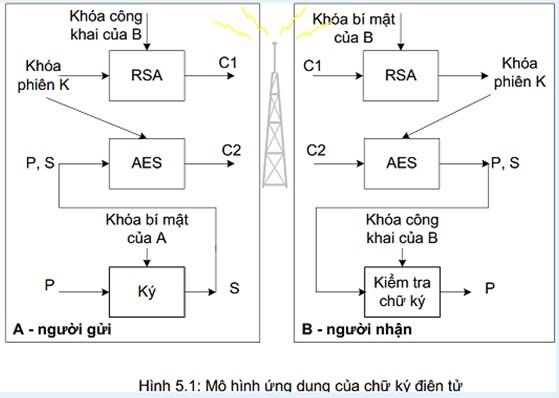
CT: phi^(-a) = phi^(p-1-a) mod p

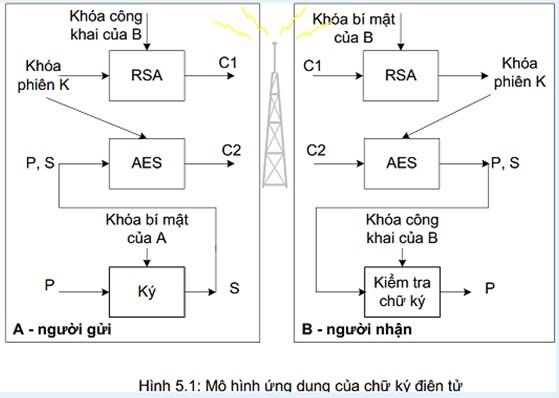
X= phi^(-a)\*xichma mod p

1. Chữ ký điện tử được hiểu là : Một phép kiểm tra trong đó mọi người có thể kiểm tra, duy nhất 1 người có thể mã hóa
2. Trong một chữ ký điện tử tiêu chuẩn, phát biểu nào sau đây là đúng: Tất cả chữ ký trên mọi văn bản đều có kích thước như nhau
3. Không thể sử dụng các thuật toán cổ điển để xây dựng chữ ký điện tử vì: Các thuật toán cổ điển là hệ mã hóa đối xứng
4. Chức năng chính của chữ ký điện tử là: Nhằm giúp xác thực tính sở hữu của văn bản
5. Hãy cho biết phát biểu nào sau đây đúng về chữ ký điện tử: Chữ ký điện tử có kích thước bằng đúng nội dung ký lên
6. Phát biểu nào sau đây đúng về chữ ký điện tử: Chữ ký điện tử có thể sử dụng để xác thực tính toàn vẹn dữ liệu
7. Phát biểu nào sau đây đúng về chữ ký điện tử: Chữ ký điện tử chỉ có thể được xây dựng trên các hệ mã hóa phi đối xứng (Công khai)
8. Chọn câu đúng:

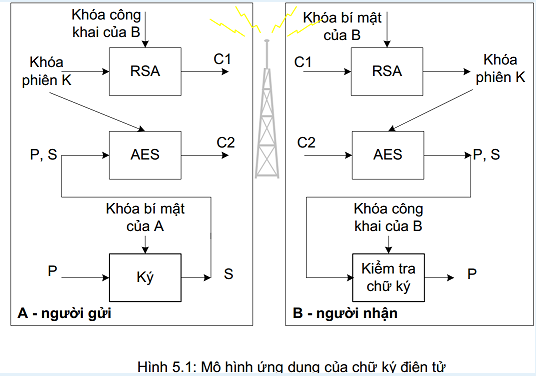


Khóa K được mã hóa bằng thuật toán RSA vì kích thước khóa K là nhỏ, thuật toán RSA có độ án toàn cao hơn

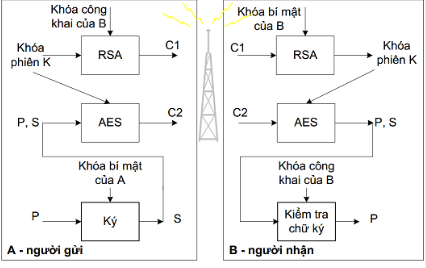
1. Chọn câu đúng:



Người gửi sẽ tự sinh khóa K rồi mã hóa khóa K bằng khóa công khai của B và gửi cho B nhằm đảm bảo an toàn

1. 

