CÂU HỎI ÔN TẬP
Môn học: AN TOÀN THÔNG TIN

Chương 1 và Chương 2:

1. Trình bày các đặc điểm chính của thông tin

2. Tại sao cần phải đảm bảo an toàn cho thông tin và hệ thống thông tin?

3. Mục đích bảo vệ thông tin trong hệ thống thông tin?

4. An ninh thông tin là gì? Nêu vai trò của An ninh thông tin?

5. Trong các kiểu tấn công mạng, hãy cho biết khái niệm DoS, DDoS ? Phân biệt sự khác nhau cơ bản của DoS và DDoS?

6. Kỹ thuật tấn công kiểu Sniffing là gì? Hãy mô tả sơ lược về kỹ thuật tấn công này.

7. Kỹ thuật tấn công kiểu Ransomware là gì? Hãy mô tả sơ lược về kỹ thuật tấn công này.

8. Vai trò của mã hóa trong an toàn thông tin?

Chương 3:

9. Áp dụng phương pháp mã hóa đổi chỗ (hoán vị):

- Cho *Plaintext* là **HAIPHONG**, ngắt đoạn từng nhóm 4 ký tự; thứ tự tự nhiên trong mỗi nhóm là **1234**;
- Khóa mã nhóm 1 là **2413** và khóa mã nhóm 2 là **3142**.
- Hãy xác định *Ciphertext*?

10. Cho bản rõ (*Plaintext*): "**DAIHOCNGUYENTATTHANH**"

a. Dùng phương pháp ma trận (5 cột) để chuyển vị "hàng thành cột" cho Plaintext trên.

b. Sử dụng mật mã *Ceasar* để mã hóa chuỗi đã chuyển vị ở phần trên với K=1

Cho biết bảng chữ cái:

(*Các bài khác tương tự trên, thay đổi* ***Plaintext*** *và/hoặc thay* ***K***).

Chương 4:

11. Vẽ sơ đồ và trình bày những đặc điểm các giải thuật mã hóa khóa đối xứng.

12. Cho *Plantext* "**NTTU**" (biểu diễn theo ASCII: **01001110 01010100 01010100 01010101**).

Sử dụng khóa là "**CNTT**" (**01000011 01001110 01010100 01010100**). Hãy xác định

Ciphertext theo phương pháp XOR ?

13. Cho *Plaintext* **P** gồm 32 bit: "**1100 0000 1010 1000 0001 1010 1000 0001**".

a. Sử dụng hệ mã dòng (*Stream Cipher*) để tạo bản mã **C** cho chuỗi *Plaintext* bằng thuật toán **XOR** với khóa **K** = 8 bits "**10101010**"

b. Hãy sử dụng khóa **K'** (8 bit bất kỳ và khác với khóa **K** trên) để giải mã cho bản mã **C** trên để tạo thành bản rõ **P'**.

c. So sánh **P'** và **P**.

(*Các bài khác tương tự trên, thay đổi* ***Plaintext*** *và/hoặc thay đổi khóa* ***K***).

14. Trình bày tiến trình mã hóa **Feitel**.

15. Trình bày tổng quát về chuẩn mã hóa **DES**.

16. Chuẩn mã hóa **3-DES**:

a. Viết công thức tổng quát của quy trình mã hóa thông điệp **M** theo chuẩn ***3-DES*** dùng 3 khóa **K1, K2, K3**.

b. Viết công thức tổng quát của quy trình giải mã thông điệp **C** theo chuẩn ***3-DES*** dùng 3 khóa **K1, K2, K3**.

17. Đặc điểm của giải thuật mã hóa khóa đối xứng **AES**

Chương 5:

18. Trình bày nguyên lý hoạt động của ***mã hóa khóa công khai*** (hay *khóa bất đối xứng*).

19. Trình bày quy trình sử dụng mã hóa khóa công khai nhằm đảm bảo tính bí mật (*Confidentiality*) cho thông tin truyền từ *Alice* sang *Bob*.

20. Trình bày quy trình sử dụng mã hóa khóa công khai nhằm đảm bảo cho *Bob* xác thực thông điệp nhận là từ *Alice*.

21. Áp dụng thuật toán bình phương liên tiếp để tính $\mathbf{7^{21} \bmod 13}$

22. Tính và chọn cặp khóa *Public key* và *Private key* bằng thuật toán **RSA** theo lựa chọn 2 số nguyên tố: **p = 3**, **q = 11**

Cho biết quy trình RSA như sau:

- Tính số n = p.q
- Tính $\varphi(n) = (p-1)(q-1)$
- Chọn e sao cho: $\gcd(e, \varphi(n))=1$

- Chọn d sao cho: e.d = 1 mod n

- Khóa công khai KU = (e, n).

