CÂU HỎI VÀ BÀI TẬP CHƯƠNG II
Môn: MẬT MÃ VÀ AN NINH MẠNG
-o0o-

I. Câu hỏi
1. Hai hàm cơ bản của mô hình mã hóa là gì?
2. Các thành phần thiết yếu của mô hình mã hóa đối xứng là gì?
3. Bao nhiêu khóa là cần thiết để hai bên giao tiếp với nhau dùng mã hóa đối xứng?
4. Khác biệt giữa mã hóa khối và mã hóa dòng là gì?
5. Mã hóa hoán vị là gì?
6. Mã hóa nhân là gì?
7. Hay cho biết chiều dài khối và khóa sử dụng với DES.
8. Mục đích của các S-box trong DES là gì?
9. Bao nhiêu khóa được dùng với 3DES?
10. Có bao nhiêu chế độ hoạt động cho DES?

II. Câu hỏi trắc nghiệm
1. Hệ mã Cesar mã hóa x∈[0; 25] thành y = x + 3 mod 26. Hãy cho biết nếu giá trị bản rõ là 10 thì giá trị bản mã tương ứng là:

a. 5 b. 7 c. 13 d. 15

2. Hệ mã Affine mã hóa x∈[0; 25] thành y = 3x + 5 mod 26. Hãy cho biết nếu giá trị bản mã là 10 thì giá trị bản rõ tương ứng là:

a. 9 b. 14 c. 19 d. 23

3. Đối với mã hóa DES, trong các phát biểu sau phát biểu nào là sai?

a. DES sử dụng khóa có chiều dài 64 bits.
b. Dữ liệu được mã hóa trong các khối có chiều dài 64 bits.
c. S-box là một hàm thay thế không tuyến tính làm tăng độ phức tạp của phép biến đổi.
d. DES dùng bộ tạo khóa để tạo ra các khóa con dùng cho mỗi vòng và chúng có chiều dài là 48 bits.

4. Hệ mã Double DES(2DES) không an toàn do tấn công gì?

a. Tấn công "man in the midle" c. Tấn công brute force
b. Tấn công "meet in the midle" d. Tấn công DOS

5. Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt?

a. ECB b. CBC c. CFB d. OFB

III. Bài tập
1. Một affine cipher mã hóa $x \in [0; 255]$ thành $y = k_1x + k_2 \bmod 256$. Một khóa (k_1, k_2) với $0 \le k_1; k_2 \le 255$ được gọi là hợp lệ nếu hàm $y = k_1x + k_2 \bmod 256$ là một ánh xạ một một. Hãy cho biết các giá trị k_1, k_2 hợp lệ và số lượng khóa (k_1, k_2) hợp lệ.
2. Xem xét thay thế được định nghĩa trong dòng đầu tiên của S-box $\mathbf{S_1}$ trong bảng 3.3([1]). Hãy cho biết sơ đồ khối tương tự như hình 3.1([1]) mà tương ứng với thay thế này.
3. Tính toán giá trị các bit 1, 16, 33, 48 của đầu ra ở vòng thứ nhất của hàm giải mã DES. Giả sử khối mã hóa (ciphertext) và khóa (key) tất cả đều là các bit 1.
4. Điền vào phần còn lại của bảng sau:

Mode	Encrypt	Decrypt
ECB	$C_j = E(K, P_j)\ j = 1,\ldots,N$	$P_j = D(K, C_j)\ j = 1,\ldots, N$
CBC	$C_1 = E(K, [P_1 \oplus IV])$ $C_j = E(K, [P_j \oplus C_{j-1}])\ j = 2,\ldots, N$	$P_1 = D(K, C_1) \oplus IV$ $P_j = D(K, C_j) \oplus C_{j-1}\ j = 2,\ldots, N$
CFB		
OFB		
CTR		