Ưu điểm của sơ đồ trên là có thể tận dụng được tốc độ xử lý nhanh của AES và tính phức tạp của RSA

1. 

Trong sơ đồ trên,P và S sử dụng AES để mã hóa vì tốc độ AES nhanh và kích thước của S lại lớn

1. Phát biểu nào sau đây sai về chữ ký điện tử: Chữ ký điện tử có thể tạo bởi các hệ mã hóa phi đối xứng hoặc đối xứng
2. Phát biểu nào là đúng về chữ ký điện tử: Chữ ký điện tử có thể xác minh đây đúng là văn bản của đối tượng sở hữu chữ ký hay không
3. Sử dụng chữ ký điện tử lên đại diện nội dung số phục vụ mục đích: Giúp giảm thiểu kích thước cần ký trên nội dung số
4. Chữ ký số giống với hệ mã hóa khóa công khai ở các điểm: Cùng sử dụng 2 khóa bí mật và công khai
5. Chữ ký số khác với hệ mã hóa khóa công khai ở điểm: Sử dụng 02 khóa bí mật và công khai như nhau nhưng vai trò đối tượng tham gia được đổi lại
6. Giải thuật chữ ký số tiêu chuẩn DSA sử dụng hàm băm SHA-1 sinh chữ ký độ dài: 160 bit
7. Kết luận nào sau là đúng cho giải thuật chữ ký số: có thể xác nhận chữ ký và văn bản đã ký
8. Giải thuật chữ ký số nào là cơ sở của giải thuật chữ ký số tiêu chuẩn: giải thuật chữ ký số El Gamal
9. Kết luận nào là đúng cho hệ chữ ký số El-Gamal: giải thuật chữ ký số có thể sinh nhiều chữ ký khác nhau từ một văn bản
10. Cấu tạo của một chữ ký số tiêu chuẩn gồm: Chỉ gồm chữ ký trên đại diện
11. Kết luận nào sau là đúng: Chữ ký số được hình thành từ các thuật toán mã hóa khóa công khai
12. Hãy cho biết những đặc điểm đúng về hàm băm: Với mỗi giá trị đầu vào chỉ duy nhất có một giá trị đầu ra tương ứng
13. Hàm băm Md-5 tạo ra được bao nhiêu giá trị băm: 4 lũy thừa 64
14. Hàm băm SHA-1 tạo ra được bao nhiêu giá trị băm: 4 lũy thừa 80
15. những đặc điểm đúng về hàm băm: Các đầu vào khác nhau sẽ băm được các giá trị đầu ra khác nhau
16. Kết luận nào sau là đúng cho hàm băm: Hàm băm xác thực sự toàn vẹn thông tin
17. Phát biểu nào sau đây đúng về hàm băm: Hai đầu vào khác nhau có thể ra các đầu ra giống nhau
18. Phát biểu nào sau đây đúng về hàm băm: Kích thước đầu vào hàm băm không phụ thuộc vào kích thước dữ liệu đầu vào và giống nhau với mọi đầu vào
19. Vì sao ta coi kết quả băm của một thông điệp qua hàm băm là đại diện của thông điệp đó: Kết quả băm được có kích thước nhỏ hơn kích thước của thông điệp và được coi là duy nhất vì khả năng 2 thông điệp băm cùng kết quả có xác xuất rất thấp
20. Một thông điệp có độ lớn là 1024 byte. Sau khi qua hàm băm lần 1 thu được kết quả là 512 byte. Hỏi nếu qua 3 lần hàm băm liên tiếp ta thu được kết quả bao nhiêu: 512 byte
21. Nếu một thông điệp có độ lớn P < k là kích thước giới hạn của hàm băm, kết quả thu được sẽ là: Đại diện P có kích thước k
22. Hiện tượng xung đột bảng băm được hiểu: Hiện tượng với hai dữ liệu đầu vào khác nhau, giá trị đầu ra bảng băm là như nhau
23. Khi sử dụng hàm băm, ta sẽ thu được đại diện của thông điệp có đặc điểm: Đại diện là duy nhất và có kích thước luôn cố định
24. Để có thể tận dụng ưu điểm của hệ mã hóa khối và hệ mã hóa công khai, mô hình kết hợp của hai hệ mã được sử dụng như sau: Hệ mã hóa khối sẽ mã hóa thông điệp với khoa K, hệ mã hóa công khai sẽ mã hóa khóa K
25. Thuật toán mã hóa khối được hiểu là: Dữ liệu đầu vào được đem đi mã hóa sẽ được chia thành các khối có độ dài quy ước
26. Thuật ngữ AES được hiểu: Một chuẩn mã hóa bí mật
27. Chuẩn mã hóa khối hiện nay là: AES
28. Tốc độ xử lý của hệ mã hóa khối thường nhanh là do: Cả 3 đáp án hiện có đều sai
29. Trong hệ thống kết hợp giữa RSA và AES thì chức năng của các hệ mã hóa là : AES mã hóa thông điệp, RSA mã hóa khóa của AES
30. Thuật toán mã hóa khối được hiểu là: Dữ liệu đầu vào được đem đi mã hóa sẽ được chia thành các khối có độ dài qui ước
31. Số lượng bảng số sử dụng trong Des là: 15
32. Không sử dụng hệ mã hóa DES để xây dựng chữ ký số DES vì: DES là hệ mã hóa đối xứng
33. Trong sơ đồ sinh khóa của Des: 16 khóa con, mỗi khóa độ dài 48 bít
34. Giải thuật mã hóa và giải mã Des có đặc điểm:

a. độ dài khóa có lựa chọn

b. cấu trúc đại số

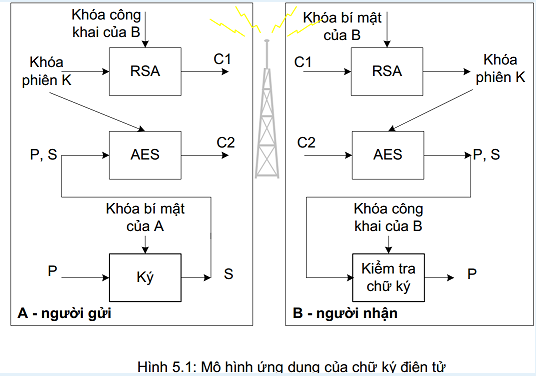
c. của ba đáp án trên

d. sử dụng nhiều hàm phi tuyến

1. Phát biểu nào sau đây là chính xác: Hệ mã hóa DES là hệ mã đối xứng vì khi có khóa để mã hóa ta dễ dàng suy ra được khóa để giải mã
2. Tăng độ an toàn của Des bằng cách: tăng độ dài khóa của Des
3. Giải thuật nào sau đây là không dùng khóa đối xứng: El-Gamal
4. Giao thức có người phân xử được hiểu: Các qui tắc giao dịch được xây dựng từ trước, người trung gian chỉ được sử dụng khi có tranh chấp xẩy ra
5. Những điều không đúng trong giao thức có trọng tài: Trọng tài là đối tượng đề ra qui tắc trong giao dịch và giám sát các bên tham gia
6. Những điều nào đúng về giao thức có trọng tài: Trọng tài là đối tượng không có quyền lợi trực tiếp trong giao dịch và được sự tin tưởng của các bên tham gia
7. Kết luận nào sau là đúng cho những giao thức quản lý khóa: sinh và quản lý khóa phiên cho mỗi bên
8. Sơ đồ phân phối khóa Kerberos, kết luận nào sau là sai: hai bên dùng khóa cũ để mã hóa và giải mã cho phiên truyền tin mới
9. Hệ phân phối khóa Kerberos có chức năng: Kết hợp 3 chức năng trên
10. Phát biểu nào sâu đây đúng về hệ mã KnapSack: Dữ hiệu vào của hệ mã Knapsack là số bit theo cài đặt riêng
11. Kết luận nào sau là đúng cho mã khối: bản mã và bản rõ có độ dài bằng nhau
12. Chế độ sử dụng mã khối nào được ứng dụng chính: 3 chế độ trên
13. Chứng chỉ khóa công khai dùng để: Cung cấp khóa công khai
14. Các bảng hoán vị trong hệ mã khối được hiểu là : Bảng hoán vị thỏa mãn điều kiện đảo ngược các bit đầu ra so với các đầu vào

