# Mục Lục

[Mục Lục 1](#_Toc466693117)

[1. Các chỉ tiêu cơ bản của hệ thống thông tin số ? 2](#_Toc466693118)

[2.Chứng minh hệ mật (MDV, OTP,…) có độ mật hoàn thiện 2](#_Toc466693119)

[3.Mô tả quá trình mã, giải mã của các hệ mật đơn biểu, đa biểu, MHV, hệ mật tích, DES, AES 5](#_Toc466693120)

[4.Nêu khái niệm về hệ mật tích do Shannon đề xuất. CM tính đúng đắn của quy tắc giải mã trong hệ mật tích.(chưa CM) 6](#_Toc466693121)

[5.M là hệ mã nhân, S là HDV CMR: MxS, SxM chính là hệ mã Affine với các khóa đồng xác suất 6](#_Toc466693122)

[6.Hệ mật DES (CM phép giải mã đồng nhất phép mã với bảng khóa đảo ngược; các chế độ hoạt động của DES: ECB, CBC, CFB, OFB và các tính chất của chúng), 2DES, 3DES.(chưa CM) 7](#_Toc466693123)

[7.Phân tích độ an toàn các hệ mật KCK( RSA, Meckle- Hellman, McEliece, ElGamal, Chor-Rivest, Elliptic) 11](#_Toc466693124)

[8.Sơ đồ phân loại hàm băm mật mã và ứng dụng, tính chất của các hàm băm không có khóa; các khía cạnh liên quan tới việc xác thực mẩu tin khi truyền tin trên mạng; vẽ sơ đồ và trình bày trạng thái băm : Matyas-Meyer-Oseas, Danes-Meyer 11](#_Toc466693125)

[9.Trình bày tòm lược các bước trong hệ phân phối khóa dựa trên định danh Okamoto-Tanaka 13](#_Toc466693126)

[10.Vẽ và mô tả sơ đồ kí số RSA 14](#_Toc466693127)

[11. Sơ đồ cấu trúc của thuật toán AES, nếu ý nghĩa của tầng phi tuyến, trộn tuyến tính, cộng khóa(chưa có sơ đồ) 15](#_Toc466693128)

[12.Hệ mật RSA (Cho ví dụ minh họa về thông báo không thể che giấu, công thức tính số thông báo không thể che giấu). CMR hệ mật RSA là không an toàn nếu dùng chung số modulo n, hoặc bên A,B chọn GCD(eA,eB) =1(chưa CM) 16](#_Toc466693129)

# 1. Các chỉ tiêu cơ bản của hệ thống thông tin số ?

* Tính hữu hiệu:

+ tốc độ truyền tin cao

+ truyền được đồng thời nhiều tin khác nhau

+ chi phí cho một bit thấp

* Độ tin cậy:
* Đảm bảo độ chính xác của việc thu nhận tin cao, xác suất thu sai (BER ) thấp .
* Hai chỉ tiêu trên mâu thuẫn nhau . Giải quyết mâu thuẫn trên là nhiệm vụ của lý thuyết thông tin
* An toàn:

+ bí mật:

* Không thể khai thác thông tin trái phép
* Chỉ có người nhận hợp lệ mới hiểu đươc thông tin

+ xác thực : gắn trách nhiệm của bên gửi – bên nhận với bản tin ( chữ ký số )

+ toàn vẹn:

* Thông tin không bị bóp méo ( cắt xén, xuyên tạc , sửa đổi )
* Thông tin được nhận phải nguyên vẹn cả về nội dung và hình thức

+ Khả dụng : mọi tài nguyên và dihcj vụ của hệ thống phải được cung cấp đầy đủ cho người dùng hợp pháp

* Đảm bảo chất lượng dịch vụ (QoS) : Đây là một chỉ tiêu rất quan trọng đặc biệt là đối với các dịch vụ thời gian thực , nhạy cảm với độ trễ ( truyền tiếng nói, hình ảnh … )

# 2.Chứng minh hệ mật (MDV, OTP,…) có độ mật hoàn thiện

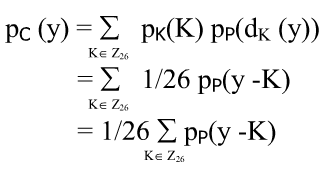
-Hệ mật mã dịch vòng(MDV):

Giả sử 26 khóa trong MDV có xác suất như nhau bằng 1/26 khi đó MDV sẽ có độ mật hoàn thiện với mọi phân bố xác suất của bản rõ.

Chứng minh : Ta có P = C = K = Z26 và với 0 ≤ K ≤ 25, quy tắc mã hóa eK là:

eK(x) = x + K mod 26(x).

