Đề thi giữa kì I mật mã & an ninh mạng 2010 (time: 30', khong tai lieu)

1) Cơ chế nào không sử dụng cho việc chống lại từ chối dịch vụ (Deny of Service)
a. Mã hóa
b. Quản lý định tuyến (routing control)
c. Trao đổi xác thực
d. Quản lý truy cập (access control)

2) Cơ chế nào không sử dụng cho xác thực
a. Mã hóa
c. Chữ kí số
b. Trao đổi xác thực
d. Quản lý truy cập

3) Tấn công Deny of Service (DOS) thuộc loại nào sau đây
a. Remote control
c. Active control
b. Passive control
d. Tất cả đều sai

4) Mã hóa thay thế một kí tự bằng một kí tự khác thuộc loại nào
a. Transposition
c. Polyanlphabetic substitution
b. Monoalphabetic substitution
d. Tất cả đều sai

Xét hàm affine cipher sau $y = k_1x + k_2 \pmod{256}$ với $x \in [0, 255]$, $0 \leq k_1, k_2 \leq 255$, x, k_1, k_2 là số nguyên. Một yêu cầu đối với hàm mã hóa là ánh xạ một một.

5) Với giá trị nào của k_1 thì khóa (k_1, k_2) hợp lệ
a. 2
c. 14
b. 8
d. Tất cả đều sai

6) Có tất cả bao nhiêu khóa hợp lệ:
a. 128
c. 32768
b. 256
d. 65536

7) Tính số dư khi chia 7^{2010} cho 13

8) Tính output bit thứ 1 và 16 của vòng thứ nhất của DES decryption. Giả sử ciphertext và key gồm toàn bit 1.
a. 0, 0
c. 0, 1
b. 1, 0
d. 1, 1

9) Chọn phát biểu sai về DES → key 64 bit

10) Tính ϕ (440)

11) Tìm phần dư 3^{2086} mod 440

12) Trong mã hóa công khai, khóa nào được sử dụng để tạo chữ kí số

13) Trong mã hóa công khai, khóa nào được sử dụng khi mã hóa data trước khi gửi.

Trao đổi key Diffie-Hellman, cho q = 71, a = 7

14) Nếu A có khóa riêng là $X_A = 5$, khóa công khai của A (Y_A) là

15) Nếu B có private key $X_B = 12$, public key của B (Y_B) là

16) Nếu A, B có khóa riêng lần lượt là 5 và 12 thì khóa bí mật dùng chung là

Mã hóa RSA, p = 3, q = 11, e = 7, C = 5

17) d = ?

18) M = ?

19) Các hướng tiếp cận xác thực thông điệp
a. Mã hóa
d. b, c đúng
b. Hash function
e. a, b, c đều đúng
c. Mã xác thực thông điệp

20) Cần thay đổi bao nhiêu chỗ trong 1 văn bản cho trước (nhằm tạo ra các phiên bản) sao cho xác suất tồn tại 2 phiên bản có giá trị hash như nhau là 0.5 nếu hash có chiều dài 128 bit
a. 128
c. 2^{128}
b. 64
d. 2^{64}