Bảng thứ tự các bit đã được sắp xếp lại theo 1 thứ tự nào đó

1. Phát biểu nào sau đây là chính xác: Hệ mã hóa RSA là hệ mã hóa phi đối xứng vì khi biết được một khóa công khai ta rất khó khăn khi suy ra khóa bí mật
2. Hệ mã RSA có thể bị giải mã theo định lý đồng dư TQ nếu: số mũ giải mã d nhỏ
3. Nguyên nhân khiến tốc độ giải mã của RSA chậm là: Số mũ giải mã d lớn
4. Phát biểu nào sau đây đúng về hệ mã RSA: Độ an toàn của hệ mã RSA phụ thuộc vào bài toán tính số nguyên tố p,q khi biết N=p\*q
5. Các yếu tố không ảnh hưởng đến sự an toàn của một hệ mã mật: Phương pháp mã hóa/ giải mã. Đáp án 2: Độ phức tạp tính toán của hệ mã.
6. Hệ thống quản lý khóa công khai có chức năng chính: Trung tâm phân phối khóa (xây dựng và quản lý khóa) với cả hệ thống
7. Trong mật mã khóa công khai, khóa công khai dùng để làm gì: mã hóa và sinh chữ ký
8. Một trong những nhược điểm của hệ mã Merkle – Hellman: giải thuật sinh khóa siêu tăng đơn giản
9. Trong các hệ mã sau, hệ mã hoá công khai là hệ mã: . Khóa được chia làm 2 phần, 1 phần được công khai và phần còn lại được giữ bí mật
10. Phát biểu nào sau đây là chính xác: Hệ mã hóa cổ điển là hệ mã hóa đối xứng vì khi ta biết khóa để mã hóa sẽ dễ dàng suy ra được khóa để giải mã
11. Phương pháp nào dễ phát hiện nhất trong các phương pháp tấn công sau: Tấn công từ chối dịch vụ
12. So sánh tốc độ mã và giải mã của hệ mật mã công khai với mật mã bí mật khối hiện đại: Mật mã công khai chậm hơn
13. Theo Kichoff, sự an toàn của hệ mật phụ thuộc vào: sự bí mật của khóa
14. Mô hình mã hóa kết hợp giữa hệ mã hóa công khai và bí mật được sử dụng là:



Sử dụng hệ mã hóa bí mật mã hóa thông điệp, hệ mã hóa công khai mã hóa khóa bí mật và cùng truyền

