức là

x1 ≡ x2 (mod 26)

Tới đây ta chứng tỏ rằng, nếu UCLN(a,26) = 1 thì một đồng dư thức dạng ax ≡ y (mod 26) chỉ có (nhiều nhất) một nghiệm trong Z26 . Do đó , nếu ta cho x thay đổi trên Z26  thì ax mod 26 sẽ nhận được 26 giá trị khác nhau theo modulo 26 và đồng dư thức ax ≡ y (mod 26) chỉ có một nghiệm y duy nhất.

Không có gì đặc biệt đối vơí số 26 trong khẳng định này. Bởi vậy, bằng cách tương tự ta có thể chứng minh được kết quả sau:

***Định lí 1.1***

*Đồng dư thức ax ≡ b mod m chỉ có một nghiệm duy nhất x ∈ Zm với mọi b ∈ Zm khi và chỉ khi UCLN(a,m) = 1.*

Vì 26 = 2 ×13 nên các giá trị a ∈ Z26 thoả mãn UCLN(a,26) = 1 là a = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23 và 25. Tham số b có thể là một phần tử bất kỳ trong Z26 . Như vậy, mã Affine có 12 × 26 = 312 khoá có thể ( dĩ nhiên con số này quá nhỉ để bảo đảm an toàn).

Bây giờ ta sẽ xét bài toán chung với modulo m. Ta cần một định nghĩa khác trong lý thuyết số.

***Định nghĩa 1.3***

*Giả sử a ≥ 1 và m ≥ 2 là các số nguyên. UCLN(a,m) = 1 thì ta nói rằng a và m là nguyên tố cùng nhau. Số các số nguyên trong Zm nguyên tố cùng nhau với m thường được ký hiệu là φ(m) ( hàm này được gọi là hàm Euler).*

Một kết quả quan trọng trong lý thuyết số cho ta giá trị của φ(m) theo các thừa số trong phép phân tích theo luỹ thừa các số nguyên tố của m. ( Một số nguyên p >1 là số nguyên tố nếu nó không có ước dương nào khác ngoài 1 và p. Mọi số nguyên m >1 có thể phân tích được thành tích của các luỹ thừa các số nguyên tố theo cách duy nhất. Ví dụ 60 = 2 3 × 3 × 5 và 98 = 2 × 7 2 ).

Ta sẽ ghi lại công thức cho φ(m) trong định lí sau:

***Định lý 1.2.*** ( thiếu )

Giả sử m = ∏ *pi*

Trong đó các số nguyên tố p*i* khác nhau và *ei* >0 ,1

Định lý này cho thấy rằng, số khoá trong mã Affine trên Zm bằng mφ(m), trong đó φ(m) được cho theo công thức trên. ( Số các phép chọn của b là m và số các phép chọn của a là φ(m) với hàm mã hoá là e(x) = ax + b). Ví dụ, khi m = 60, φ(60) = 2 × 2 × 4 = 16 và số các khoá trong mã Affine là 960.

Bây giờ ta sẽ xét xem các phép toán giải mã trong mật mã Affine với modulo m = 26. Giả sử UCLN(a,26) = 1. Để giải mã cần giải phương trình đồng dư y ≡ax+b (mod 26) theo x. Từ thảo luận trên thấy rằng, phương trình này có một nghiệm duy nhất trong Z26 . Tuy nhiên ta vẫn chưa biết một phương pháp hữu hiệu để tìm nghiệm. Điều cần thiết ở đây là có một thuật toán hữu hiệu để làm việc đó. Rất mayb là một số kết quả tiếp sau về số học modulo sẽ cung cấp một thuật toán giải mã hữu hiệu cần tìm.

***Định nghĩa 1.4***

*Giả sử a ∈ Zm . Phần tử nghịch đảo (theo phép nhân) của a là phần tử a-1 ∈ Zm sao cho aa-1 ≡ a-1a ≡ 1 (mod m).*

Bằng các lý luận tương tự như trên, có thể chứng tỏ rằng a có nghịch đảo theo modulo m khi và chỉ khi UCLN(a,m) =1, và nếu nghịch đảo này tồn tại thì nó phải là duy nhất. Ta cũng thấy rằng, nếu b = a-1 thì a = b-1 . Nếu p là số nguyên tố thì mọi phần tử khác không của ZP đều có nghịch đảo. Một vành trong đó mọi phần tử đều có nghịch đảo được gọi là một trường.

Trong phần sau sẽ mô tả một thuật toán hữu hiệu để tính các nghịch đảo của Zm với m tuỳ ý. Tuy nhiên, trong Z26 , chỉ bằng phương pháp thử và sai cũng có thể tìm được các nghịch đảo của các phần tử nguyên tố cùng nhau với 26: 1-1 = 1, 3-1 = 9, 5-1 = 21, 7-1 = 15, 11-1 = 19, 17-1 =23, 25-1 = 25. (Có thể dễ dàng kiểm chứng lại điều này, ví dụ: 7 × 5 = 105 ≡ 1 mod 26, bởi vậy 7-1 = 15).

Xét phương trình đồng dư y ≡ ax+b (mod 26). Phương trình này tương đương với

ax ≡ y-b ( mod 26)

Vì UCLN(a,26) =1 nên a có nghịch đảo theo modulo 26. Nhân cả hai vế của đồng dư thức với a-1 ta có:

a-1(ax) ≡ a-1(y-b) (mod 26)

Áp dụng tính kết hợp của phép nhân modulo:

a-1(ax) ≡ (a-1a)x ≡ 1x ≡ x.

Kết quả là x ≡ a-1(y-b) (mod 26). Đây là một công thức tường minh cho x. Như vậy hàm giải mã là:

d(y) = a-1(y-b) mod 26

Hình 1.4 cho mô tả đầy đủ về mã Affine. Sau đây là một ví dụ nhỏ

Cho *P = C* = Z26 và giả sử

*P* = { (a,b) ∈ Z26 × Z26 : UCLN(a,26) =1 }

Với K = (a,b) ∈*K*  , ta định nghĩa:

eK(x) = ax +b mod 26

và

dK(y) = a-1(y-b) mod 26,

x,y ∈ Z26

***Hình 1.4 Mật mãA ffine***

*Ví dụ 1.3*

Giả sử K = (7,3). Như đã nêu ở trên, 7-1 mod 26 = 15. Hàm mã hoá là

eK(x) = 7x+3

Và hàm giải mã tương ứng là:

dK(x) = 15(y-3) = 15y -19

Ở đây, tất cả các phép toán đều thực hiện trên Z26. Ta sẽ kiểm tra liệu dK(eK(x)) = x với mọi x ∈ Z26 không?. Dùng các tính toán trên Z26 , ta có

dK(eK(x)) =dK(7x+3)

=15(7x+3)-19

= x +45 -19

= x.

Để minh hoạ, ta hãy mã hoá bản rõ "*hot*". Trước tiên biến đổi các chữ h, o, t thành các thặng du theo modulo 26. Ta được các số tương ứng là 7, 14 và 19. Bây giờ sẽ mã hoá:

7 × 7 +3 mod 26 = 52 mod 26 = 0

7 × 14 + 3 mod 26 = 101 mod 26 =23

7 × 19 +3 mod 26 = 136 mod 26 = 6

Bởi vậy 3 ký hiệu của bản mã là 0, 23 và 6 tương ứng với xâu ký tự AXG. Việc giải mã sẽ do bạn đọc thực hiện như một bài tập.

* + 1. ***Mã Vigenère***

Trong cả hai hệ MDV và MTT (một khi khoá đã được chọn) mỗi ký tự sẽ được ánh xạ vào một ký tự duy nhất. Vì lý do đó, các hệ mật còn được gọi hệ thay thế đơn biểu. Bây giờ ta sẽ trình bày ( trong hùnh 1.5) một hệ mật không phải là bộ chữ đơn, đó là hệ mã Vigenère nổi tiếng. Mật mã này lấy tên của Blaise de Vigenère sống vào thế kỷ XVI.

Sử dụng phép tương ứng A ⇔ 0, B ⇔ 1, . . . , Z ⇔ 25 mô tả ở trên, ta có thể gắn cho mỗi khoa K với một chuỗi kí tự có độ dài m được gọi là từ khoá. Mật mã Vigenère sẽ mã hoá đồng thời m kí tự: Mỗi phần tử của bản rõ tương đương với m ký tự.

Xét một ví dụ nhỏ

*Ví dụ 1.4*

Giả sử m =6 và từ khoá là CIPHER. Từ khoá này tương ứng với dãy số K = (2,8,15,4,17). Giả sử bản rõ là xâu:

*thiscryptosystemisnotsecure*

***Hình 1.5 Mật mã Vigenère***

Cho m là một số nguyên dương cố định nào đó. Định nghĩa *P = C = K* = (Z26)m . Với khoá K = (k1, k2, . . . ,km) ta xác định :

eK(x1, x2, . . . ,xm) = (x1+k1, x2+k2, . . . , xm+km)

và

dK(y1, y2, . . . ,ym) = (y1-k1, y2-k2, . . . , ym-km)

trong đó tất cả các phép toán được thực hiện trong Z26

Ta sẽ biến đổi các phần tử của bản rõ thành các thặng dư theo modulo 26, viết chúng thành các nhóm 6 rồi cộng với từ khoá theo modulo 26 như sau:

19 7 8 18 2 17 24 15 19 14 18 24

2 8 15 7 4 17 2 8 15 7 4 17

21 15 23 25 6 8 0 23 8 21 22 15

18 19 4 12 8 18 13 14 19 18 4 2

2 8 15 7 4 17 2 8 15 7 4 17

20 1 19 19 12 9 15 22 8 15 8 19

20 17 4

2 8 15

22 25 19

Bởi vậy, dãy ký tự tương ứng của xâu bản mã sẽ là:

V P X Z G I A X I V W P U B T T M J P W I Z I T W Z T

Để giải mã ta có thể dùng cùng từ khoá nhưng thay cho cộng, ta trừ cho nó theo modulo 26.

Ta thấy rằng các từ khoá có thể với số độ dài m trong mật mã Vigenère là 26m, bởi vậy, thậm chí với các giá trị m khá nhỏ, phương pháp tìm kiếm vét cạn cũng yêu cầu thời gian khá lớn. Ví dụ, nếu m = 5 thì không gian khoá cũng có kích thước lớn hơn 1,1 × 107 . Lượng khoá này đã đủ lớn để ngaen ngừa việc tìm khoá bằng tay( chứ không phải dùng máy tính).

