# CÂU HỎI ÔN TẬP & BÀI TẬP

1 . Hệ mật DES sử dụng khối khoá được tạo bởi :

a. 56 bit ngẫu nhiên

b. 64 bit ngẫu nhiên

c. 128 bit ngẫu nhiên

d. 56 bit ngẫu nhiên và 8 bit kiểm tra "Parity"

2 . Hệ mật DES xử lý từng khối " plain text " có độ dài :

a. 56 bit

b. 32 bit

c. 64 bit

d. 48 bit

3 . Thuật giải SHA là :

a. Hàm băm một chiều

b. Dùng trong thuật giải tạo chữ ký số

c. Cho giá trị băm 160 bit

d. Tất cả đều đúng

4 . DSA là thuật giải :

a. Lấy dấu tay "PrintingFinger"

b. Tạo chữ ký số (DS)

c. Phân phối khoá trước

d. Bảo mật thông điệp

5 . Thuật giải MD5 cho ta một giá trị băm có độ dài :

a. 156 bit

b. 128 bit

c. 256 bit

d. 512 bit

6 . Trong các cặp khoá sau đây của hệ mật RSA với p=5 ; q=7 , cặp khóa nào có khả năng đúng nhất :

a. (e = 12 , d =11)

b. (e = 4 , d =11)

c. ( e = 7 , d =23)

d. ( e = 3 , d =18)

d. 512 bit

7 . Cho k = 7, N = 26, mã hóa văn bản P = GOOD TIME dùng thuật mã Caesar

8 . Cho k = 15, n = 26, mã hóa văn bản P= HELLO MY FRIEND dùng thuật mã Caesar

9 . Cho k = 6, n = 26, giải mã văn bản C = ORUBKEUA dùng thuật mã Caesar

10 . Cho k = 18, n = 26, giải mã văn bản C = SFZQWMWE dùng thuật mã Caesar

11 . Cho k = KEY, N = 22, mã hóa văn bản dùng thuật mã Vigenere
P = KHOACONGNGHETHONGTIN

12 . Cho k = KEY, N = 26, mã hóa văn bản dùng thuật mã Vigenere
P = TRUONG DAI HOC MO

13 . Cho k = KEY, N = 26, mã hóa văn bản dùng thuật mã Vigenere
P = TRUONG DAI HOC MO

14 . Cho k = KEY, N = 26, giải mã văn bản dùng thuật mã Vigenere :
P = ULM KGM XKL QLC DLM XKR SR

15 . Cho k = MONARCHY, mã hóa văn bản P = TRUONG DAI HOC MO dùng thuật mã Playfair

16 .Cho k = MONARCHY, mã hóa văn bản P = ANTOANBAOMATTHONGTIN dùng Playfair

17 .Cho k = KEY, giải mã văn bản C= ZO BA TC ZI SN dùng Playfair

18 Cho k = KEY, giải mã văn bản C= IK QB dùng Playfair

19 . Cho a = 5, b = 3: y = 5x + 3 (mod 26).
Mã hoá bản rõ : DAIHOCMO dùng thuật mã Affine ?

20 .Cho bản rõ “TK” khóa k= (23,7). Tìm bản mã, dùng thuật mã Affine ?

21 .Cho bản rõ “EXIT” khóa k= (7,3). Tìm bản mã, dùng thuật mã Affine ?

22 .Cho bản mã “IZB” khóa k= (19, 3). Tìm bản rõ, dùng thuật mã Affine ?

23 .Cho bản mã “HUAXTGO ” khóa k= (5, 6). Tìm bản rõ, dùng thuật mã Affine ?

24 .Cho bản rõ “so” khóa k là:

7 2

3 3

Hãy mã hóa bản rõ với khóa k theo hệ mã Hill. Biết hàm mã y=xk (Đáp án : MA, thử lại TH: y=kx)

25 . Cho bản rõ “lo” khóa k là:

8 11

1 2

Hãy mã hóa bản rõ với khóa k theo hệ mã Hill. Biết hàm mã y=kx(Đáp án: IN, thử lại TH: y=xk)

26 . Cho bản mã “KS” khóa k là ma trận cấp 2 sau:

3 4

1 3

Hãy giải mã bản mã với khóa k theo hệ mã Hill tìm bản rõ nào . Biết hàm mã hóa y=kx

27 .Với M= 88, n= 187, e = 7, d = 23

Dùng thuật mã RSA hãy minh họa mã hóa & giải mã bản rõ M

28 .Cho A,B chọn 2 số nguyên tố chung là g = 10 , p = 541, với a=5, b=7 . Tính khóa công khai, khóa riêng của người gửi và người nhận A,B với thuật mã Diffie-Hellman.

29 .Cho A,B chọn 2 số nguyên tố chung là g=2 , p = 997, a=11, b= 13. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B Diffie-Hellman.

30 . Cho A,B chọn 2 số nguyên tố chung là g=2 , p = 23, a=5, b= 13. Tính khóa công khai, khóa riêng của người gửi và người nhận A, B Diffie-Hellman.