- Khóa bí mật KR = (d, n).

(*Các bài khác tương tự trên, thay đổi cặp số nguyên tố* ***p, q*** *và/hoặc thay đổi* ***Plaintext***).

23. Áp dụng thuật giải RSA: giả sử:

- Có cặp khóa: *Public key* $\mathbf{K_U}$(e,n) = (**11,15**) và *Private key* $\mathbf{K_R}$(d,n) = (**3,15**).

- Cho bản rõ **M = 8**.

Hãy tính:

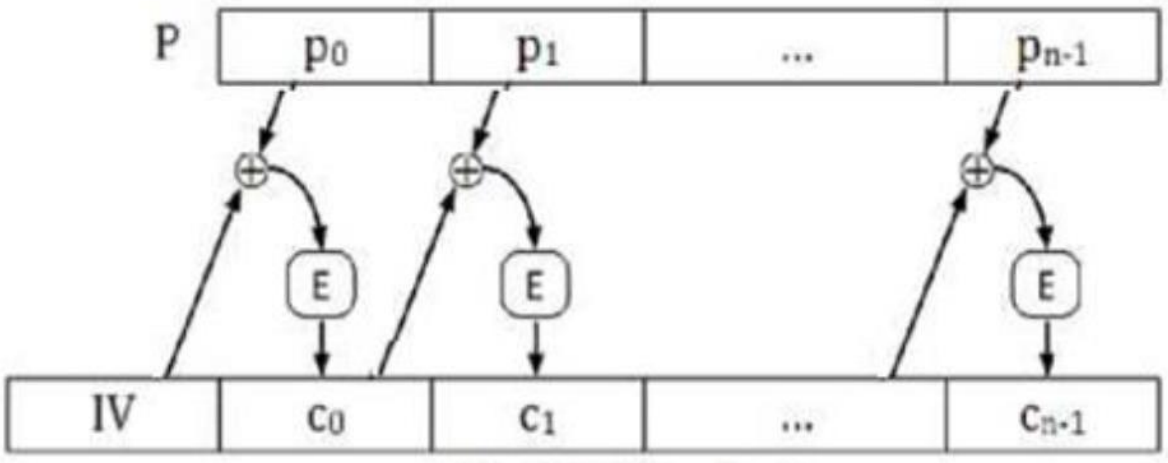
a. Mã hóa **M** bằng *Public Key* theo công thức: **C** = M^e mod n

b. Giải mã **C** bằng *Private Key* theo công thức: **M'** = C^d mod n

Chương 6:

24. Vẽ sơ đồ quy trình mã hóa của mô hình mật mã chuỗi khối CBC (Cipher Block Chaining)

25. Cho quy trình mã hóa của mô hình mật mã chuỗi khối CBC (*Cipher Block Chaining*) như ảnh bên dưới:



a. Hãy diễn đạt hoạt động của quy trình mã hóa CBC này.

b. Nếu có một khối P_I nào đó bị thay đổi nội dung thành Pi'. Hãy cho biết khối mã cuối cùng C'n-1 sẽ như thế nào khi so với Cn-1.

c. Giải thích vấn đề trên.

26. Cho *Message* **M** 32 bit: "**1100 0000 1010 1000 0001 1010 1000 0001**"

a. Dùng thuật toán **XOR** để băm (hash) **M** trên thành mã băm **8 bit**.

b. Giả sử: 4 bit đầu tiên để M đã bị sửa đổi thành **1001**. Tiến hành dùng **XOR** để băm bản sửa đổi (**M'**) thành mã băm **8 bit**.

c. Cho biết kết luận sau khi so sánh 2 mã băm của **M** và **M'**.

(*Các bài khác tương tự trên, thay đổi **M** và/hoặc thay đổi **số bit mã băm***).

27. Khái niệm chứng chỉ số là gì? Mô tả các thành phần chính trong chứng chỉ số ?

Chương 7 và 8:

28. Vai trò và tính chất của hàm băm trong việc xác định tính toàn vẹn của thông tin?

29. Cho biết khái niệm về **IDS** và **IPS**? So sánh giữa IDS và IPS?

30. Trong hệ thống hạ tầng mạng bảo mật, các hệ thống IDS/IPS thường đặt ở đâu trong trong hệ thống mạng? Giải thích lý do.

31. Trình bày các loại tường lửa trong hệ thống mạng.