Trong hệ mật Vigenère có từ khoá độ dài m,mỗi ký tự có thể được ánh xạ vào trong m ký tự có thể có (giả sử rằng từ khoá chứa m ký tự phân biệt). Một hệ mật như vậy được gọi là hệ mật thay thế đa biểu (polyalphabetic). Nói chung, việc thám mã hệ thay thế đa biểu sẽ khó khăn hơn so việc thám mã hệ đơn biểu.

***1.1.5 Mật mã Hill***

Trong phần này sẽ mô tả một hệ mật thay thế đa biểu khác được gọi là mật mã Hill. Mật mã này do Lester S.Hill đưa ra năm 1929. Giả sử m là một số nguyên dương, đặt *P = C =*  (Z26)m . Ý tưởng ở đây là lấy m tổ hợp tuyến tính của m ký tự trong một phần tử của bản rõ để tạo ra m ký tự ở một phần tử của bản mã.

Ví dụ nếu m = 2 ta có thể viết một phần tử của bản rõ là x = (x1,x2) và một phần tử của bản mã là y = (y1,y2). Ở đây, y1cũng như y2 đều là một tổ hợp tuyến tính của x1và x2. Chẳng hạn, có thể lấy

y1 = 11x1+ 3x2

y2 = 8x1+ 7x2

Tất nhiên có thể viết gọn hơn theo ký hiệu ma trận như sau

11 8

3 7

(y1 y2) = (x1 x2)

Nói chung, có thể lấy một ma trận K kích thước m × m làm khoá. Nếu một phần tử ở hàng i và cột j của K là ki,,j thì có thể viết K = (ki,,j), với x = (x1, x2, . . . ,xm) ∈ *P* và K ∈*K* , ta tính y = eK(x) = (y1, y2, . . . ,ym) như sau:

(y1,. . .,ym) (x1, . . . ,xm)

k1,1 k1,2 ... k1,m

k2,1 k2,2 ... k2,m

... ... ... . .

km,1 km,2 ... km,m

Nói một cách khác y = xK.

Chúng ta nói rằng bản mã nhận được từ bản rõ nhờ phép biến đổi tuyến tính. Ta sẽ xét xem phải thực hiện giải mã như thế nào, tức là làm thế nào để tính x từ y. Bạn đọc đã làm quen với đại số tuyến tính sẽ thấy rằng phải dùng ma trận nghịch đảo K-1 để giả mã. Bản mã được giải mã bằng công thức y K-1 .

Sau đây là một số định nghĩa về những khái niệm cần thiết lấy từ đại số tuyến tính. Nếu A = (xi,j) là một ma trận cấp l × m và B = (b1,k ) là một ma trận cấp m × n thì tích ma trận AB = (c1,k ) được định nghĩa theo công thức:

m

c1,k  = Σ ai,j bj,k

j=1

Với 1 ≤ i ≤ l và 1 ≤ k ≤ l. Tức là các phần tử ở hàng i và cột thứ k của AB được tạo ra bằng cách lấy hàng thứ i của A và cột thứ k của B, sau đó nhân tương ứng các phần tử với nhau và cộng lại. Cần để ý rằng AB là một ma trận cấp l × n.

Theo định nghĩa này, phép nhân ma trận là kết hợp (tức (AB)C = A(BC)) nhưng noiâ chung là không giao hoán ( không phải lúc nào AB = BA, thậm chí đố với ma trận vuông A và B).

Ma trận đơn vị m × m (ký hiệu là Im ) là ma trận cấp m × m có các số 1 nằm ở đường chéo chính và các số 0 ở vị trí còn lại. Như vậy ma trận đơn vị 2 × 2 là:

1. 0

0 1

Im được gọi là ma trận đơn vị vì AIm = A với mọi ma trận cấp l × m và ImB =B với mọi ma trận cấp m × n. Ma trận nghịch đảo của ma trận A cấp m × m ( nếu tồn tại) là ma trận A-1 sao cho AA-1 = A-1A = Im . Không phải mọi ma trận đều có nghịch đảo, nhưng nếu tồn tại thì nó duy nhất.

I2 =

Với các định nghĩa trên, có thể dễ dàng xây dựng công thức giải mã đã nêu: Vì y = xK, ta có thể nhân cả hai vế của đẳng thức với K-1 và nhận được:

yK-1 = (xK)K-1 = x(KK-1) = xIm = x

( Chú ý sử dụng tính chất kết hợp)

Có thể thấy rằng, ma trận mã hoá ở trên có nghịch đảo trong Z26:

1. 8

3 7

-1

=

1. 18

23 11

vì

1. 8

3 7

1. 18

23 11

=

11×7+8×23 11×18+8×11

3×7+7×23 3×18+7×11

(Hãy nhớ rằng mọi phép toán số học đều được thực hiện theo modulo 26).

=

261 286

182 131

=

1. 0

0 1

Sau đây là một ví dụ minh hoạ cho việc mã hoá và iải mã trong hệ mật mã Hill.

*Via dụ 1.5*

1. 8

3 7

=

Từ các tính toán trên ta có:

1. 18

23 11

K-1 =

Giả sử khoá K

Giả sử cần mã hoá bản rõ "July". Ta có hai phần tử của bản rõ để mã hoá: (9,20) (ứng với Ju) và (11,24) (ứng với ly). Ta tính như sau:

(9,20)

1. 8

3 7

= (99+60, 72+140) = (3,4)

và

(11,24)

1. 8

3 7

= (121+72, 88+168) = (11,22)

Bởi vậy bản mã của July là DELW. Để giải mã Bob sẽ tính

(11,22)

1. 18

23 11

= (11,24)

và

Như vậy Bob đã nhận được bản đúng.

Cho tới lúc này ta đã chỉ ra rằng có thể thực hiện phép giải mã nếu K có một nghịch đảo. Trên thực tế, để phép giải mã là có thể thực hiện được, điều kiện cần là K phải có nghịch đảo. ( Điều này dễ dàng rút ra từ đại số tuyến tính sơ cấp, tuy nhiên sẽ không chứng minh ở đây). Bởi vậy, chúng ta chỉ quan tâm tới các ma trận K khả nghich.

(3,4)

1. 18

23 11

= (9,20)

Tính khả nghịch của một ma trận vuông phụ thuộc vào giá trị định thức của nó. Để tránh sự tổng quát hoá không cần thiết, ta chỉ giới hạn trong trường hợp 2×2.

***Định nghĩa 1.5***

*Định thức của ma trận A = (a,i j ) cấp 2× 2 là giá trị*

*det A = a1,1 a2,2 - a1,2 a2,1*

*Nhận xét:* Định thức của một ma trận vuông cấp mm có thể được tính theo các phép toán hằng sơ cấp: hãy xem một giáo trình bất kỳ về đại số tuyến tính.

Hai tính chất quan trọng của định thức là det Im = 1 và quy tắc nhân det(AB) = det A × det B.

Một ma trận thức K là có nghịch đảo khi và chỉ khi định thức của nó khác 0. Tuy nhiên, điều quan trọng cần nhớ là ta đang làm việc trên Z26 . Kết quả tương ứng là ma trận K có nghịch đảo theo modulo 26 khi và chỉ khi UCLN(det K,26) = 1.

Sau đây sẽ chứng minh ngắn gọn kết quả này.

Trước tiên, giả sử rằng UCLN(det K,26) = 1. Khi đó det K có nghịch đảo trong Z26 . Với 1 ≤ i ≤ m, 1 ≤ j ≤ m, định nghĩa Ki j ma trận thu được từ K bằng cách loại bỏ hàng thứ i và cột thứ j. Và định nghĩa ma trận K\* có phần tử (i,j) của nó nhận giá trị(-1) det Kj i (K\* được gọi là ma trận bù đại số của K). Khi đó có thể chứng tỏ rằng:

K-1 = (det K)-1K\* .

Bởi vậy K là khả nghịch.

Ngược lại K có nghịch đảo K-1 . Theo quy tắc nhân của định thức

1 = det I = det (KK-1) = det K det K-1

Bởi vậy det K có nghịch đảo trong Z26 .

Nhận xét: Công thức đối với ở trên không phải là một công thức tính toán có hiệu quả trừ các trường hợp m nhỏ ( chẳng hạn m = 2, 3). Vớim lớn, phương pháp thích hợp để tính các ma trận nghịch đảo phải dựa vào các phép toán hằng sơ cấp.

Trong trường hợp 2×2, ta có công thức sau:

***Định lý 1.3***

*Giả sử A = (ai j) là một ma trận cấp 2 × 2 trên Z26 sao cho det A = a1,1a2,2 - a1,2 a2,1 có nghịch đảo. Khi đó*

A-1 = (det A)-1

a2,2 -a1,2

-a2,1 a1,1

Trở lại ví dụ đã xét ở trên . Trước hết ta có:

det

1. 8

3 7

= 11 × 7 - 8 ×3 mod 2

= 77 - 24 mod 26 = 53 mod 26

= 1

Vì 1-1 mod 26 = 1 nên ma trận nghịch đảo là

1. 8

3 7

-1

=

1. 18

23 11

Đây chính là ma trận đã có ở trên.

Bây giờ ta sẽ mô tả chính xác mật mã Hill trên Z26 (hình 1.6)

***Hình 1.6 Mật mã HILL***

Cho m là một số nguyên dương có định. Cho *P = C =* (Z26 )m và cho

*K*  = { các ma trận khả nghịch cấp m × m trên Z26}

Với một khoá K ∈*K* ta xác định

eK(x) = xK

và dK(y) = yK -1

Tất cả các phép toán được thực hiện trong Z26

* + 1. ***Mã hoán vị (MHV)***

Tất cả các hệ mật thảo luận ở trên ít nhiều đều xoay quanh phép thaythế: các ký tự của bản rõ được thay thế bằng các ký tự khác trongbản mã. Ý tưởng của MHV là giữ các ký tự của bản rõ không thay đổi nhưng sẽ thay đôỉi vị trí của chúng bằng cách sắp xếp lại các ký tự này. MHV (còn được gọi là mã chuyển vị) đã được dùng từ hàng trăm năm nay. Thật ra thì sự phân biệt giữa MHV và MTT đã được Giovani Porta chỉ ra từ 1563. Định nghĩa hình thức cho MHV được nêu ra trên hình 1.7.

