Tổng hợp đề An Toàn và bảo mật thông thin

**ĐỀ 1**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(K,M) || E(PRa, H(M))

**Câu 2:**

Quy trình chuyển giao khoá phiên giữa client và server trong TLS diễn ra như thế nào? Quy trình đó có đảm bảo an toàn cho khoá phiên không, tại sao?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím. Nhập khóa K (dài 16 bit) từ bàn phím . Chia chuỗi thành từng khối 16bit (nếu độ dài chuỗi không phải là bội số của 16 bít thì có thể chèn thêm các kí tự quy ước). Mã hóa chuỗi ban đầu bằng cách XOR từng khối của chuỗi với K. Hiện thị chuỗi sau khi mã hóa màn hình. Giải mã và hiện chuỗi sau khi giải mã ra màn hình.

**Đề 2**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(PU­B, [M || E(K1, H(M))])

**Câu 2:**

Worm và virus máy tính có gì giống và khác nhau ? Kỹ thuật tìm diệt chúng khác nhau như thế nào ?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập số nguyên k thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức: C = 7\*P + k Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 3**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(K, [M || E(PRA, H(M)) ]) || E(PUB, K)

**Câu 2:**

Trong giao dịch điện tử SET, thông tin đơn hàng OI cần được gửi cho người bán. OI thường được ghép với chữ ký kép và PIMD trước khi gửi đi . Ghép PIMD vào đề làm gì , bỏ đi có được không ?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên x ,y thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = P/x +y

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 4**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(K,M) || H(E(K, M))

**Câu 2:**

Loại hàm toán học nào thường được sử dụng trong mật mã khoá công khai? Đặc điểm cơ bản của chúng là gì ? Hãy lấy ví dụ một hàm như vậy và giải thích

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên x ,y thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = P/x +y

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 5**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

A -> B : E(K2 , [M || C(K1, M)]) || E(PUB, [K1 || K2])

**Câu 2:**

Phân biệt Mật mã cổ điển và mật mã hiện đại, Nêu ưu và nhược điểm của mật mã cổ điển và mật mã hiện đại?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên a ,b thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = P + a \* b

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 6**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(K1,M) | | C(K2, E(K1, M)) | | E(PUB, [K1 || K2])

**Câu 2:**

Quy trình chuyển giao khóa phiên giữa client và server trong **SSL** diễn ra như thế nào? Quy trình đó có đảm bảo an toàn cho khóa phiên không, tại sao?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên x ,y thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = x/y + P

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 7**

**Câu 1 :**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(K1, M) || C (K2, E(K1, M))

**Câu 2:**

Trong giao dịch điện tử SET, thông tin thanh toán PI cần được gửi cho người bán. PI thường được ghép với chữ ký kép và OIMD trước khi gửi đi. Ghép OIMD vào để làm gì, bỏ đi có được không?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên x ,y thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = x \* y + P

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 8**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(PUB, [H(M) || M])

**Câu 2:**

Trong giao dịch điện tử SET, chữ ký kép (dual signature) thường được sử dụng để đảm bảo tính toàn vẹn và xác thực của thông tin thanh toán (PI) và thông tin đơn hàng (OI). Chữ ký kép có vai trò gì trong việc bảo vệ tính toàn vẹn và xác thực của giao dịch? Việc thiếu chữ ký kép có ảnh hưởng gì đến độ tin cậy của giao dịch?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên a ,b thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = P/b \* a

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 9**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(K,M) || H(M) || E(PUB, K)

**Câu 2:**

Mã hóa đối xứng và mã hóa bất đối xứng có gì giống và khác nhau? Kỹ thuật triển khai và sử dụng chúng khác nhau như thế nào? Trong mã hoá đối xứng trọng tài có thể thấy và không thấy nội dung thông điệp trong các tình huống nào và nên ưu tiên sử dụng từng loại mã hóa này như thế nào?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên a ,b thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = a – P/b

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 10**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(PUB, M) || E(PRa, H(M))

**Câu 2:**

Loại hàm toán học nào thường được sử dụng trong mã hoá đối xứng? Đặc điểm cơ bản của chúng là gì? Hãy lấy ví dụ một hàm như vậy và giải thích cách hoạt động của nó.

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên a ,b thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = b – P/a

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 11**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(PUB, [M || E(PRA, C(K,M))])

**Câu 2:**

Loại hàm toán học nào thường được sử dụng trong mã hoá bất đối xứng? Đặc điểm cơ bản của chúng là gì? Hãy lấy ví dụ một hàm như vậy và giải thích cách hoạt động của nó.

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên a ,b thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = P – b/a

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**Đề 12**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(K1, [M || E(PRA, C(K2, M))])

**Câu 2:**

Hàm MAC và hàm hash có điểm tương đồng và khác nhau như thế nào? Làm thế nào để triển khai và sử dụng chúng trong các ứng dụng bảo mật khác nhau?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên a ,b thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = P – (b\*a)

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 13**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(K1,M) || E(PRA, C(K2,M))

**Câu 2:**

Giao dịch điện tử và giao dịch truyền thống khác nhau như thế nào? Các yếu tố nào làm nên tính bảo mật và tính xác thực của giao dịch điện tử?Nêu các thành phần và các bước trong giao dịch điện tử

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên x ,y thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = P – (x\*y)

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 14**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ A đến B, rồi giải thích tác dụng của sơ đồ đó:

E(K, [M || H(M)]) || E(PUB,K)

**Câu 2:**

Dịch vụ chứng thực X.509 là gì và vai trò của nó trong môi trường bảo mật như thế nào? Các thành phần cơ bản của một chứng chỉ X.509 là gì và chúng hoạt động như thế nào để đảm bảo tính xác thực và bảo mật trong các hệ thống thông tin?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên x ,y thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = (x \* y ) / P

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình

**ĐỀ 15**

**Câu 1:**

Cho công thức mô tả dữ liệu trên đường truyền , hãy vẽ sơ đồ quá trình truyền và nhận dữ liệu từ X đến Y với mã hoá đối xứng trọng tài thấy nội dung thông điệp, rồi giải thích tác dụng của sơ đồ đó:

(1) X 🡪A: ID*X*|| *M*||E(*Kxa*, [*IDX*||H(*M*)])

(2) A 🡪Y: E(*Kay*, [ID*X*||*M*||E(*Kxa*, [*IDX*||H(*M*)])||*T*])

**Câu 2:**

Các kỹ thuật lấy mật khẩu (password cracking) là gì và các phương pháp phổ biến như thế nào? Các biện pháp bảo mật nào có thể được áp dụng để ngăn chặn các cuộc tấn công này và cải thiện tính an toàn của hệ thống thông tin?

**Câu 3:**

Lập trình một chuỗi kí tự plaintext từ bàn phím( các kí tự trong khoảng từ A đến Z ). Nhập 2 số nguyên x ,y thuộc Z26 từ bàn phím. Mã hóa chuỗi ban đầu theo công thức:

C = (x \* y ) / P + (x – y)

Trong đó P là kí tự bản rõ, C là kí tự mã hóa, các phép tính được thực hiện trong Z26. Hiện chuỗi sau khi mã hóa ra màn hình. Hiện chuỗi sau khi giải mã ra màn hình