1. Trong hệ thống có n thành viên tham gia, nếu sử dụng hệ mã hóa bí mật mỗithành viên cần nắm số khóa là: n\*(n-1)/2
2. Phát biểu nào sau đây đúng về độ an toàn của hệ mã hóa trên đường cong Elliptic: Phụ thuộc vào bài toán tìm k khi biết Q,p trong phép Q=k\*p với Q,p là 2 điểm trên đường cong
3. Hình thức tấn công giao thức thụ động được hiểu: Đối tượng thứ 3 nghe lén các giao dịch, thu thập thông tin về các giao dịch
4. Hình thức tấn công giao thức chủ động được hiểu: Đối tượng thứ 3 nghe lén các giao dịch, tìm hiểu các qui tắc và sau đó can thiệp các phiên giao dịch
5. Phát biểu nào sau đây đúng về hình thức tấn công giao thức thụ động: Đối tượng tấn công là người ngoài hệ thống, thu thập thông tin về các giao dịch trong hệ thống
6. Mã hóa là: Biến đổi thông tin từ dạng đọc được sang dạng không đọc được
7. Giải mã là: biến đổi thông tin từ dạng không đọc được sang dạng đọc được
8. Ưu điểm của hệ mã khóa bí mật so với hệ mã hóa khóa công khai là: Tốc độ xử lý của hệ mã khóa bí mật cao hơn hệ mã khóa công khai
9. Giải thuật Oclit dùng để: Tìm giá trị nghịch đảo của số nguyên và tìm ước số chung lớn nhất giữa hai số nguyên
10. Khi ký lên một nội dung số có kích thước lớn ta thường thực hiện: Ký trên đại diện của nội dung số
11. Giải thích nào là đúng về tấn công thụ động trong các ý dưới đây: Tấn công thụ động là việc đối tượng tấn công chờ đợi quá trình truyền dữ liệu giữa các bên để qua đó đọc dữ liệu trên đường truyền
12. Giao thức trao đổi khóa sử dụng chứng chỉ khóa công khai nhằm mục tiêu: chống giả mạo danh tính
13. Mục tiêu chung của an toàn bảo mật thông tin: Cả 3 phương án trên
14. Theo luật của Kirchoff thì độ an toàn của hệ mã phụ thuộc vào yếu tố nào: Khóa
15. Ứng dụng của hệ mật mã bao gồm: Bảo mật dữ liệu, xác thực toàn vẹn thông tin, chữ ký số và quản lý khóa
16. Các cách tăng sự an toàn của bản rõ trong hệ mã là: Nén bản rõ, che giấu mqh giữa bản rõ và bản mã, tăng sự phụ thuộc giữa bản mã và bản rõ
17. Lược đồ của một hệ mật mã có mấy thành phần : 5 tập khác nhau
18. SKC(Symmetric Key Cryptosytems) được hiểu là: Hệ mã khóa đối xứng
19. PKC(Asymmetric Key Cryptosytems) được hiểu là: Hệ mã khóa phi đối xứng
20. Các yếu tố không ảnh hưởng đến sự an toàn của 1 hệ mã mật : Độ dài bản mã
21. Có mấy phương pháp chính cho việc mã hóa và giải mã: 3 ( mã hóa khóa đối xưng, mã hóa khóa công khai, hàm băm)
22. Theo Shannon, để che giấu sự dư thừa thông tin bảng rõ: Bản mã có sự lộn xộn và sự rườm rà
23. Theo Shannon, entropy được hiểu là gì: Đo khối lượng thông tin của thông điệp
24. **Nghịch đảo của một số nguyên tố a trong tập ZN là số:**  Tồn tại theo điều kiện
25. Tập giá trị của Z26 có bao nhiều phần tử khả nghịch: 12
26. Tìm nghịch đảo của 7 trong Z11: 8
27. Cho a=6 có phải phần tử khả nghịch trong Z8: Không
28. Tập Z9 có bao nhiêu phần tử khả nghịch: 6
29. Tìm tập giá trị khả nghịch của Z10: 1,3,7,9
30. Trong các số sau số nào không đồng dư với 9 khi modulo với 5: -11
31. Trong các số sau số nào không đồng dư với -132 khi modulo với 5: -12
32. Tập Z13 có bao nhiều phần tử khả nghịch: 12
33. Trong hệ mã khối, sử dụng bảng thay thế số liệu ( s-box) cho biểu thức tính toán để : Tăng tốc độ tính toán
34. Các hộp mật(S-Box) của giải thuật Des : Đầu vào là chuỗi bit có độ dài 48 và đầu ra là các chuỗi 32 bit
35. Kết luận nào sau là đúng cho DES : Là hệ mã hóa dựa trên mã Lucipher
36. AES có mấy khóa chính( khóa chủ) : 3