Không giống như MTT, ở đây không có các phép toán đại số nào cần thực hiện khi mã hoá và giải mã nên thích hợp hơn cả là dùng các ký tự mà không dùng các thặng dư theo modulo 26. Dưới đây là một ví dụ minh hoạ

Ví dụ 1.6

Giả sử m = 6 và khoá là phép hoán vị ( π ) sau:

1 2 3 4 5 6

3 5 1 6 4 2

***Hình 1.7 Mã hoán vị***

Cho m là mộ số nguyên dương xác định nào đó. Cho *P = C =* (Z26 )m và cho *K*  gồm tất cả các hoán vị của {1, . . ., m}. Đối một khoá π ( tức là một hoán vị) ta xác định

eπ(x1, . . . , xm ) = (xπ(1), . . . , xπ(m))

và dπ(x1, . . . , xm ) = (yπ -1(1), . . . , yπ -1(m))

trong đó π -1 là hoán vị ngược của π

Khi đó phép hoán vị ngược π -1 sẽ là:

1 2 3 4` 5 6

3 6 1 5 2 4

Bây giờ giả sử có bản rõ

*Shesellsseashellsbytheseashore*

Trước tiên ta nhóm bản rõ thành các nhóm 6 ký tự:

shesel | lsseas | hellsb | ythese | ashore

Bây giờ mỗi nhóm 6 chữ cái được sắp xếp lại theo phép hoán vị π, ta có:

EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS

Như vậy bản mã là

EESLSH SALSES LSHBLE HSYEET HRAEOS

Như vậy bản mã đã được mã theo cách tương tự banừg phép hoán vị đảo π -1.

Thực tế mã hoán vị là trường hợp đặc biệt của mật mã Hill. Khi cho phép hoán vị π của tập {1, . . . ,m}, ta có thể xác định một ma trận hoán vị m × m thích hợp Kπ = { ki,j} theo công thức:

ki,j=

1. nếu j = π(i)

0 với các trường hợp còn lại

( ma trận hoán vị là ma trận trong đó mỗi hàng và mỗi cột chỉ có một số "1", còn tất cả các giá trị khác đều là số "0". Ta có thể thu được một ma trận hoán vị từ ma trận đơn vị bằng cách hoán vị các hàng hoặc cột).

Dễ dàng thấy rằng, phép mã Hill dùng ma trận Kπ trên thực tế tương đương với phép mã hoán vị dùng hoán vị π. Hơn nữa K-1π= Kπ -1 tức ma trận nghịch đảo của Kπ là ma trận hoán vị xác định theo hoán vị π -1. Như vậy, phép giải mã Hill tương đương với phép giải mã hoán vị.

Đối với hoán vị π được dung trong ví dun trên, các ma trận hoán vị kết hợp là:

Kπ =

0 0 1 0 0 0

0 0 0 0 0 1

1 0 0 0 0 0

0 0 0 0 1 0

0 1 0 0 0 0

0 0 0 1 0 1

và K-1π =

0 0 1 0 0 0

0 0 0 0 1 0

1 0 0 0 0 0

0 0 0 0 0 1

0 0 0 1 0 0

0 1 0 0 0 0

Bạn đọc có thể kiểm tra để thấy rằng, tích của hai ma trạn này là một ma trận đơn vị.

***1.1.7 Các hệ mã dòng***

Trong các hệ mật nghiên cứu ở trên, cácb phần tử liên tiếp của bản rõ đều được mã hoá bằng cùng một khoá K. Tức xâu bản mã y nhạn được có dạng:

y = y1y2. . . = eK(x1) eK(x2 ) . . .

Các hệ mật thuộc dạng này thường được gọi là các mã khối. Một quan điểm sử dụng khác là mật mã dòng. Ý tưởng cơ bản ở đây là tạo ra một dòng khoá z = z1z2 . . . và dùng nó để mã hoá một xâu bản rõ x = x1x2 . . . theo quy tắc:

y = y1y2. . . = ez1(x1) ez2(x1). . .

Mã dòng hoạt động như sau. Giả sử K ∈*K* là khoá và x = x1x2 . . .là xâu bản rõ. Hàm fi được dùng để tạo zi (zi  là phần tử thứ i của dòng khoá) trong đó fi là một hàm của khoá K và i-1 là ký tự đầu tiên của bản rõ:

zi = fi (K, x1 , . . ., xi -1 )

Phần tử zi của dòng khoá được dùng để mã xi tạo ra yi = eiz(xi). Bởi vậy, để mã hoá xâu bản rõ x1 x2 . . . ta phải tính liên tiếp: z1, y1, z2 , y2  ...

Việc giải mã xâu bản mã y1y2. . . có thể được thực hiện bằng cách tính liên tiếp: z1, x1, z2 , x2  ...

Sau đây làb định nghĩa dưới dạng toán học:

***Định nghĩa 1.6.***

*Mật mã dòng là một bộ (P,C,K,L,F,E,D) thoả mãn dược các điều kiện sau:*

1. *P là một tập hữu hạn các bản rõ có thể.*
2. *C là tập hữu hạn các bản mã có thể.*
3. *K là tập hữu hạn các khoá có thể ( không gian khoá)*
4. *L là tập hữu hạn các bộ chữ của dòng khoá.*
5. *F = (f1 f2...) là bộ tạo dòng khoá. Với i ≥ 1*

*fi : K × P i -1 →L*

1. *Với mỗi z ∈L có một quy tắc mã ez ∈ E và một quy tắc giải mã tương ứng dz ∈D . ez : P →C và dz : C →P là các hàm thoả mãn dz(ez(x))= x với mọi bản rõ x ∈ P.*

Ta có thể coi mã khối là một trường hợp đặc biệt của mã dòng trong đó dùng khoá không đổi: Zi = K với mọi i ≥1.

Sau đây là một số dạng đặc biệt của mã dòng cùng với các ví dụ minh hoạ. Mã dòng được gọi là đồng bộ nếu dòng khoá không phụ thuộc vào xâu bản rõ, tức là nếu dòng khoá đựoc tạo ra chỉ là hàm của khoá K. Khi đó ta coi K là một "mần" để mở rộng thành dòng khoá z1z2 . . .

Một hệ mã dòng được gọi là tuần hoàn với chu kỳ d nếu zi+d= zi với số nguyên i ≥ 1. Mã Vigenère với độ dài từ khoá m có thể coi là mã dòng tuần hoàn với chu kỳ m. Trong trường hợp này, khoá là K = (k1, . . . km ). Bản thân K sẽ tạo m phần tử đầu tiên của dòng khoá: zi = ki, 1 ≤ i ≤ m. Sau đó dòng khoá sẽ tự lặp lại. Nhận thấy rằng, trong mã dòng tương ứng với mật mã Vigenère, các hàm mã và giải mã được dùng giống như các hàm mã và giải mã được dùng trong MDV:

ez(x) = x+z và dz(y) = y-z

Các mã dòng thường được mô tả trong các bộ chữ nhi phân tức là *P= C=L=* Z2. Trong trường hợp này, các phép toán mã và giải mã là phép cộng theo modulo 2.

ez(x) = x +z mod 2 và dz(x) = y +z mod 2.

Nếu ta coi "0" biểu thị giá trị "sai" và "1" biểu thị giá trị "đúng" trong đại số Boolean thì phép cộng theo moulo 2 sẽ ứng với phép hoặc có loại trừ. Bởi vậy phép mã (và giải mã ) dễ dàng thực hiện bằng mạch cứng.

Ta xem xét một phương pháp tạo một dòng khoá (đồng bộ ) khác. Giả sử bắt đầu với (k1, . . , km ) và zi = ki, 1 ≤ i ≤ m ( cũng giống như trước đây), tuy nhiên bây giờ ta tạo dòng khoá theo một quan hệ đệ quy tuyến tính cấp m:

m-1

zi+m = ∑ cj zi+j mod 2

j=0

trong đó c0, . . , cm-1 ∈ Z2 là các hằng số cho trước.

*Nhận xét:*

Phép đệ quy được nói là có bậc m vì mỗi số hạng phụ thuộc vào m số hạng đứng trước. Phép đệ quy này là tuyến tính bởi vì Zi+m là một hàm tuyến tính của các số hạng đứng trước. Chú ý ta có thể lấy c0= 1 mà không làm mất tính tổng quát. Trong trường hợp ngược lại phép đệ quy sẽ là có bậc m-1.

Ở đây khoá K gồm 2m giá trị k1, . . , km, c0, . . , cm-1. Nếu (k1, . . , km)= (0, . . . , 0) thì dòng khoá sẽ chứa toàn các số 0. Dĩ nhiên phải tránh điều này vì khi đó bản mã sẽ đồng nhất với bản rõ. Tuy nhiên nếu chọn thích hợp các hằng số c0, . . , cm-1 thì một véc tơ khởi đầu bất kì khác (k1, . . , km) sẽ tạo nên một dòng khoá có chu kỳ 2m -1. Bởi vậy một khoá ngắn sẽ tạo nên một dòng khoá có chu kỳ rất lớn. Đây là một tính chất rất đáng lưu tâm vì ta sẽ thấy ở phần sau, mật mã Vigenère có thể bị thám nhờ tận dụng yếu tố dòng khoá có chu kỳ ngắn.

Sau đây là một ví dụ minh hoạ:

*Ví dụ 1.7*

Giả sử m = 4 và dòng khoá được tạo bằng quy tắc:

zi+4 = zi + zi+1 mod 2

Nếu dòng khoá bắt đầu một véc tơ bất kỳ khác với véc tơ (0,0,0,0) thì ta thu được dòng khoá có chu kỳ 15. Ví dụ bắt đầu bằng véc tơ (1,0,0,0), dòng khoá sẽ là:

1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1

Một véc tơ khởi đầu khác không bất kỳ khác sẽ tạo một hoán vị vòng (cyclic) của cùng dòng khoá.