Trước tiên tính phân bố PC. Giả sử y Z26 , khi đó:



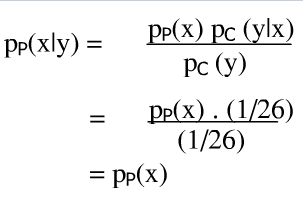
Xét thấy với y cố định, các giá trị y − Kmod 26 sẽ tạo thành một hoán vị của Z26 và  
PP là một phân bố xác suất. Bởi vậy ta có:



Do đó: pC (y ) = 1/26 với bất kỳ y ∈ Z26 .  
Tiếp theo ta có:



Với mọi x ,y vì với mỗi cặp x ,y khóa duy nhất K (khoá đảm bảo eK (x ) = y ) là khoá  
K = y − x mod 26 . Bây giờ sử dụng định lý Bayes, ta có thể dễ dàng tính:



Bởi vậy, MDV có độ mật hoàn thiện.  
Như vậy, mã dịch vòng là hệ mật không phá được miễn là chỉ dùng một khoá ngẫu  
nhiên đồng xác suất để mã hoá mỗi ký tự của bản rõ

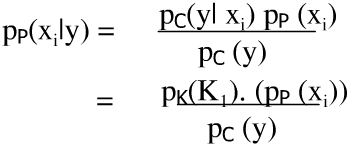
- Mật mã khoá sử dụng một lần của Vernam (One-Time-Pad: OTP):

+ Mô tả hệ mật:

Giả sử n ≥ 1 là số nguyên và P = C = K = (Z2 )n . Với K ∈ (Z2 )n , ta xác định eK(x )  
là tổng vector theo modulo 2 của K và x (hay tương đương với phép hoặc loại trừ của hai dãy  
bit tương ứng). Như vậy, nếu x = (x1 ,...,xn ) và K = (K1,...,Kn ) thì:  
eK(x ) = (x1 + K1,...,xn + Kn ) mod 2  
Phép mã hoá là đồng nhất với phép giải mã. Nếu y = (y1,...,yn ) thì:  
dK(x ) = (y1 + K1 ,...,yn + Kn ) mod 2

+Giả sử (P,C,K,E,D) là một hệ mật , trong đó = = . Khi đó, hệ mật có độ mật  
hoàn thiện khi và chỉ khi khoá K được dùng với xác suất như nhau bằng 1/, và với mỗi  
x ∈ P , mỗi y ∈ C có một khoá duy nhất K sao cho eK(x ) = y .  
 Chứng minh  
Giả sử hệ mật đã cho có độ mật hoàn thiện. Như đã thấy ở trên, với mỗi x ∈ P và  
y ∈ C , phải có ít nhất một khoá K sao cho eK(x ) = y . Bởi vậy ta có bất đẳng thức:  
 =   
Tuy nhiên, ta giả sử rằng = , bởi vậy ta phải có:

Tức là ở đây không tồn tại hai khoá K1 và K2 khác nhau để eK1 (x ) = eK2 (x ) = y . Như vậy ta đã chứng tỏ được rằng, với bất kỳ x ∈ P và y ∈ C có đúng một khoá K để eK (x ) = y .  
Ký hiệu n = . Giả sử P = {xi : 1 ≤ i ≤ n} và cố định một giá trị y ∈ C Ta có thể ký hiệu các khoá K1,K2,...,Kn sao cho eKi (xi) = yi ,1≤ i ≤ n. Sử dụng định lý Bayes ta có:



Xét điều kiện độ mật hoàn thiện pP (x i|y ) = pP (xi) . Điều kiện này kéo theo pK (Ki) = pC (y ) với 1 ≤ i ≤ n . Tức là khoá được dùng với xác suất như nhau (chính bằng pC(y) ). Tuy nhiên vì số khoá là n = nên ta có pK (K ) = 1/ với mỗi K ∈ C .  
Ngược lại, giả sử hai điều giả định đều thoả mãn. Khi đó dễ dàng thấy được hệ mật có độ mật hoàn thiện với mọi phân bố xác suất bất kỳ của bản rõ.

- Ưu điểm của OTP

+An toàn: Giải quyết tốt các vấn đề giả mạo, đánh cắp, Key logger. Đối với hai yếu tố xác thực, thiết bị này có thể được kết hợp với một mã PIN hoặc mật khẩu.  
+Dễ dàng sử dụng: Việc nhận dạng và xác thực được thực hiện trong vài giây tránh được nguy cơ bị lỗi khi gõ các mã OTP dài qua các mã từ một thiết bị chứng thực vào một máy tính (Ví dụ OTP Token sử dụng màn hình hiển thị). Nó hoạt động với  tài nguyên và đăng nhập được trên tất cả các nền tảng máy tính, và trình duyệt không cần phần mềm cài đặt Client. Nhanh chóng và tích hợp dễ dàng vào bất kỳ ứng dụng web nào (Windows, Linux, Mac, Internet Explorer, Firefox,...).  
+Linh hoạt: Người dùng dễ dàng sử dụng cho các máy tính khác nhau và dễ mang theo bên mình.  
+ Mã nguồn mở: Sẵn sàng tích hợp với nhiều ứng dụng mã nguồn mở.

