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

I. Câu hỏi

1. Cho biết các hướng tiếp cận nhằm cung cấp khả năng xác thực thông điệp. MAC + hash
2. Khác biệt giữa mã xác thực thông điệp(MAC) và hàm băm một chiều là gì? secret key
3. Mã xác thực thông điệp dựa trên hàm băm được gọi là gì? CMAC
4. Cho biết các đặc tính mà chữ ký số phải có.
5. Cho biết ưu điểm của lược đồ chữ ký số với DSA so với lược đồ chữ ký số với RSA.

II. Câu hỏi trắc nghiệm

1. DAA(Data Authentication Algorithm) tạo ra mã xác thực thông điệp có kích thước là: DES

a. 128 bits
b. 64 bits
c. 128 bytes
d. 64 bytes

2. Cho một hàm băm với kết quả băm có chiều dài là 128 bits. Hãy cho biết cần sửa đổi ít nhất bao nhiêu chỗ trong văn bản P sao cho xác xuất để có hai văn bản P_1 và P_2 mà giá trị băm của chúng bằng nhau là 0.5 tấn công ngày sn

a. 128
b. 64
c. 2^{64}
d. 2^{128}

3. Mã xác thực thông điệp dựa trên hàm băm MD5 tạo ra mã xác thực thông điệp có kích thước là :

a. 128 bits
b. 64 bits
c. 128 bytes
d. 64 bytes

4. Chữ ký số là một cơ chế xác thực nhằm:

a. Xác minh tính toàn vẹn của thông điệp.
b. Xác nhận danh tính của người tạo ra thông điệp.
c. Chống thoái thác về xuất xứ
d. Cả ba câu trên đều đúng

5. Cho biết phát biểu sai khi nói về các lược đồ tạo chữ ký số:

a. Lược đồ DSA tạo chữ ký có chiều dài 512 bits. = 2 * SHA
b. Lược đồ DSA tạo và xác minh chữ ký nhanh hơn so với lược đồ RSA.
c. Lược đồ RSA tạo chữ ký có chiều dài lớn hơn so với lược đồ DSA.
d. DSA không thể dùng cho các vấn đề mã hóa dữ liệu và trao đổi khóa.

6. Dịch vụ xác thực X.509 dùng mã hóa dạng gì?

a. Mã hóa đối xứng
b. Mã hóa khóa bí mật
c. Mã hóa khóa công khai
d. Cả câu (b) và (c)

7. Chữ ký số trong chứng chỉ X.509 được tạo dùng khóa nào sau đây :

a. Khóa công khai của người sở hữu chứng chỉ.
b. Khóa riêng của người sở hữu chứng chỉ.
c. Khóa công khai của đơn vị phát hành chứng chỉ.
d. Khóa riêng của đơn vị phát hành chứng chỉ.

III. Bài tập

1. Xem xét một hàm băm. Thông điệp M là một chuỗi các số thập phân M = (a_1, a_2,..., a_i). Giá tri băm h được tính toán là $\left(\sum_{i=1}^{t} a_i\right) \bmod n$ với giá trị n được ấn định trước.

a. Hàm băm này có thỏa mãn các yêu cầu của hàm băm được liệt kê trong mục 11.4 ([1]). Giải thích câu trả lời.

$$h = \left(\sum_{i=1}^{t} (a_i)^2\right) \bmod n$$

b. Tương tự như câu (a) cho hàm băm:

c. Tính toán giá trị băm của hàm băm câu (b) cho M = (189, 632, 900, 722, 349) và n = 989.

2. Vấn đề gì xảy ra nếu giá trị k (được tạo ngẫu nhiên) dùng để tạo chữ ký trong DSA bị thỏa hiệp. Hãy giải thích vì sao.

Tạo chữ ký số giả mạo