Một hướng đáng quan tâm khác của phương pháp tạo dòng khoá hiệu quả bằng phần cứng là sử dụng bộ ghi dịch hồi tiếp tuyến tính (hay LFSR). Ta dùng một bộ ghi dịch có m tầng. Véc tơ (k1, . . , km) sẽ được dùng để khởi tạo ( đặt các giá trị ban đầu) cho thanh ghi dịch. Ở mỗi đơn vị thời gian, các phép toán sau sẽ được thực hiện đồng thời.

1. k1 được tính ra dùng làm bit tiếp theo của dòng khoá.
2. k2, . . , km sẽ được dịch một tầng về phía trái.
3. Giá trị mới của sẽ được tính bằng:

m-1

∑ cjkj+1

j=0

(đây là hồi tiếp tuyến tính)

Ta thấy rằng thao tác tuyến tính sẽ được tiến hành bằng cách lấy tín hiệu ra từ một số tầng nhất định của thanh ghi (được xác định bởi các hằng số cj có giá trị "1" ) và tính tổng theo modulo 2 ( là phép hoặc loại trừ ). Hình 1.8 cho mô tả của LFSR dùng để tạo dòng khoá cho ví dụ 1.7.

***Hình 1.8 Thanh ghi dịch hồi tiếp tuyến tính (LFSR)***

**k2**

**k3**

**k4**

**k1**

Một ví dụ về mã dòng không đồng bộ là mã khoá tự sinh được cho ở hình 1.9. Hình như mật mã này do Vigenère đề xuất.

***Hình 1.9. Mật mã khoá tự sinh***

Cho *P = C = K = L =* Z26

Cho z1 = K và zi = xi-1 (i ≥ 2)

Với 0 ≤ z ≤ 25 ta xác định

ez(x) = x + z mod 26

dz(y) = y - z mod 26

(x,y ∈ Z26 )

Lý do sử dụng thuật nghữ "khoá tự sinh" là ở chỗ: bản rõ được dùng làm khoá ( ngoài "khoá khởi thuỷ" ban đầu K).

Sau đây là một ví dụ minh hoạ

*Ví dụ 1.8:*

Giả sử khoá là k = 8 và bản rõ là *rendezvous*. Trước tiên ta biến đổi bản rõ thành dãy các số nguyên:

17 4 13 3 4 25 21 14 20 18

Dòng khoá như sau:

1. 17 4 13 3 4 25 21 14 20

Bây giờ ta cộng các phần tử tương ứng rồi rút gọn theo modulo 26:

1. 21 17 16 7 3 20 9 8 12

Bản mã ở dạng ký tự là: ZVRQHDUJIM

Bây giờ ta xem Alice giải mã bản mã này như thế nào. Trước tiên Alice biến đổi xâu kí tự thành dãy số:

1. 21 17 16 7 3 20 9 8 12

Sau đó cô ta tính:

x1 = d8(25) = 25 - 8 mod 26 = 17

và x2 = d17(21) = 21 - 17 mod 26 = 4

và cứ tiếp tục như vậy. Mỗi khi Alice nhận được một ký tự của bản rõ, cô ta sẽ dùng nó làm phần tử tiếp theo của dòng khoá.

Dĩ nhiên là mã dùng khoá tự sinh là không an toàn do chỉ có 26 khoá.

Trong phần sau sẽ thảo luận các phương pháp thám các hệ mật mã mà ta đã trình bày.

* 1. MÃ THÁM CÁC HỆ MÃ CỔ ĐIỂN

Trong phần này ta sẽ bàn tới một vài kỹ thuật mã thám. Giả thiết chung ở đây là luôn coi đối phương Oscar đã biết hệ mật đang dùng. Giả thiết này được gọi là nguyên lý Kerekhoff. Dĩ nhiên, nếu Oscar không biết hệ mật được dùng thì nhiệm vụ của anh ta sẽ khó khăn hơn. Tuy nhiên ta không muốn độ mật của một hệ mật lại dựa trên một giả thiết không chắc chắn là Oscar không biết hệ mật được sử dụng. Do đó, mục tiêu trong thiết kế một hệ mật là phải đạt được độ mật dưới giả thiết Kerekhoff.

Trước tiên ta phân biệt các mức độ tấn công khác nhau vào các hệ mật. Sau đây là một số loại thông dụng nhất.

*Chỉ có bản mã:*

Thám mã chỉ có xâu bản mã y.

*Bản rõ đã biết:*

Thám mã có xâu bản rõ x và xâu bản mã tương ứng y.

*Bản rõ được lựa chọn:*

Thám mã đã nhận được quyền truy nhập tạm thời vào cơ chế mã hoá. Bởi vậy, thám mã có thể chọn một xâu bản rõ x và tạo nên xâu bản mã y tương ứng.

*Bản mã được lựa chọn:*

Thám mã có được quyền truy nhập tạm thời vào cơ chế giải mã. Bởi vậy thám mã có thể chọn một bản mã y và tạo nên xâu bản rõ x tương ứng.

Trong mỗi trường hợp trên, đối tượng cần phải xác định chính là khoá đã sử dụng. Rõ ràng là 4 mức tấn công trên đã được liệt kê theo độ tăng của sức mạnh tấn công. Nhận thấy rằng, tấn công theo bản mã được lựa chọn là thích hợp với các hệ mật khoá công khai mà ta sẽ nói tới ở chương sau.

Trước tiên, ta sẽ xem xét cách tấn công yếu nhất, đó là tấn công chỉ có bản mã. Giả sử rằng, xâu bản rõ là một văn bản tiếng Anh thông thường không có chấm câu hoặc khoảng trống ( mã thám sẽ khó khăn hơn nếu mã cả dấu chấm câu và khoảng trống).

Có nhiều kỹ thuật thám mã sử dụng các tính chất thống kê của ngôn ngữ tiếng Anh. Nhiều tác giả đã ước lượng tần số tương đối của 26 chữ cái theo các tính toán thống kê từ nhiều tiểu thuyết, tạp chí và báo. Các ước lượng trong bảng 1.1 lấy theo tài liệu của Beker và Piper.

***Bảng 1.1 Xác suất xuất hiện của 26 chữ cái:***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Kí tự | Xác suất | Kí tự | Xác suất | Kí tự | Xác suất |
| A | .082 | J | .002 | S | .063 |
| B | .015 | K | .008 | T | .091 |
| C | .028 | L | .040 | U | .028 |
| D | .043 | M | .024 | V | .010 |
| E | .0127 | N | .067 | W | .023 |
| F | .022 | O | .075 | X | .001 |
| G | .020 | P | .019 | Y | .020 |
| H | .061 | Q | .001 | Z | .001 |
| I | .070 | R | .060 |  |  |

Từ bảng trên, Beker và Piper phân 26 chữ cái thành 5 nhóm như sau:

1. E: có xác suất khoảng 1,120
2. T, A, O, I, N, S, H, R : mỗi ký tự có xac suất khoảng 0,06 đến 0,09
3. D, L : mỗi ký tự có xác suất chừng 0,04
4. C, U, M, W, F, G, Y, P, B: mỗi ký tự có xác suất khoảng 0,015 đến 0,023
5. V, K, J, X, Q, Z mỗi ký tự có xác suất nhỏ hơn 0,01

Việc xem xét các dãy gồm 2 hoặc 3 ký tự liên tiếp ( được gọi là bộ đôi - diagrams và bộ ba - Trigrams )cũng rất hữu ích. 30 bộ đôi thông dụng nhất ( theo hứ tự giảm dần ) là: TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI và OF. 12 bộ ba thông dụng nhất (theo thứ tự giảm dần ) là: THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR và DTH.

***1.2.1 Thám hệ mã Affine***

Mật mã Affine là một ví dụ đơn giản cho ta thấy cách thám hệ mã nhờ dùng các số liệu thống kê. Giả sử Oscar đã thu trộm được bản mã sau:

***Bảng 1.2: Tần suất xuất hiện của 26 chữ cái của bản mã***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Kí tự | Tần suất | Kí tự | Tần suất | Kí tự | Tần suất | Kí tự | Tần suất |
| A | 2 | H | 5 | O | 1 | U | 2 |
| B | 1 | I | 0 | P | 3 | V | 4 |
| C | 0 | J | 0 | Q | 0 | W | 0 |
| D | 6 | K | 5 | R | 8 | X | 2 |
| E | 5 | L | 2 | S | 3 | Y | 1 |
| F | 4 | M | 2 | T | 0 | Z | 0 |
| G | 0 | N | 1 |  |  |  |  |

Ví Dụ 1.9:

Bản mã nhận được từ mã Affine:

FMXVEDRAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKPKDLYEVLRHHRH

Phân tích tần suất của bản mã này được cho ở bảng 1.2

Bản mã chỉ có 57 ký tự. Tuy nhiên độ dài này cũng đủ phân tích thám mã đối với hệ Affine. Các ký tự có tần suất cao nhất trong bản mã là: R ( 8 lần xuất hiện), D (6 lần xuất hiện ), E, H, K (mỗi ký tự 5 lần ) và F, S, V ( mỗi ký tự 4 lần).

Trong phỏng đoán ban đầu, ta giả thiết rằng R là ký tự mã của chữ e và D là kí tự mã của t, vì e và t tương ứng là 2 chữ cái thông dụng nhất. Biểu thị bằng số ta có: eK(4) = 17 và eK(19) = 3. Nhớ lại rằng eK(x) = ax +b trong đó a và b là các số chưa biết. Bởi vậy ta có hai phương trình tuyến tính hai ẩn:

4a +b = 17

19a + b = 3

Hệ này có duy nhất nghiệm a = 6 và b = 19 ( trong Z26 ). Tuy nhiên đây là một khoá không hợp lệ do UCLN(a,26) = 2 1. Bởi vậy giả thiết của ta là không đúng.

Phỏng đoán tiếp theo của ta là: R là ký tự mã của e và E là mã của t. Thực hiện như trên, ta thu được a =13 và đây cũng là một khoá không hợp lệ. Bởi vậy ta phải thử một lần nữa: ta coi rằng R là mã hoá của e và H là mã hoá của t. Điều này dẫn tới a = 8 và đây cũng là một khoá không hợp lệ. Tiếp tục, giả sử rằng R là mã hoá của e và K là mã hoá của t. Theo giả thiết này ta thu được a = 3 và b = 5 là khóa hợp lệ.