37. Có mấy chế độ sử dụng mã khối : 3
38. Số lượng S-box của giải thuật Des : 8
39. Các hệ mã hóa cổ điển là hệ mã: Mã hóa một hoặc cụm ký tự rời rạc
40. Trong hệ mã VIGENERE, nếu áp dụng bộ ký tự ASCII cho không gian bản rõ và bản mã thì với khóa độ dài 10 sẽ có số lượng khóa : 256˄10
41. Giải thuật mã hóa AES sử dụng khóa chủ độ dài 192 có số vòng lặp : 12
42. Chế độ sử dụng mã khối nào là phổ thông : CBC
43. Chế độ sử dụng mã khối nào k sử dụng giá trị IV ( Initialization Vector): ECB
44. Hệ mã Aes có mấy bảng thế S-box cho quá trình mã hóa : 1
45. Cấu trúc đại số của DES khiến :Độ phức tạp không tăng nếu mã hóa lặp nhiều lần với các khóa cùng kích thước
46. Trong hệ mã hóa khóa công khai nhận định nào sau đây là ĐÚNG :Sử dụng khóa công khai để MÃ HÓA, khóa bí mật để GIẢI MÃ
47. Nhận định nào Sai trong hệ mã hóa PKC: Sử dụng 1 khóa mật chung cho cả 2 hệ mã
48. Kết luận nào ĐÚNG cho hệ mã hóa trên đường cong Elliptic: Độ dài khóa nhỏ hơn RSA nhưng đáp ứng độ an toàn
49. Ý tưởng của hệ mã hóa Knapsack ( Merkle – Hellman) là :Bài toán đóng thùng
50. Ý tưởng của hệ mã hóa RSA : Tính khó giải của bài toán phân tích một số thành 2 thừa số nguyên tố
51. Ý tưởng của hệ mã hóa Elgama : Tính khó giải của bài toán Logarit rời rạc
52. Trong các hệ mã hóa sau hệ mã nào không phải hệ mã hóa khóa công khai : DES
53. Trong các hệ mã hóa sau hệ mã nào không phải hệ mã hóa khóa bí mật :Trapdoor
54. Trong các hệ mã hóa sau hệ mã nào không phải hệ mã hóa khóa khối : DSA
55. Chữ ký số là gì : sử dụng khóa bí mật để ký, khóa công khai để kiểm tra chữ ký
56. Nhược điểm của hệ mật mã khóa công khai : Tốc độ xử lý của thuật toán chậm
57. Mô hình mã hóa kết hợp giữa hệ mã hóa công khai và bí mật được sử dụng là : Sử dụng hệ mã hóa bí mật mã hóa thông điệp, hệ mã hóa công khai mã hóa khóa bí mật và cùng truyền
58. Hiện tượng lộ bản rõ trong thuật toán RSA được hiểu : Kết quả mã hóa không thay đổi so với thông điệp gốc
59. Kết luận nào đúng về hệ mã hóa trên đường cong Elliptic : Khóa riêng là một điểm trên đường cong
60. Kết luận nào đúng cho hệ mã hóa trên đường cong Elliptic : Độ dài khóa nhỏ hơn RSA nhưng đáp ứng độ an toàn
61. Trong hệ thống kết hợp giữa RSA và AES thì chức năng của các hệ mã hóa là: AES mã hóa thông điệp, RSA mã hóa khóa của AES
62. Kết luận nào đúng : Mật mã ECC được ứng dụng trong chữ ký số
63. Kết luận nào đúng: Hệ mã Merkle - hellman có cửa bẫy là khóa siêu tăng
64. Kết luận nào sai : Hệ mã hóa Elgamal luôn tồn tại hiện tượng bản rõ trùng bản mã
65. KẾT LUẬN SAI : Hệ mã hóa Elgamal được ứng dụng rộng rãi
66. Kết luận nào sai: Hệ mã hóa Merkle – Hellman có độ dài khóa nhỏ
67. Kết luận nao sai vs hệ mã khóa ECC :ECC dễ triển khai cài đặt
68. So với hệ mã khối, hệ mã mật khoa công khai có đặc tính gì :Có tốc độ tính toán chậm
69. Hàm băm có số lượng giá trị băm là 216 , nếu thám mã thử 512 văn bản khác nhau thì khả năng đụng độ : 0.86
70. Hàm băm có số lượng giá trị băm là chuỗi 16 bit , nếu thám mã tìm khả năng đụng độ là 0.5 thì số lượng ít nhất văn bản khác nhau đem thử: 301.4144
71. Kết luận nào đúng :Hệ mã PKC cho phép mã hóa khóa của hệ mã SKC
72. Kết luận nào đúng :Hệ mã Merkle - Hellman an toàn kém so với RSA
73. Chữ ký số được hiểu là : Một phép kiểm tra trong đó nhiều người có thể kiểm tra nhưng chỉ một người được tạo chữ ký
74. Sử dụng chữ ký số lên đại diện nội dung số: Tăng tính bảo mật của nội dung số