# 3.Mô tả quá trình mã, giải mã của các hệ mật đơn biểu, đa biểu, MHV, hệ mật tích, DES, AES

• HMTT đơn biểu:

+Mã:

– Khi khóa đã được chọn thì mỗi kí tự của bản rõ được ánh xạ đến một kí tự duy nhất của bản mã.

– Mỗi cách mã hóa như vậy sẽ tương ứng với một hoán vị của bảng chữ và hoán vị đó chính là khóa của mã đã cho.

– Như vậy độ dài của khóa ở đây là 26 và số khóa có thể có là 26!

+Giải mã:

Bằng cách thống kê trên bản mã:

– Đếm tần suất của các chữ trong bản mã

– So sánh với các giá trị đã biết

– Tìm kiếm các chữ đơn, bộ đôi và bộ ba hay dùng; và các bộ ít dùng

– Dựa vào bảng tần suất xuất hiện của các chữ cái để đoán và tìm ra bản rõ

•HMTT đa biểu:

+Mã

-Yếu điểm của các mã pháp đơn biểu: Phân bố tần suất của chúng phản ánh phân bố của bảng chữ cái cơ sở. Một mã pháp an toàn hơn về mặt mật mã sẽ thể hiện phân bố bằng phẳng hơn, điểu này sẽ không cho kẻ thám mã chút thông tin nào.

-Một hướng khác làm tăng độ an toàn cho mã trên bảng chữ là sử dụng nhiều bảng chữ để mã.

-Mỗi chữ sẽ được mã bằng bất kì chữ nào trong bản mã tùy thuộc vào ngữ cảnh khi mã hóa. Làm như vậy để trải bằng tần suất các chữ xuất hiện trong bản mã. Do đó làm mất bớt cấu trúc của bản rõ được thể hiện trên bản mã và làm cho mã thám đa bảng khó hơn.

+Giải mã:

Sử dụng phương pháp Kasiski:

-Nhận diện Các mẫu bị lặp có 3 kí tự hoặc hơn

-Với mỗi mẫu ghi ra vị trí bắt đầu mỗi thể hiện của mẫu.

-Tính khoảng cách giữa các điểm bắt đầu của các thể hiện kế tiếp nhau

-Xác định tất cả các tham số cho mỗi khoảng cách.

# 4.Nêu khái niệm về hệ mật tích do Shannon đề xuất. CM tính đúng đắn của quy tắc giải mã trong hệ mật tích.(chưa CM)

Khái niệm

Giả sử P= C= Z26 và giả sử:

K={a Z26: UCLN(a,26)=1}

Với a K ta xác định ea(x)= ax mod 26 và da(y)=a-1y mod 26

Hệ mã Affine

Cho P=C=Z26 và giả sử

K={(a,b) Z26 x Z26:UCLN(a,26)=1}

Với k =(a,b) K, t định nghĩa

ek(x) = ax + b mod 26 và dk(y)= a-1(y-b)mod 26

# 5.M là hệ mã nhân, S là HDV CMR: MxS, SxM chính là hệ mã Affine với các khóa đồng xác suất

-Một khoá dịch vòng là phần tử k ∈ Z26 và quy tắc mã hóa tương ứng là ek (x ) = x + k mod 26 . Còn khoá trong hệ mã nhân là phần từ a ∈ Z26 sao cho ƯCLN (a, 26) = 1. Quy tắc mã tương ứng là ea (x ) = a mod 26 . Bởi vậy, một khoá trong mã tích M × S có dạng (a,k) , trong đó  
 e(a ,k ) = ax + k mod 26  
Đây chính là định nghĩa về khoá trong hệ mã Affine. Hơn nữa, xác suất của một khoá trong hệ mã Affine là: 1/312 = (1/12)(1/26) . Đó là tích của xác suất tương ứng của các khoá a và k . Bởi vậy M × S là hệ mã Affine.  
Bây giờ ta sẽ xét S × M . Một khoá này trong hệ mã này có dạng (k,a) , trong đó:  
 e(k,a ) (x ) = a(x + k) = ax +ak mod 26  
Như vậy, khoá (k,a) của mã tích S × M đồng nhất với khoá (a,ak) của hệ mã Affine. Vấn đề còn lại là phải chứng tỏ rằng mỗi khoá của mã Affine xuất hiện với cùng xác suất 1/312 như trong mã tích S × M . Nhận thấy rằng ak = k1 khi và chỉ khi k = a−1k1 , ( hãy nhớ lại rằng ƯCLN (a, 26) = 1 , bởi vậy a có phần tử nghịch đảo). Nói cách khác, khoá (a,k1 ) của hệ mã Affine tương đương với khoá (a−1k1,a ) của mã tích S × M . Bởi vậy, ta có một song ánh giữa hai không gian khoá. Vì mỗi khoá là đồng xác suất nên có thể thấy rằng S × M thực sự là mã Affine.