Ta sẽ tính toán hàm giải mã ứng với K = (3,5) và gải mã bản mã để xem liệu có nhận được xâu tiếng Anh có nghĩa hay không. Điều này sẽ khẳng định tính hợp lệ của khoá (3,5). Sau khi thực hiện các phép toán này, ta có dK (y) = 9y - 19 và giải mã bản mã đã cho, ta được:

*algorithmsarequitegeneraldefinitionsof*

*arithmeticprocesses*

Như vậy khoá xác định trên là khoá đúng.

* + 1. **Thám hệ mã thay thế**

Sau đâyta phân tích một tình huống phức tạp hơn, đó là thay thế bản mã sau

Ví dụ 1.10

Bản mã nhận được từ MTT là:

YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ

NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ

NZUCDRJXỷYMTMEYIFZWDYVZVYFZUMRZCRWNZDZJT

XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDINZDIR

Phân tích tần suất của bản mã này đươch cho ở bảng 1.3.

***Bảng 1.3. Tần suất xuất hiện của 26 chưz cái trong bản mã.***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Ký tự | Tần suất | Ký tự | Tần suất | Ký tự | Tần suất | Ký tự | Tần suất |
| A | 0 | H | 4 | O | 0 | U | 5 |
| B | 1 | I | 5 | P | 1 | V | 5 |
| C | 15 | J | 11 | Q | 4 | W | 8 |
| D | 13 | K | 1 | R | 10 | X | 6 |
| E | 7 | L | 0 | S | 3 | Y | 10 |
| F | 11 | M | 16 | T | 2 | Z | 20 |
| G | 1 | N | 9 |  |  |  |  |

Do Z xuÊt hiÖn nhiÒu h¬n nhiÒu so víi bÊt kú mét ký tù nµo kh¸c trong b¶n m· nªn cã thÓ pháng ®o¸n r»ng, dZ(Z) = e. c¸c ký tù cßn l¹i xuÊt hiÖn Ýt nhÊt 10 lÇn ( mçi ký tù ) lµ C, D, F, J, R, M, Y. Ta hy väng r»ng, c¸c ký tù nµy lµ m· kho¸ cña ( mét tËp con trong ) t, a, c, o, i, n, s, h, r, tuy nhiªn sù kh¸c biÖt vÒ tÇn suÊt kh«ng ®ñ cho ta cã ®­îc sù pháng ®o¸n thÝch hîp.

Tíi lóc nµy ta ph¶i xem xÐt c¸c bé ®«i, ®Æc biÖt lµ c¸c bé ®«i cã d¹ng -Z hoÆc Z- do ta ®· gi¶ sö r»ng Z sÏ gi¶i m· thµnh e. NhËn thÊy r»ng c¸c bé ®«i th­êng gÆp nhÊt ë d¹ng nµy lµ DZ vµ ZW ( 4 lÇn mçi bé ); NZ vµ ZU ( 3 lÇn mçi bé ); vµ RZ, HZ, XZ, FZ, ZR, ZV, ZC, ZD vµ ZJ ( 2 lÇn mçi bé ). V× ZW xuÊt hiÖn 4 lÇn cßn WZ kh«ng xuÊt hiÖn lÇn nµo vµ nãi chung W xuÊt hiÖn Ýt h¬n so víi nhiÒu ký tù kh¸c, nªn ta cã thÓ pháng ®o¸n lµ dK(W) = d. V× DZ xuÊt hiÖn 4 lÇn vµ ZD xuÊt hiÖn 2 lÇn nªn ta cã thÓ nghÜ r»ng dK(D) ∈ {r,s,t}, tuy nhiªn vÉn cßn ch­a râ lµ ký tù nµo trong 3 ký tù nµy lµ ký tù ®óng.

Nªu tiÕn hµnh theo gi¶ thiÕt dK(Z) = e vµ dK(W) = d th× ta ph¶i nh×n trë l¹i b¶n m· vµ thÊy r»ng c¶ hai bé ba ZRW vµ RZW xuÊt hiÖn ë gÇn ®Çu cña b¶n m· vµ RW xuÊt hiÖn l¹i sau ®ã v× R th­êng xuÊt hiÖn trong b¶n m· vµ nd lµ mét bé ®«i th­êng gÆp nªn ta nªn thö dK(R) = n xem lµ mét kh¶ n¨ng thÝch hîp nhÊt.

Tíi lóc nµy ta cã:

- - - - - - end - - - - - - - - - e - - - - ned- - - e - - - - - - - - -

YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ

- - - - - - - - e- - - - e - - - - - - - - n - - d - - - en - - - - e - - - -e

NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ

- e - - - n - - - - - n - - - - - - ed - - - e - - - - - - ne - nd- e- e - -

NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ

- ed - - - - - n - - - - - - - - - - e - - - ed - - - - - - - d - - - e - - n

XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

Bước tiếp theo là thử dK(N) = h vì NZ là một bộ đôi thường gặp còn ZN không xuất hiện. Nếu điều này đúng thì đoạn sau của bản rõ ne - ndhe sẽ gợi ý rằng dK(C) = a. Kết hợp các giả định này, ta có:

- - - - - -end- - - - - a- - -e -a - - nedh- -e- - - - - -a - - - - -

YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ

h - - - - - - - a- - - e - a- - - a - - - nhad - a - -en -a - e - h- -e

NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ

he - a - n- - - - - - n - - - - - - ed - - - e- - - e - - neandhe -e - -

NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ

- ed - a - - -nh - - - ha - - - a- e - - - - ed - - - - -a -d - - he- -n

XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

Bây giờ ta xét tới M là ký tự thường gặp nhất sau Z. Đoạn bản mã RNM mà ta tin là sẽ giải mã thành nh- gợi ý rằng h- sẽ bắt đầu một từ, bởi vậy chắc là M sẽ biểu thị môt nguyên âm. Ta đã sử dụng a và e, bởi vậy, phỏng đoán rằng dK(M) = i hoặc o. Vì ai là bộ đôi thường gặp hơn ao nên bộ đôi CM trong bản mã gợi ý rằng, trước tiên nên thử dK(M) = i. Khi đó ta có:

- - - - -iend- - - - - a -i - e -a -inedhi - e- - - - - -a - - -i -

YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ

h - - - - - i - ea - i - e -a - - -a - i -nhad -a - en - -a - e -hi -e

NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ

he - a - n - - - - -in -i - - - - ed - - -e - - - e - ineandhe - e - -

NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ

- ed - a - - inhi - - hai - - a - e - i- -ed- - - - - a - d - - he - -n

XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

Tiếp theo thử xác định xem chữ nào được mã hoá thành o. Vì o là một chữ thường gặp nên giả định rằng chữ cái tương ứng trong bản mã là một trong các ký tự D,F,J,Y. Y có vẻ thích hợp nhất, nếu không ta sẽ có các xâu dài các nguyên âm, chủ yếu là aoi ( từ CFM hoặc CJM ). Bởi vậy giả thiết rằng dK(Y) = o.

Ba ký tự thường gặp nhất còn lại trong bản mã là D,F,J, ta phán đoán sẽ giải mã thành r,s,t theo thứ tự nào đó. Hai lần xuất hiện của bộ ba NMD gợi ý rằng dK(D) = s ứng với bộ ba his trong bản rõ ( điều này phù hợp với giả định trước kia là dK(D) ∈{r,s,t} ). Đoạn HNCMF có thể là bản mã của chair, điều này sẽ cho dK(F) = r (và dK(H) = c ) và bởi vậy (bằng cách loại trừ ) sẽ có dK(J) = t.

Ta có:

o- r - riend - ro - - arise - a - inedhise - - t - - - ass - it

YIFQFMZRWQFYVECFMDZPCVMRZNMDZVEJBTXCDDUMJ

hs - r - riseasi - e - a - orationhadta - - en - -ace - hi - e

NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREZCHZUNMXZ

he - asnt - oo - in - i - o - redso - e - ore - ineandhesett

NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ

- ed - ac - inhischair - aceti - ted - - to - ardsthes - n

XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

Bây giờ việc xác định bản rõ và khoá cho ví dụ 1.10 không còn gì khó khăn nữa. Bản rõ hoàn chỉnh như sau:

*Our friend from Pais examined his empty glass with surprise, as if evaporation had taen place while he wasn't looking. I poured some more wine and he settled back in his chair, face tilted up towards the sun.*

**1.2.3. Thám hệ mã Vigenère**

Trong phần này chúng ta sẽ mô tả một số phương pháp thám hệ mã Vigenère. Bước đầu tiên là phải xác định độ dài từ khoá mà ta ký hiệu là m. Ở đây dùng hai kỹ thuật. Kỹ thuật thứ nhất là phép thử Kasiski và kỹ thuật thứ hai sử dụng chỉ số trùng hợp.

Phép thử Kasiski lần đầu tiên được Kasiski Friendrich mô tả vào năm 1863. Kỹ thuật này được xây dựng trên nhận xét là: hai đoạn giống nhau của bản rõ sẽ được mã hoá thành cùng một bản mã khi chúng xuất hiện trong bản rõ cách nhau x vị trí, trong đó x ≡ o md m. Ngược lại, nếu ta thấy hai đoạn giống nhau của bản mã ( mỗi đoạn có độ dài ít nhất là 3 ) thì đó là một dấu hiệu tốt để nói rằng chúng tương ứng với các đoạn bản rõ giống nhau.

Phép thử Kasiski như sau. Ta tòm trong bản mã các cặp gồm các đoạn như nhau có độ dài tối thiểu là 3 và ghi lại khoảng cách giữa các vị trí bắt đầu của hai đoạn. Nếu thu được một vài giá trị d1, d2 ,. . . thì có thể hy vọng rằng m sẽ chia hết cho ước chung lớn nhất của các di.

Việc xác minh tiếp cho giá trị của m có thể nhận được bằng chỉ số trùng hợp. Khái niệm này đã được Wolfe Friedman đưa ra vào 1920 như sau:

Định nghĩa 1.7.

 Giả sử x = x1x2 . . . xn là một xâu ký tự. Chỉ số trùng hợp của x (ký hiệu là Ic(x)) được định nghĩa là xác suất để hai phần tử ngẫu nhiên của x là đồng nhất. Nếu ký hiệu các tần suất của A,B,C,. . . ,Z trong x tương ứng là f0,f1 ,. . . f25 , có thể chọn hai phần tử của x theo ??? cách. Với mỗi i, 0 ≤ i ≤ 25, có ??? cách chọn hai phần tử là i. Bởi vậy ta có công thức:

Ghi chú: Hệ số nhị thức ?????? xác định số cách chọn một tập con k đối tượng từ một tập n đối tượng.