Tạo và xác nhận chữ ký nhanh chóng

1. Để ký lên một nội dung số có kích thước lớn, thực hiện: ký trên đại diện của nội dung số
2. Chữ ký số RSA giống với hệ mã hóa RSA ở các điểm: Sử dụng khóa bí mật và công khai
3. Chữ ký số RSA khác với hệ mã hóa RSA ở các điểm : Sử dụng khóa bí mật và công khai nhưng 2 khóa được định nghĩa khác nhau hoàn toàn (80%)

Sử dụng chung cặp khóa nhưng thứ tự sử dụng khóa ngược nhau

1. Hãy cho biết đặc điểm hàm băm:Tạo giá trị đầu ra có độ dài không đối
2. Kết luận nào đúng cho hàm băm: Giá trị băm là đại diện của đầu vào
3. Kết luận nào đúng cho hàm băm: Hàm băm mạnh là hàm băm phi đụng độ cao
4. Cấu trúc của một hệ chữ ký số gồm: Đại diện thông điệp và chữ ký
5. Chữ ký số tiêu chuẩn DSS sinh chữ ký độ dài: 512 bit
6. Kết luận nào đúng cho hàm băm MD-5: có 2^128 giá trị băm
7. Kết luận nào đúng cho hàm băm SHA-I: có 2\*160 giá trị băm
8. kết luận nào đúng cho hàm băm: Phi đụng độ của MD-5 hơn so với SHA-1
9. kết luận nào đúng cho hàm băm: Hàm băm được dùng tạo tài khoản người dùng trên mạng
10. Một thông điệp có độ lớn là 1024 byte. Sau khi qua hàm băm lần 1 thu được kết quả 16 byte. Hỏi nếu qua 2 lần hàm băm liên tiếp ta thu được kết quả bao nhiêu: 16 byte
11. Cơ sở của giải thuật chữ ký số tiêu chuẩn DSA: Giải thuật chữ ký số El-gamal
12. Hàm băm có số lượng giá trị băm là 10 bit, nếu thám mã thử 120 văn bản khác nhau thì khả năng đụng độ : 0.99906
13. Hàm băm có số lượng giá trị băm là 2 mũ 10 , nếu thám mã tìm khả năng đụng độ là 0.5 thì số lượng ít nhất văn bản khác nhahu đem đi thử: 37.67 sấp sỉ 38
14. Cho hàm băm có không gian băm 10 bit, nếu thám mã tìm khả năng đụng độ là 0.4 thì sô lượng ít nhất vb khác nhau đem thử: 33
15. Hệ thống phân phối khóa Blom thực hiện: Phân phối một hàm số riêng, người dùng tự xây dựng khóa dùng chung nhờ kết hợp hàm số riêng với khóa công khai
16. Nhãn thời gian trong giao thức Kerberos loại bỏ trường hợp thám mã: Sử dụng khóa cũ
17. Giao thức Diffie-Hellman sử dụng chứng chỉ loại trừ thám mã: Giả mạo danh tính
18. Giao thức thỏa thuận khóa Diffie-Hellman sinh khóa phiên dựa trên: Mật mã trên đường cong Elliptic
19. Giao thức phân phối khóa được hiểu là gì: Có trung tâm phân phối khóa tham gia tạo, gửi khóa
20. Giao thức thỏa thuận khóa: Hai bên thực hiện quản lý, trao đổi khóa
21. Hệ thống phân phối khóa Blom trường hợp đơn giản chỉ an toàn cho nhóm có tối đa: 3
22. Giao thức có người phân xử được hiểu : Các quy tắc giao dịch được xây dựng từ trước, người trung gian chỉ được sử dụng khi có tranh chấp xẩy ra.
23. Giao thức tự phân xử được hiểu: Các bên tự giám sát lẫn nhau, khi thấy có dấu hiệu vi phạm quá trình giao dichj bị dừng lại để xác minh
24. Hình thức tấn công thụ động được hiểu: Đối tượng thứ 3 nghe lén các giao dịch, thu thập thông tin về các giao dịch.