# 6.Hệ mật DES (CM phép giải mã đồng nhất phép mã với bảng khóa đảo ngược; các chế độ hoạt động của DES: ECB, CBC, CFB, OFB và các tính chất của chúng), 2DES, 3DES.(chưa CM)

Có 4 chế độ làm việc đã được phát triển cho DES:

1-Chế độ quyển mã điện tử (ECB)

– Mẫu tin được chia thành các khối độc lập, sau đó mã từng khối

– Mỗi khối là giá trị cần thay thế như dùng sách mã, do đó có tên như vậy

– Mỗi khối được mã độc lập với các mã khác Ci = DESK1(Pi)

– Khi dùng: truyền an toàn từng giá trị riêng lẻ

Ưu và nhược của ECB:

– Lặp trên bản mã được chỉ rõ lặp trên bản tin nếu dóng đúng khối, đặc biệt với hình ảnh, hoặc với bản tin mà thay đổi rất ít sẽ trở thành đối tượng để thám mã

– Được sử dụng chủ yếu khi gửi một ít dữ liệu

2-Chế độ phản hồi mã (CFB)

– Bản tin coi như dòng các bít

– Bổ sung vào đầu ra của mã khối

– Kết quả phản hồi trở lại cho giai đoạn tiếp theo, vì vậy có tên như vậy.

– Nói chung cho phép số bít phản hồi là 1, 8, 64, hoặc tuỳ ý: ký hiệu tương ứng là CFB1, CFB8, CFB64,…

– Thường hiệu quả sử dụng cả 64 bít Ci = Pi XOR DESK1(Ci-1 ); C-1 = IV

– Được dùng cho mã dữ liệu dòng, xác thực

Ưu và nhược điểm của CFB

– Được dùng khi dữ liệu đến theo byte/bit. Đây là chế độ dòng thường gặp nhất

– Lỗi sẽ lan ra một vài block sau lỗi

3-Chế độ liên kết khối mã (CBC)

– Các mẫu tin được chia thành các khối

– Nhưng chúng được liên kết với nhau trong quá trình mã hoá

– Các block được sắp thành dãy, vì vậy có tên như vậy

– Sử dụng véctơ ban đầu IV để bắt đầu quá trình Ci = DESK1(Pi XOR Ci-1); C-1 = IV

– Dùng khi: mã dữ liệu lớn, xác thực

Ưu và nhược của CBC

– Mỗi khối mã phụ thuộc vào tất cả các khối bản rõ

– Sự thay đổi của bản tin ở đâu đó sẽ kéo theo sự thay đổi của mọi khối mã

– Cần giá trị véc tơ ban đầu IV được biết trước bởi người gửi và người nhận

• Tuy nhiên nếu IV được gửi công khai, kẻ tấn công có thể thay đổi bít đầu tiên và thay đổi cả IV để bù trừ

• Vậy IV cần phải có giá trị cố định trước hoặc mã hoá trong chế độ ECB và gửi trước phần còn lại của mẩu tin

– Ở cuối bản tin, để kiểm soát các block ngắn còn lại

• Có thể bổ sung các giá trị không phải dữ liệu như NULL

• Hoặc dùng bộ đệm cuối với số byte đếm kích thước của nó. – Ví dụ: [ b1 b2 b3 0 0 0 0 5] <- 3 data bytes, vậy có 5 bytes dành cho đệm và đếm

4-Chế độ phản hồi đầu ra (OFB)

– Mẩu tin xem như dòng bit

– Đầu ra của mã được bổ sung cho mẩu tin

– Đầu ra do đó là phản hồi, do đó có tên như vậy

– Phản hồi ngược là độc lập đối với bản tin

– Có thể được tính trước Ci = Pi XOR Oi ; Oi = DESK1(Oi-1); O-1 = IV

– Được dùng cho mã dòng trên các kênh âm thanh

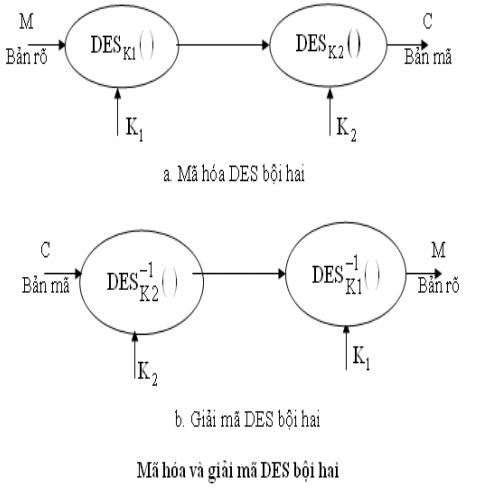
Ưu điểm và nhược điểm của OFB

– Được dùng khi lỗi phản hồi ngược lại hoặc ở nơi cần mã trước khi mẩu tin sẵn sàng