 Bây giờ, giả sử x là một xâu văn bản tiếng Anh. Ta kí hiệu các xác suất xuất hiện của các kí tự A,B,. . .,Z trong bảng 1.1 là p0,...p25. Khi đó:

do xác suất để hai phần tử ngẫu nhiên đều là A là p02, xác suất để cả hai phần tử này đều bằng B bằng p12 . . . Tình hình tương tự cũng xảy ra nếu x là một bản mã nhận được theo một hệ mã thay thế đơn bất kì. Trong trường hợp này, từng xác suất riêng rẽ sẽ bị hoán vị nhưng tổng ??? sẽ không thay đổi.

Bây giờ giả sử có một bản mã y = y1y2. . .yn được cấu trúc theo mật mã Vigenère. Ta xác định các xâu con m của y(y1,y2,. . .,ym) bằng cách viết ra bản mã thành một hình chữ nhật có kích thước m×(n/m). Các hàng của ma trận này là các xâu con yi, 1 ≤ i ≤ m. Nếu m thực sự là độ dài khoá thì mỗi Ic(yi) phải xấp xỉ bằng 0,065. Ngược lại, nếu m không phải là độ dài khoá thì các xâu con yi sẽ có vẻ ngẫu nhiên hơn vì chúng nhận được bằng cách mã dịch vòng với các khoá khác nhau. Xét thấy rằng, một xâu hoàn toàn ngẫu nhiên sẽ có:

 Hai giá trị 0,065 và 0,038 đủ cách xa nhau để có thể xác định được độ dài từ khoá đúng ( hoặc xác nhận giả thuyết đã được làm theo phép thử Kasiski). Hai kỹ thuật này sẽ được minh hoạ qua ví dụ dưới đây:

Ví dụ 1.11.

Bản mã nhận được từ mật mã Vigenère.

CHEEVOAHMAERATBTAXXWTNXBEEOPHBSBQMQEQERBW

RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK

LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX

VRVPRTULHDNQWTWDTYGBPHXTFEALJHASVBFXNGLLCHR

ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT

AMRVLCRRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI

PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP

WQAIIWXNRMGWOIIFKEE

Trước tiên, ta hãy thử bằng phép thử Kasiski xâu bản mã CHR xuất hiện ở bốn vị trí trong bản mã, bắt đầu ở các vị trí 1, 166,236 và 286. Khoảng cách từ lầ xuất hiện đầu tiên tới 3 lần xuất hiện còn lại tương ứng là 165,235 và 285. UCLN của 3 số nguyên này là 5, bởi vậy giá trị này rất có thể là độ dài từ khoá.

Ta hãy xét xem liệu việc tính các chỉ số trùng hợp có cho kết luận tương tự không. Với m = 1 chỉ số trùng hợp là 0,045. Với m = 2, có 2 chỉ số là 0,046 và 0,041. Với m = 3 ta có 0,043; 0,050; 0,047. Với m = 4 các chỉ số là 0,042; 0,039; 0,046; 0,040. Với m = 5 ta có các giá trị 0,063; 0,068; 0,069; 0,061 và 0,072. Điều này càng chứng tỏ rằng độ dại từ khoá là 5.

Với giả thiết trên, làm như thế nào để xác định từ khoá? Ta sẽ sử dụng khái niệm chỉ số trùng hợp tương hỗ của hai xâu sau:

***Định nghĩa 1.8.***

Giả sử x = x1x2. . .xn và y = y1y2. . .yn' là các xâu có n và n' kí tự anphabet tương ứng. Chỉ số trùng hợp tương hỗ của x và y ( kí hiệu là MIc(x,y)) được xác định là xác suất để một phần tử ngẫu nhiên của x giống với một phần tử ngẫu nhiên của y. Nếu ta kí hiệu các tần suất của A,B,. . .,Z trong x và y tương ứng là f0,f1,. . .,f25 thì MIc(x,y) sẽ được tính bằng:



Với các giá trị m đã xác định, các xâu con yi thu được bằng mã dịch vòng bản rõ. Giả sử K = (k1,k2,. . .,km) là từ khoá. Ta sẽ xem xét có thể đánh giá MIc(yi,yj) như thế nào. Xét một kí tự ngẫu nhiên trong yi và một kí tự ngẫu nhiên trong yj . Xác suất để cả hai kí tự là A bằng p-ki p-kj, xác suất để cả hai là B bằng p1-ki p1-kj,. . .( Cần chú ý rằng tất cả các chỉ số dưới đều được rút gọn theo modulo 26). Bởi vậy có thể ước lượng rằng:

 Ta thấy rằng, giá trị ước lượng này chỉ phụ thuộc vào kiếu hiệu ki-kj mod 26 ( được gọi là độ dịch tương đối của yi và yj). Cũng vậy, ta thấy rằng:

Bởi vậy độ dịch tương đối *l* sẽ dẫn đến cùng một ước lượng MIc như độ dịch tương đối 26-*l* .

Ta lập bảng các ước lượng cho độ dịch tương đối trong phạm vi từ 0 đến 13.( Xem bảng 1.4).

***Bảng 1.4. Các chỉ số trùng hợp tương hỗ tính được.***

|  |  |
| --- | --- |
| **Độ dịch tương đối** | **Giá trị tính được của MIc** |
| 0 | 0.065 |
| 1 | 0,039 |
| 2 | 0,032 |
| 3 | 0,034 |
| 4 | 0,044 |
| 5 | 0,033 |
| 6 | 0,036 |
| 7 | 0,039 |
| 8 | 0,034 |
| 9 | 0,034 |
| 10 | 0,038 |
| 11 | 0,045 |
| 12 | 0,039 |
| 13 | 0,043 |

 Xét thấy rằng, nếu độ dịch tương đối khác 0 thì các ước lượng này thay đổi trong khoảng từ 0.031 đến 0,045; ngược lại nếu độ dịch tương đối bằng 0 thì ước lượng bằng 0,065. Có thể dùng nhận xét này để tạo nên một phỏng đoán thích hợp cho *l* = ki-kj (độ dịch tương đối của yi và yj) như sau: Giả sử cố định yi và xét việc mã hoá yj bảng e0,e1,e2. . . Ta kí hiệu các kết quả bằng yj0,yj1,. . . Dễ dàng dùng các chỉ số MIc(yi,yjg), 0 ≤ g ≤ 25 theo công thức sau:

Khi g = *l* thì MIc phải gần với giá trị 0,065 vì độ dịch tương đối của yi và yj bằng 0. Tuy nhiên, với các giá trị g ≠ *l* thì MIc sẽ thay đổi giữa 0,031 và 0,045.

Bằng kỹ thuật này, có thể thu được các độ dịch tương đối của hai xâu con yi bất kỳ. Vấn đề còn lại chỉ là 26 từ khoá có thể và điều này dễ dàng tìm được bằng phương pháp tìm kiếm vét cạn.

Trở lại ví dụ 1.11 để minh hoạ.

Ví dụ 1.11( tiếp ):

Ở trên đã giả định rằng, độ dài từ khoá là 5. Bây giờ ta sẽ thử tính các độ dịch tương đối. Nhờ máy tính, dễ dàng tính 260 giá trị MIc(yi,yjg), trong đó 1 ≤ i ≤ j ≤ 5; 0 ≤ g ≤ 25. Các giá trị này được cho trên bảng 1.5. Với mỗi cặp ( i,j), ta tìm các giá trị của MIc(yi,yjg) nào gần với 0,065. Nếu có một giá trị duy nhất như vậy( Đối với mỗi cặp (i,j) cho trước), thì có thể phán đoán đó chính là giá trị độ dịch tương đối.

Trong bảng 1.5 có 6 giá trị như vậy được đóng khung. Chúng chứng tỏ khá rõ ràng là độ dịch tương đối của y1 và y2 bằng 9; độ dịch tương đối của y2 và y3 bằng 13; độ dịch tương đối của y2 và y5 bằng 7; độ dịch tương đối của y3 và y5 bằng 20; của y4 và y5 bằng 11. Từ đây có các phương trình theo 5 ẩn số K1, K2, K3, K4, K5 như sau:

K1 - K2 = 9

K1 - K2 = 16

K2 - K3 = 13

K2 - K5 = 17

K3 - K5 = 20

K4 - K5 = 11

Điều này cho phép biểu thị các Ki theo K1 ;

K2 = K1 + 17

K3 = K1 + 4

K4 = K1 + 21

K5 = K1 + 10

Như vậy khoá có khả năng là ( K1, K1+17, K1+4, K1+21, K1+10) với giá trị K1 nào đó ∈ Z26. Từ đây ta hy vọng rằng, từ khoá là một dịch vòng nào đó của AREVK. Bây giờ , không tốn nhiều công sức lắm cũng có thể xác định được từ khoá là JANET. Giải mã bản mã theo khoá này, ta thu được bản rõ sau:

*The almond tree was in tentative blossom. The days were longer often ending with magnificient evenings of corrugated pink skies. The hunting seasun was over, with hounds and guns put away for six months. The vineyards were busy again as the well-organized farmers treated their vinesand the more lackadaisical neighbors hurried to do the pruning they have done in November.*