Thám mã nghe lén các giao dịch, thu thập thông tin về các giao dịch.

1. Hình thức tấn công chủ động được hiểu: Đối tượng thứ 3 nghe lén các giao dịch, tìm hiểu các quy tắc và sau đó can thiệp các phiên giao dịch.

Thám mã nghe lén các giao dịch, tìm hiểu các qui tắc và sau đó can thiệp các phiên giao dịch

1. Giải thuật Lehman có thể được áp dụng cho: Giải hệ mã RSA
2. Giải thuật lũy thừa nhanh được áp dụng cho: Hệ mã khóa công khai và chữ ký số
3. Định lý phần dư Trung hoa dùng cho: Giải hệ mã RSA
4. Theo khái niệm Entropy thì số bit thông tin để cần thiết cho bảng mã ASCII chuẩn là: 256
5. Hệ mã Ceasar được biết là một: Hệ mã khóa cổ điển
6. Ý tưởng mã hóa của Ceasar là gì: Cả hai phương án A B
7. Trong thao tác với chuỗi bit phép toán modulo 2 tương ứng với phép logic nào sau đây: XOR
8. Hệ mã cải tiến của DES là TDES dựa trên việc: Thực hiện bội 3 của DES
9. Các phép biến đổi LSi trong sơ đồ tạo khóa của mã hóa Des là: Phép dịch vòng trái
10. Phép toán cộng bit trong sô đồ hàm f là phép:
11. Chữ ký số khác với hệ mã khóa công khai ở điểm: Sử dụng 2 khóa bí mật và công khai như nhau nhưng vai trò đối tượng tham gia được đổi lại.
12. Chứng chỉ khóa công khai có mô tả: Khóa, giải thuật mã hóa và giải mã văn bản
13. Kết luận nào đúng cho X.509: Chuẩn chứng chỉ khóa công khai
14. Giao thức thỏa thuận khóa: Tạo khóa cho hệ mã khóa đối xứng, khóa phi đối xứng, và hệ chữ ký số.
15. Cho chuỗi trạng thái vào 48 7E 52 FA sẽ tương ứng với bao nhiêu bit trong hệ mã AES: 32
16. Trong hệ mã RSA có n, e là khóa công khai, trong đó e được chọn như thế là: E được chọn là khả nghịch theo Zn
17. Chứng chỉ khóa công khai được dùng cho: Mã hóa khóa công khai, chữ ký số và giao thức quản lý khóa
18. Một điều kiện của một hệ mã mạnh: không thể giải mã bởi thám mã
19. Hệ mã khóa dòng được biết là một: Hệ mã khóa đối xứng
20. Al-Kindi, một nhà toán học Ả Rập nổi tiếng đã phát minh ra phương pháp phá mã thông tin sử dụng kỹ thuật Ceasar bằng cách nào: Phân tích tần suất của các ký tự trong bản mã
21. Giải thuật mã hóa của Aes có số vòng lặp: 10, 12, hoặc 14
22. Đầu vào của hệ mã DES là một: Khối 64 bit
23. Các hộp S (Secure – Box) các tác dụng gì: Biến chuỗi bit vào 6 bit thành chuỗi ra 4 bít
24. Trong hệ mã RSA, n, e là khóa công khai, trong đó n được chọn như thế là: N = tích của 2 số nguyên tố lẻ