– Rất giống CFB, nhưng phản hồi là từ đầu ra của mã và độc lập với mẩu tin

– Người gửi và người nhận phải đồng bộ, có phương pháp khôi phục nào đó là cần thiết để đảm bảo việc đó.

\*DES bội hai

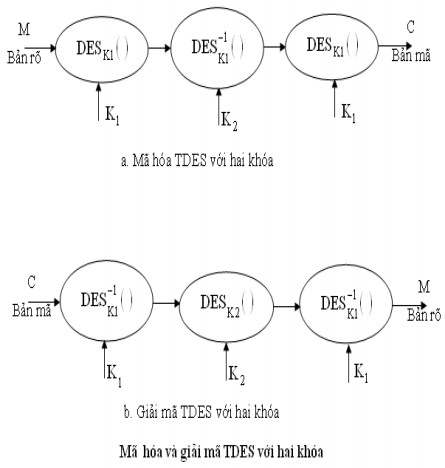


– Mã hóa: C = DESK2[DESK1(M)]

– Giải mã: M = DESK1 -1[DESK2 -1(C)]

¬Có 256 sự lựa chọn cho khóa K1 và 256 sự lựa chọn cho khóa K2 . Bởi vậy có 2112 sự lựa chọn cho cặp khóa (K1 , K2 )

\*DES bội ba



– Mã hóa: C= DESK1{DES-1K2[DES K1(M)]}

– Giải mã: M= DES-1K1{DESK2[DES-1K1(C)]}

– Với TDES việc tìm khóa vét cạn yêu cầu khoảng: 2112 = 5,1923.1023 phép tính TDES, bởi vậy thực tế khó có thể thám mã thành công.

# 7.Phân tích độ an toàn các hệ mật KCK( RSA, Meckle- Hellman, McEliece, ElGamal, Chor-Rivest, Elliptic)

-Hệ mật RSA:  
Độ bảo mật của hệ RSA dựa trên độ khó của việc phân tích ra thừa số nguyên lớn  
- Hệ mật xếp ba lô Merkle - Hellman:  
 Hệ này và các hệ liên quan dựa trên tính khó giải của bài toán tổng các tập con (bài toán này là bài toán NP đầy đủ).  
-Hệ mật McEliece:  
Hệ này dựa trên lý thuyết mã đại số và vẫn còn được coi là an toàn. Hệ mật McEliece dựa trên bài toán giải mã cho các mã tuyến tính (cũng là một bài toán NP đầy đủ)  
-Hệ mật ElGamal:  
Hệ mật ElGamal dựa trên tính khó giải của bài toán logarithm rời rạc trên các trường hữu hạn  
-Hệ mật Chor-Rivest:  
Hệ mật Chor-Rivest cũng được xem như mọt hệ mật xếp ba lô. Tuy nhiên nó vẫn được coi là an toàn

-Hệ mật trên các đường cong Elliptic:

Các hệ mật này là biến tướng của các hệ mật khác(chẳng hạn như hệ mật ElGamal), chúng làm việc trên các đường cong Elliptic chứ không phải là trên các trường hữu hạn. Hệ mật này đảm bảo độ mật với số khoá nhỏ hơn các hệ mật khoá công khai khác.

# 8.Sơ đồ phân loại hàm băm mật mã và ứng dụng, tính chất của các hàm băm không có khóa; các khía cạnh liên quan tới việc xác thực mẩu tin khi truyền tin trên mạng; vẽ sơ đồ và trình bày trạng thái băm : Matyas-Meyer-Oseas, Danes-Meyer

\*Sơ đồ phân loại các hàm băm và ứng dụng:

Hàm băm gồm:

-Không có khóa:

+ MDC:

* OWHF(hàm băm 1 chiều yếu)
* CRHF(hàm băm 1 chiều mạnh

+ Các ứng dụng khác

-Có khóa:

+ MDC

+ Các ứng dụng khác

\*Tính chất của các hàm băm không khóa:

- Hàm băm h là không va chạm yếu: Hàm băm h là không va chạm yếu nếu  
khi cho trước một bức điện x, không thể tiến hành về mặt tính  
toán để tìm ra một bức điện x’ ≠ x mà h(x’) = h(x).