***Bảng 1.5. Các chỉ số trùng hợp tương hỗ quan sát được.***

|  |  |  |
| --- | --- | --- |
| **i** | **j** | **Giá trị của MIc(yj,yjg)** |
| 1 | 2 | 0,028 0,027 0,028 0,034 0,039 0,037 0,026 0,025 0,052  0,068 0,044 0,026 0,037 0,043 0,037 0,043 0,037 0,028  0,041 0,041 0,041 0,034 0,037 0,051 0,045 0,042 0,036 |
| 1 | 3 | 0,039 0,033 0,040 0,034 0,028 0,053 0,048 0,033 0,029  0,056 0,050 0,045 0,039 0,040 0,036 0,037 0,032 0,027  0,037 0,047 0,032 0,027 0,039 0,037 0,039 0,035 |
| 1 | 4 | 0,034 0,043 0,025 0,027 0,038 0,049 0,040 0,032 0,029  0,034 0,039 0,044 0,044 0,034 0,039 0,045 0,044 0,037  0,055 0,047 0,032 0,027 0,039 0,037 0,039 0,035 |
| 1 | 5 | 0,043 0,033 0,028 0,046 0,043 0,044 0,039 0,031 0,026  0,030 0,036 0,040 0,041 0,024 0,019 0,048 **0,070** 0,044  0,028 0,038 0,044 0,043 0,047 0,033 0,026 |
| 2 | 3 | 0,046 0,048 0,041 0,032 0,036 0,035 0,036 0,020 0,024  0,039 0,034 0,029 0,040 **0,067** 0,061 0,033 0,037 0,045  0,033 0,033 0,027 0,033 0,045 0,052 0,042 0,030 |
| 2 | 4 | 0,046 0,034 0,043 0,044 0,034 0,031 0,040 0,045 0,040  0,048 0,044 0,033 0,024 0,028 0,042 0,039 0,026 0,034  0,050 0,035 0,032 0,040 0,056 0,043 0,028 0,028 |
| 2 | 5 | 0,033 0,033 0,036 0,046 0,026 0,018 0,043 **0,080** 0,050  0,029 0,031 0,045 0,039 0,037 0,027 0,026 0,031 0,039  0,040 0,037 0,041 0,046 0,045 0,043 0,035 0,030 |
| 3 | 4 | 0,038 0,036 0,040 0,033 0,036 0,060 0,035 0,041 0,029  0,058 0,035 0,035 0,034 0,053 0,030 0,032 0,035 0,036  0,036 0,028 0,043 0,032 0,051 0,032 0,034 0,030 |
| 3 | 5 | 0,035 0,038 0,034 0,036 0,030 0,043 0,043 0,050 0,025  0,041 0,051 0,050 0,035 0,032 0,033 0,033 0,052 0,031  0,027 0,030 **0,072** 0,035 0,034 0,032 0,043 0,027 |
| 4 | 5 | 0,052 0,038 0,033 0,038 0,041 0,043 0,037 0,048 0,028  0,028 0,036 **0,061** 0,033 0,033 0,032 0,052 0,034 0,027  0,039 0,043 0,033 0,027 0,030 0,039 0,048 0,035 |

***1.2.4.TÊn c«ng víi b¶n râ ®· biÕt trªn hÖ mËt Hill.***

HÖ m· Hill lµ mét hÖ mËt khã pha h¬n nÕu tÊn c«ng chØ víi b¶n m·. Tuy nhiªn hÖ mËt nµy dÔ bÞ ph¸ nÕu tÊn c«ng b»ng b¶n râ ®· biÕt. Tr­íc tiªn, gi¶ sö r»ng, th¸m m· ®· biÕt ®­îc gi¸ trÞ m ®ang sö dông. Gi¶ sö th¸m m· cã Ýt nhÊt m cÆp vÐc t¬ kh¸c nhau xj = (x1,j, x2,j, , . . ., xm,j) vµ yj = (y1,j, y2,j,...,ym,j) (1 ≤ j ≤ m) sao cho yj = eK(xj), 1 ≤ j ≤ m. NÕu x¸c ®Þnh hai ma trËn: X = (xi,j) Y = (yi,j) cÊp m×m th× ta cã ph­¬ng tr×nh ma trËn Y = XK, trong ®ã ma trËn K cÊp m×m lµ kho¸ ch­a biÕt. Víi ®iÒu kiÖn ma trËn Y lµ kh¶ nghÞch. Oscar cã thÓ tÝnh K = X-1Y vµ nhê vËy ph¸ ®­îc hÖ mËt. ( NÕu Y kh«ng kh¶ nghÞch th× cÊn ph¶i thö c¸c tËp kh¸c gåm m cÆp râ - m·).

VÝ dô 1.12.

Gi¶ sö b¶n râ *Friday* ®­îc m· ho¸ b»ng m· Hill víi m = 2, b¶n m· nhËn ®­îc lµ PQCFKU.

Ta cã eK(5,17) = (15,16), eK(8,3) = (2,5) vµ eK(0,24) = (10,20). Tõ hai cÆp râ - m· ®Çu tiªn, ta nhËn ®­îc ph­¬ng tr×nh ma trËn:



Dïng ®Þnh lý 1.3, dÔ dµng tÝnh ®­îc:

Bëi vËy:

Ta cã thÓ dïng cÆp râ - m· thø 3 ®Ó kiÓm tra kÕt qu¶ nµy.

VÊn ®Ò ë ®©y lµ th¸m m· ph¶i lµm g× nÕu kh«ng biÕt m?. Gi¶ sö r»ng m kh«ng qu¸ lín, khi ®ã th¸m m¸ cã thÓ thö víi m = 2,3,. . . cho tíi khi t×m ®­îc kho¸. NÕu mét gi¸ trÞ gi¶ ®Þnh cña m kh«ng ®óng th× mµ trËn m×m t×m ®­îc theo thuËt to¸n ®· m« t¶ ë trªn sÏ kh«ng t­¬ng thÝch víi c¸c cÆp râ - m· kh¸c. Ph­¬ng ph¸p nµy, cã thÓ x¸c ®Þnh gi¸ trÞ m nÕu ch­a biÕt.

***1.2.5. Th¸m m· hÖ m· dßng x©y dùng trªn LFSR.***

Ta nhí l¹i r»ng, b¶n m· lµ tæng theo modulo 2 cña b¶n râ vµ dßng kho¸, tøc yi = xi + zi mod 2. Dßng khãa ®­îc t¹o tõ (z1,z2,. . .,zm) theo qu¹n hÖ ®Ö quy tuyÕn tÝnh:

trong ®ã c0,. . .,cm ∈ Z2 (vµ c0 = 1)

V× tÊt c¶ c¸c phÐp to¸n nµy lµ tyuÕn tÝnh nªn cã thÓ hy väng r»ng, hÖ mËt nµy cã thÓ bÞ ph¸ theo ph­¬ng ph¸p tÊn c«ng víi b¶n râ ®· biÕt nh­ tr­êng hîp mËt m· Hill. Gi¶ sö r»ng, Oscar cã mét x©u b¶n râ x1x2. . .xn vµ x©u b¶n m· t­¬ng øng y1y2. . .yn . Sau ®ã anh ta tÝnh c¸c bÝt dßng kho¸ zi = xi+yi mod 2, 1 ≤ i ≤ n. Ta còng gi¶ thiÕt r»ng Oscar còng ®· biÕt gi¸ trÞ cña m. Khi ®ã Oscar chØ cÇn tÝnh c0, . . ., cm-1 ®Ó cã thÓ t¸i t¹o l¹i toµn bé dßng kho¸. Nãi c¸ch kh¸c, Oscar cÇn ph¶i cã kh¶ n¨ng ®Ó x¸c ®Þnh c¸c gi¸ trÞ cña m Èn sè.

Víi i ≥ 1 bÊt k× ta cã :

lµ mét ph­¬ng tr×nh tuyÕn tÝnh n Èn. NÕu n ≥ 2n th× cã m ph­¬ng tr×nh tuyÕn tÝnh m Èn cã thÓ gi¶i ®­îc.

HÖ m ph­¬ng tr×nh tuyÕn tÝnh cã thÓ viÕt d­íi d¹ng ma trËn nh­ sau:

NÕu ma trËn hÖ sè cã nghÞch ®¶o ( theo modulo 2 )th× ta nhËn ®­îc nghiÖm:

 Trªn thùc tÕ, ma trËn sÏ cã nghÞch ®¶o nÕu bËc cña phÐp ®Ö quy ®­îc dïng ®Ó t¹o dßng kho¸ lµ m.(xem bµi tËp). Minh ho¹ ®iÒu nµy qua mét vÝ dô.

VÝ dô 1.13.

Gi¶ sö Oscar thu ®­îc x©u b¶n m·

101101011110010

t­¬ng øng víi x©u b¶n râ

011001111111001

Khi ®ã anh ta cã thÓ tÝnh ®­îc c¸c bÝt cña dßng kho¸:

110100100001010

Ta còng gi¶ sö r»ng, Oscar biÕt dßng kho¸ ®­îc t¹o tõ mét thanh ghi dÞch ph¶n håi (LFSR) cã 5 tÇng. Khi ®ã, anh ta sÏ gi¶i ph­¬ng tr×nh mµ trËn sau ( nhËn ®­îc tõ 10 bÝt ®Çu tiªn cña dßng kho¸):

Cã thÓ kiÓm tra ®­îc r»ng:

Tõ ®ã ta cã:



= (1, 0, 0, 1, 0)

Nh­ vËy phÐp ®Ö quy ®­îc dïng ®Ó t¹o dßng kho¸ lµ:

zi+5 = zi + zi+3 mod 2

**1.3. CÁC CHÚ GIẢI VÀ TÀI LIỆU DẪN**

Nhiều tài liệu về mật mã cổ điển đã có trong các giáo trình, chẳng hạn như giáo trình của Beker và Piper [BP82] và Denning [DE82]. Xác suất đánh giá cho 26 kí tự được lấy của Beker và Piper. Cũng vậy, việc phân tích mã Vigenère được sửa đổi theo mô tả của Beker và Piper. Rosen [Ro93] là một tài liệu tham khảo tốt về lý thuyết số. Cơ sở của Đại số tuyến tính sơ cấp có thể tìm thấy trong sách của Anton [AN91]. Cuốn " Những người mã thám " của Kahn [KA67] là một cấu chuyện hấp dẫn và phong phú về mật mã cho tới năm 1967, trong đó Kahn khẳng định rằng mật mã Vigenère thực sự không phải là phát minh của Vigenère.

Mật mã Hill lần đầu tiên được mô tả trong [HI29]. Các thông tin về mật mã dòng có thể tìm được trong sách của Rueppel [RU86].

BÀI TẬP

1.1. Dưới đây là 4 bản mã thu được từ mã thay thế. Một bản thu được từ mã Vigenère, một từ mật mã Affine và một bản chưa xác định. Nhiệm vụ ở đây là xác định bản rõ trong mỗi trường hợp.

Hãy mô tả các bước cần thực hiện để giải mã mỗi bản mã ( bao gồm tất cả các phân tích thống kê và các tính toán cần thực hiện).

Hai bản rõ đầu lấy từ cuốn " The diary of samuenl marchbanks " của Robertson Davies, Clack Iriwin,1947; bản rõ thứ tư lấy từ " Lake wobegon days" của Garrison Keillor, Viking Penguin, 1985.