-Hàm băm h là không va chạm mạnh: Hàm băm h là không va chạm mạnh nếu không có  
khả năng tính toán để tìm ra hai bức thông điệp x và x’ mà x ≠ x’  
và h(x) = h(x’).

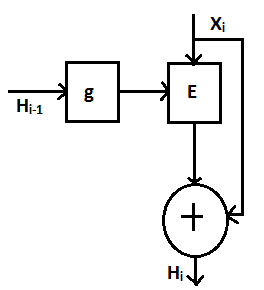
-Hàm băm h là hàm 1 chiều: Hàm băm h là một chiều nếu khi cho trước một bản tóm lược thông  
báo z thì không thể thực hiện về mặt tính toán để tìm ra thông điệp  
ban đầu x sao cho h(x) = z .

\* Các khía cạnh liên quan tới việc xác thực nguồn tin khi truyền tin trên mạng:

- Bảo vệ tính toàn vẹn của mẩu tin: bảo vệ mẩu tin không bị thay đổi hoặc có các biện pháp phát hiện nếu mẩu tin bị thay đổi trên đường truyền

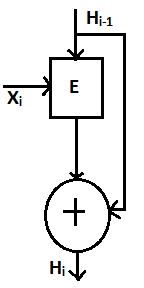
- Kiểm chứng danh tính và nguồn gốc: xem xét mẩu tin có đúng do người xưng tên gửi không hay 1 kẻ mạo danh nào khác gửi mẩu tin chức các thông tin chứng tỏ chỉ có người xưng danh, không 1 ai khác có thể làm điều đó. Như vậy người gửi không thể từ chối hoạt động gửi, thời gian gửi và nội dung của mẩu tin. Ngoài ra có thể xem xét bổ sung thêm các yêu cầu bảo mật như mã hóa có thể sử dụng các phương pháp sau: mã mẩu tin bằng mã đối xứng hoặc bất đối xứng, hoặc sử dụng mã xác thực mẩu tin (MAC) hoặc sử dụng hàm hash (hàm băm),...

-Matyas-Meyer-Oseas



Vào: Xâu bit n  
\* Ra: Mã băm n bit của x  
\* (1) Đầu vào x được phân chia thành các khối n bit và được độn nếu cần thiết nhằm tạo khối cuối cùng hoàn chỉnh. Ta được t khối n bit: x1 x2 … xt. Xác định trước một giá trị ban đầu n bit (kí hiệu IV)  
\* (2) Đầu ra là Ht được xác định như sau: H0 = IV, Hi = Eg(xi) ⊕ xi, 1 ≤ i ≤t

-Danes-Meyer



(1) Đầu vào x được phân chia thành các khối n bit và được độn nếu cần thiết nhằm tạo khối cuối cùng hoàn chỉnh. Ta được t khối n bit: x1 x2 … xt. Xác định trước một giá trị ban đầu n bit (kí hiệu IV)  
(2) Đầu ra là Ht được xác định như sau: H0 = IV, Hi = Exi(Hi-1) ⊕ Hi-1, 1 ≤ i ≤ t

# 9.Trình bày tòm lược các bước trong hệ phân phối khóa dựa trên định danh Okamoto-Tanaka

1. Pha chuẩn bị: Trung tâm xác thực tin cậy chọn 2 số nguyên tố p và q và đưa công khai các giá trị n, g và e, trong đó:

n = p.q

g là phần tử sinh của cả Zp \* và Zq \*

e ∈ Z\* λ(n). Ở đây, hàm Carmichael của n được xác định như sau:

λ(n) = BCNN(p – 1, q – 1)

Tính khoá bí mật của trung tâm d = e-1 mod λ(n) với d ∈ Z\* λ(n).

1. Pha tham gia của người dùng

Cho IDi là thông tin định danh của người dùng thứ i (i = A, B, C, …).

Cho si là khoá bí mật của người dùng i thoả mãn: si ≡ IDi -d mod n.

Sau đó trung tâm sẽ công bố (e, n, g, IDi ) và phân phát si tới mỗi người dùng i qua một kênh an toàn (hoặc bằng cách dùng thẻ)

1. Pha tạo khóa chung

Ta giả sử ở đây rằng hai người dùng Alice và Bob muốn chia sẻ một khoá chung (chẳn hạn để dùng cho một hệ mật khoá bí mật).

Trước tiên Alice tạo một số ngẫu nhiên rA và tính: xASAgrA mod n và gửi nó cho Bob.

Tương tự, Bob tạo một số ngẫu nhiên rB và tính: xBSBgrB mod n và gửi nó cho Alice.

Tiếp theo, Alice tính: WKAB=(IDB.xeB)rA mod n

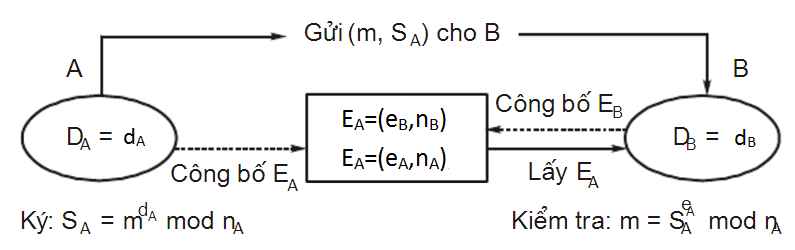
Tương tự, Bob tính: WKBA=(IDA.xeA)rB mod n

# 10.Vẽ và mô tả sơ đồ kí số RSA

a. Trường hợp bản tin rõ m không cần bí mật

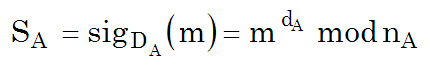
A kí bản tịn m và gửi cho B

B kiểm tra chữ kí của A



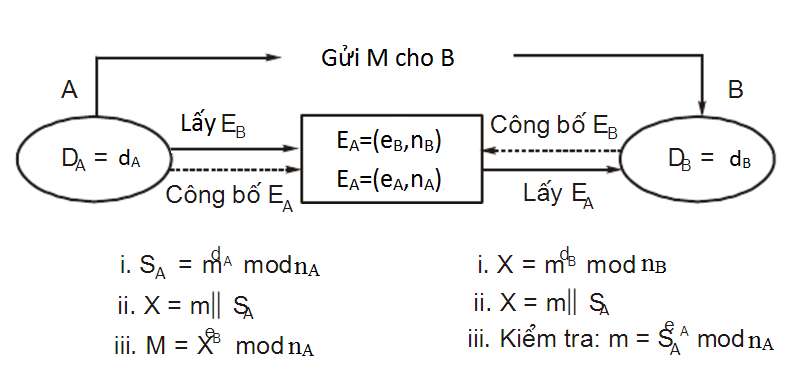
Sơ đồ chữ kí số RSA(không bí mật bản tin)

Giả sử A muốn gửi cho B bản tin rõ m có xác thực bằng chữ kí số của mình. Trước tiên A tính chữ kí số



Sau đó A gửi cho B bộ đôi (m, SA). B nhận được (m, SA) và kiểm tra xem điều kiện m SAeA mod nA có thỏa mãn không. Nếu thỏa mãn, thì B khẳng định rằng verEA (m, SA) nhận giá trị Đúng và chấp nhận chữ kí của A trên m.

b. Trường hợp bản tin rõ m cần giữ bí mật

Sơ đồ chư kí số RSA(có bí mật bản tin)

A kí bản tin rõ m để được chữ kí SA. Sau đó A dùng khóa mã công khai EB của B để lập bản mã

M = EB(m, SA) rồi gửi đến B. Khi nhận được bản mã M, B dùng khóa bí mật DB của mình để giải mã cho M và thu được m, SA. . Tiếp đò dùng thuật toán kiểm tra verEA để xác nhận chữ kí của A.

# 11. Sơ đồ cấu trúc của thuật toán AES, nếu ý nghĩa của tầng phi tuyến, trộn tuyến tính, cộng khóa(chưa có sơ đồ)

\*Sơ đồ

\*Ý nghĩa:

-Tầng phi tuyến: sử dụng hàng subBytes được thiết kế như 1 phép thay thế phi tuyến, tính chất phi tuyến là 1 tính chất quan trọng để ngăn chặn tấn công thám mã.

-Tầng trộn tuyến tính: Tầng này được thực hiện thông qua 2 hàng là ShiftRows và MixColums được thiết kế để trộn các byte trong khối bản rõ. Tầng này đảm bảo khuếch tán cao qua nhiều vòng.

-Tầng cộng khóa: là phép so từng bít của RoundKey và trạng thái trung gian.

Add RoundKey cung cấp tính mật ngẫy nhiên cần thiết cho công bố của thông điệp.