*a) Mã thay thế:*

EMGLXUDCGDNCUSWYXFPHNSFCYKDPUMLWGYICOXYFIPJCK

QPKUGKMGOLICGINCGACKFNIFACYKZSCKXECJCKFHYFXCG

0IDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUFIGLEDFPWZU

GFZCCNDGYYFFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNF

ACIGOYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCSZCCNC

IACZEJNCFFZEJZEGMXCYHCJUMGKUSI

*Chỉ dẫn:* F sẽ giải mã thành W.

*b) Hệ mã Vigenère*

KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGLLTXRGUD

DKBTMBPVGEGLTGCKQRACQCWDNAWCRXIZAKSTLEWRPTYC

QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL

SVSKCGCZQQDZXGSFRLFWCWSJTBHAFSIASPRJAHKJRJUMP

FFSQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI

CWHJVLNHIQIBTKHJVNPIST

*c) Hệ mã Affine.*

KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUP

KRIOFKPACUZQEPBKRXPEIIEABDKPBCPFCDCAFIEABDKP

BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFF

ERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERK

IVKSCPICBRKIJPKABI

*d) Hệ mã chưa xác định được.*

BNVSNSIHQCEELSSKKYERISJKXUMBGYKAMQLJTYAVFBKVT

DVBPVVRJYYLAOKYMPQSCGDLFLLPROYGEFEBUUALRWXM

MASAZLGLEDFJBZAVVPXWYCGJXASCBYEHOSNMULKCEAHTQ

OKMFLEBKFXLRRFDTZXCIWBJSICBGAWDVYDHAVFJXZIBKC

GJIWEAHTTOEWTUHKRQVVRGZBXYIREMMASCSPBNLHJGBLR

FFJELHWEYLWISTFVVYFJCMHYURUFSFMGESIGRLWALSWM

NUHSIMYYITCCQPZSICEHBCCMZFEGVJYOCDEMMPGHVAAMU

ELCMOEHVLTIPSUYILVGFLMVWDVYDBTHERAYISYSGKVSUU

HYHGGCKTMBLRX

1.2. a) Có bao nhiêu ma trận khả nghịch cấp 2×2 trên Z26 .

1. Giả sử p là số nguyên tố. Hãy chứng tỏ số các ma trận khả nghịch cấp 2×2 trên Zp là (p2-1)(p2-p).

*Chỉ dẫn:* Vì p là số nguyên tố nên Zp là một trường. Hãy sử dụng khẳng định sau: Một ma trận là khả nghịch trên một trường là khả nghịch khi và chỉ khi các hàng của nó là các véc tơ độc lập tuyến tính ( tức không tồn tại một tổ hợp tuyến tính các hàng khác 0 mà tổng của chúng là một véc tơ toàn số 0).

c) Với p là số nguyên tố và m là một số nguyên ≥ 2. Hãy tìm công thức tính số các ma trận khả nghịch cấp m×m trên Zp.

1.3. Đôi khi chọn một khoá mà phép mã và giải mã là đồng nhất rất hữu ích. Trong trường hợp mất mã Hill, ta phải tìm các ma trận K sao cho K = K-1 ( ma trận này được gọi là ma trận đối hợp). Trên thực tế, Hill đã đề nghị sử dụng các ma trận này làm khoá trong các hệ mật của mình. Hãy xác định số các ma trận đối hợp trên Z26 trong trường hợp m = 2.

*Chỉ dẫn:* Hãy dùng công thức trong định lý 1.3 và để ý rằng detA = ± với một ma trận đối hợp trên Z26.

1.4. Giả sử ta đã biết rằng bản rõ " *conversation* " sẽ tạo nên bản mã " HIARRTNUYTUS " ( được mã theo hệ mã Hill nhưng chưa xác định được m). Hãy xác định ma trận mã hoá.

1.5. Hệ mã Affine - Hill là hệ mã Hill được sửa đổi như sau: Giả sử m là một số nguyên dương và P = C = (Z26)m. Trong hệ mật này, khoá K gồm các cặp (L,b), trong đó L là mọt ma trận khả nghịch cấp m×m trên Z26 và b∈(Z26)m. Với x = ( x1,. . .,xm)∈P và K = (L,b) ∈ K, ta tính y = eK(x) = (y1,. . .,ym) theo công thức y = xL + b. Bởi vậy, nếu L = (*l*i,j) và b = (b1,. . .,bm) thì:



Giả sử Oscar đã biết bản rõ là "*adisplayedequation*" và bản mã tương ứng là " DSRMSIOPLXLJBZULLM". Oscar cũng biết m =3. Hình tính khoá và chỉ ra tất cả các tính toán cần thiết.

1.6. Sau đây là cách thám mã hệ mã Hill sử dụng phương pháp tấn công chỉ với bản mã. Giả sử ta biết m = 2. Chia các bản mã thành các khối có độ dài 2 kí tự ( các bộ đôi). Mỗi bộ đôi này là bản mã của một bộ đôi của bản rõ nhờ dùng một ma trận mã hoá chưa biết. Hãy nhặt ra các bộ đôi thường gặp nhất trong bản mã và coi rằng đó là mã của một bộ đôi thường gặp trong danh sách ở bảng 1.1 ( ví dụ TH và ST). Với mỗi giả định, hãy thực hiện phép tấn công với bản rõ đã biết cho tới khi tìm được ma trận giải mã đúng.

Sau đây là một ví dụ về bản mã để bạn giải mã theo phương pháp đã nêu:

LMQETXYEAGTXCTUIEWNCTXLZEWUAISPZYVAPEWLMGQWYA

XFTCJMSQCADAGTXLMDXNXSNPJQSYVAPRIQSMHNOCVAXFV.

1.7. Ta sẽ mô tả một trường hợp đặc biệt của mã hoán vị. Giả sử m, n là các số nguyên dương. Hãy viết bản rõ theo thành từng hàng thành một hình chữ nhật m×n. Sau đó tạo ra bản mã bằng cách lấy các cột của hình chữ nhật này. Ví dụ, nếu m = 4, n = 3 thì ta sẽ mã hoá bản rõ "*cryptography*" bằng cách xây dựng hình chữ nhật :

*cryp*

*togr*

*aphy*

Bản mã sẽ là: 'CTAROPYGHPRY'

1. Hãy mô tả cách Bob giải mã một bản mã ( với m, n đã biết)
2. Hãy giải mã bản mã sau: ( nhận được theo phương pháp đã nêu):

MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW

1.8. Có 8 phép đệ quy tuyến tính bậc 4 khác nhau trên Z2 với c0 = 1. Hãy xác định những phép đệ quy nào tạo được dòng khoá có chu kỳ 15 ( với véc tơ khởi tạo khác 0).

1.9. Mục đích của bài tập này để chứng minh khẳng định ở phần 1.2.5 là : ma trận hệ số cấp m×m có nghịch đảo. Điều này tương đương với khẳng định rằng, các hàng ma trận này là các véc tơ độc lập tuyến tính trên Z2.

Giả sử rằng phép đệ quy có dạng:

( z1,. . .,zm) là véc tơ khởi tạo. Với i ≥ 1 ta xác định:

vi = (zi,. . .,zi+m-1)

Chú ý rằng, ma trận hệ số có các véc tơ v1,. . .,vm là các hàng của nó. Bởi vậy, nhiệm vụ của ta là chứng tỏ rằng m véc tơ này là độc lập tuyến tính.

Hãy chứng minh hai khẳng định sau:

1. Với i ≥ 1 bất kì:

b)Chọn h là số nguyên nhỏ nhất sao cho tồn tại một tổ hợp tuyến tính không tầm thường của các véc tơ v1,. . .,vh có tổng là véc tơ (0, . . . , 0) theo modulo 2. Khi đó:

( Các αj không đồng nhất bằng 0). Để ý rằng, h ≤ m+1 vì m+1 là véc tơ bất kỳ trong không gian tuyến tính m chiều đều phụ thuộc tuyến tính .

1. Hãy chứng tỏ rằng dòng khoá phải thảo mãn phép đệ quy:

với bất kì i ≥ 1.

d) Ta nhận thấy rằng, nếu h ≤ m thì dòng khoá thảo mãn phép đệ quy tuyến tính có bậc nhỏ hơn m. Điều này mâu thuẫn. Bởi vậy h = m + 1 và ma trận phải là khả nghịch.

1.10. Hãy giải mã bản mã sau ( thu được từ mã khoá tự sinh ) bằng phương pháp tìm khoá vét cạn.

MALVVMAFBHBUQPTSOXALTGVWWRG

1.11. Ta sẽ mô tả một hệ mã dòng là biến thể của mã Vigenère như sau. Với một từ khoá độ dài m cho trước ( k1,. . .,km ), ta tạo dòng khoá theo quy tắc zi=ki (1 ≤ i ≤ m), zi+m = zi+1 mod 26 ( i ≥ m+1). Nói cách khác, mỗi lần dùng từ khoá ta sẽ thay mỗi kí tự bằng kí tự đứng sau nó theo modulo 26. Ví dụ, nếu SUMMER là từ khoá thì ta dùng SUMMER để mã hoá 6 kí tự đầu.,sau đó dùng TVNNFS để mã hoá 6 kí tự tiếp theo và cú tiếp tục như vậy.

Hãy mô tả cách có thể dùng khái niệm chỉ số trùng hợp như thế nào để trước hết là xác định độ dài từ khoá và sau đó là tìm từ khoá.

Hãy kiểm tra phương pháp của bạn bằng cách bằng cách phân tích bản mã sau:

IYMYSILONRFNCQXQJEDSHBUIBCJUZBOLFQYSCHATPEQGQ

JEJNGNXZWHHGƯFSUKULJQACZKKJOAAHGKEMTAFGMKVRDO

PXNEHEKZNKFSKIFRQVHHOVXINPHMRTJPYWQGJWPUUKFP

OAWPMRKKQZWLQDYAZDRMLPBJKJOBWIWPSEPVVQMBCRYVC

RUZAAOUMBCHDAGDIEMSZFZHALIGKEMJJFPCIWKRMLMPIN

AYOFIREAOLDTHITDVRMSE

Bản rõ được lấy từ "The codebreakers" của D.Kahn, 1967.