# 12.Hệ mật RSA (Cho ví dụ minh họa về thông báo không thể che giấu, công thức tính số thông báo không thể che giấu). CMR hệ mật RSA là không an toàn nếu dùng chung số modulo n, hoặc bên A,B chọn GCD(eA,eB) =1(chưa CM)

\*Ví dụ:

-Giả sử cặp khóa công khai là (e,n) =(17,35)

-Giả sử thông báo có giá trị bằng 8

-Ta có: 8^17 đồng dư 8mod35

=> Mã hóa của thông báo vẫn là thông báo ban đầu hay với khóa mã là 17 thì thông tin không được che giấu

\*Công thức tính số thông báo không thể che giấu:

-Nếu các thông báo được mã bằng hệ mật RSA với cặp KCK (e,n) với n=p.q thì số các thông báo không thể che giấu được bằng:

N = (1+UCLN(e-1,p-1)).(1+UCLN(d-1,q-1))

BÀI TẬP (về đường cong Elliptic)

1. Cho đường cong E11(1, 6); P = (2, 7)
   * Khóa riêng của B nB = 7. Tính khóa công khai của B
   * Giả sử A cần gửi tin cho B. Hãy mô phỏng quy trình mã hóa bản tin Pm = (10, 9) và giải mã bản mã thu được. Cho giá trị ngẫu nhiên k = 3.
2. Cho đường cong E11(1, 6)
   * Giả sử cần mã hóa các số m = {0, 1, 2, 3, 4, 5}
   * Hãy nhúng các giá trị nói trên thành các điểm trên đường cong và chuyển các điểm trên đường cong thành các giá trị m tương ứng

Giải bài 1 :.

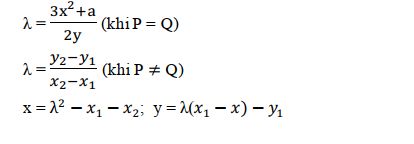
Nhóm E được tạo nên từ đường cong Ep(a, b) = E11(1, 6). Vậy đường cong có phương trình tương ứng là:

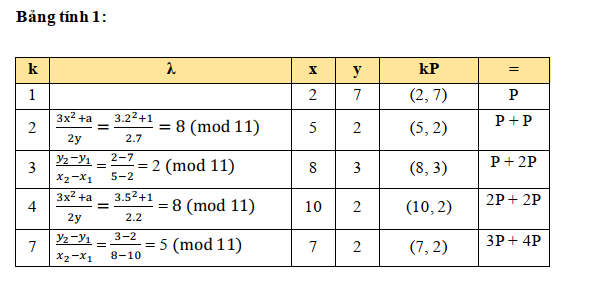
y2 = x3 + x + 6 (mod 11) Trong đó: a = 1, b = 6 và p = 11

- Ta tính được khóa công khai của B là:

PB = nB.P = 7.(2, 7)

Ta có bảng tính bên dưới. Trong đó:





Từ bảng tính trên ta tính được khóa công khai của B : P(B) = ( 7, 2)

**Mã hóa thông điệp:**

Khi A muốn gửi tin cho B: A sử dụng khóa công khai của B và số ngẫu nhiên để mã hóa thông điệp gửi qua cho B.

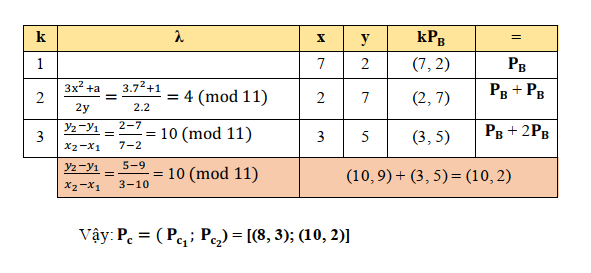
Với: k = 3; P = (2, 7); PB = (7, 2) và Pm = (10, 9)

Ta có:

- Bản mã: Pc = [(kP); (Pm + kPB )]:

Xét Pc1= kP = 3(2, 7) = (8, 3) {Bảng tính 1}

Xét Pc2= Pm + kPB = (10, 9) + 3(7, 2). Ta có bảng tính 2:



A sẽ gửi bản mã để B giải mã

# Giải mã thông điệp:

Khi A gửi tin cho B, B nhận được cặp điểm của bản mã là:

Pc = ( Pc1 ; Pc2) = [(kP); (Pm + kPB )] = [(8, 3); (10, 2)]

Giải mã lại bằng khóa bí mật của B: nB = 7 và k = 3. Ta có:

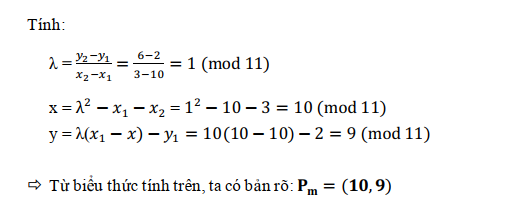
Pm = (Pm + kPB ) − nB(kP)

= (10,2) − 7(8, 3) = (10, 2) − 7[3(2, 7)]

= (10,2) − 21(2, 7)= (10, 2) − (3, 5) {Bảng tính 2}

= (10,2) + (3, −5) = (10, 2) + (3, 6)

Tính:



Bài 2 : Giải

Đường cong E97 (1, 6) và các số cần mã hóa: m = {0, 1, 2, 3, 4, 5} Ta tính hệ số nhúng:

