Đề số 1 – Lần 2

ĐỀ THI KẾT THÚC HỌC PHẦN **AN TOÀN – AN NINH MẠNG** *Thời gian làm bài : 90 phút – Đề thi có 2 trang* *Được phép sử dụng tài liệu – Không trao đổi bài*	**Họ tên :** **Lớp :** **Số thứ tự :** **Số tờ :**

I. PHẦN TRẮC NGHIỆM *(3 điểm – Làm trực tiếp trên đề thi)*

Sinh viên khoanh tròn vào tất cả các câu trả lời đúng.

1. Mã Ceasar thực hiện bằng những phép biến đổi nào ?
   a) Phép thế b) Phép hoán vị c) Gama xoring

2. Thuật toán nào sau đây không phải là đối xứng ?
   a) DES b) El-Gamal c) RC5 d) IDEA

3. Khóa mật trong hệ mã hoá DES có độ dài là bao nhiêu ?
   a) 48 bit b) 64 bit c) 128 bit d) 192 bit e) 256 bit

4. Thành phần nào của cơ sở hạ tầng của khóa công khai (PKI – Public Key Infrastructure) chịu trách nhiệm việc tạo danh sách vủa các chứng chỉ được thu hồi?
   a) Trung tâm cấp phát chứng chỉ c) Người sử dụng cuối cùng
   b) Trung tâm đăng ký d) Cẩm nang tra cứu mạng

5. Thủ tục phân phối khóa không sử dụng kênh mật để truyền khóa đến người nhận là:
   a) Mã hóa theo thuật toán DES
   b) Sử dụng phương pháp mã hóa công khai
   c) Mã hóa Vizhiner

6. Lý thuyết hệ mật Shannon cho thấy:
   a) Khóa và thuật toán mật mã phải được an toàn
   b) Thông điệp và Khóa phải có quan hệ thống kê
   c) Khóa phải có độ dài lớn hơn hoặc bằng thông điệp
   d) Bản tin mật phải có quan hệ thốgn kê với bản tin rõ
   e) Khóa phải được sử dụng một lần

7. Thám mã là:
   a) Tập hợp các phương pháp và môi trường để thực hiện việc giải mã thông tin mà không cần có chìa khóa cần thiết
   b) Khôi phục thông tin ban đầu bằng khóa tương ứng
   c) Sửa lỗi.

8. Thuật toán RSA thuộc dạng nào của thuật mã hóa (xét trên phương diện độ bền vững khi bị bẻ khóa) ?
   a) An toàn không điều kiện b) An toàn theo tính toán

9. Cơ sở của độ an toàn của phương pháp RSA là :
   a) Tính lôgarít rời rạc trong trường hữu hạn
   b) Phép khai triển các số nguyên lớn thành các thừa số nguyên tố
   c) Tính nghiệm của phương trình đại số
   d) Tính nghiệm của hệ phương trình tuyến tính

10. Hàm băm một chiều là gì ?

a) Hàm băm, khó khăn trong việc tính toán theo hướng thuận và dễ dàng trong việc tính toán theo hướng ngược lại

b) Hàm băm, dễ dàng trong việc tính toán theo hướng thuận và hướng ngược lại

c) Hàm băm, là hàm tính không có tính thuận nghịch

11. Những thuật toán nào sau đây không sử dụng để tính toán mẫu thông điệp (Digest) ?

a) DES b) MD5 c) SHA-1 d) RSA

12. Đâu là điểm khác biệt của MAC so với hàm băm:

a) Thuật toán mã hoá đối xứng b) Thuật toán mã hóa không đối xứng

c) Khóa mật mã d) Phương pháp biểu diễn hàm

II. PHẦN TỰ LUẬN *(7 điểm)*

Câu 1. Sử dụng phương pháp mã hóa Hill với khóa K = $\begin{bmatrix} 3 & 2 \\ 4 & 1 \end{bmatrix}$ để mã thông điệp "Have a good time"

Câu 2. Để vừa đảm bảo tính xác thực, vừa đảm bảo tính riêng tư cho thông điệp, có thể kết hợp xác thực thông điệp với các phương pháp mã mật. Có hai cơ chế thực hiện:

a. Xác thực thông điệp trước rồi mã hóa và
b. Mã hóa thông điệp rồi xác thực.

Hãy phân tích những đặc điểm của hai sơ đồ trên.

Câu 3. Trong sơ đồ cấp phát chứng chỉ, CA (Certificate Authority) gửi thông tin $E_{KRCA}(K_{Ua}| ID_A| Time_1)$ cho bên A. Giải thích tính chất những thông tin nhận được. Trước đó, bên A gửi yêu cầu gì cho CA. Bên A sẽ sử dụng thông tin nhận được như thế nào ?

Câu 4. Cho ma trận xác thực sau :

K \ X	0	1
0	0	2
1	1	3
2	0	3
3	1	2

Với các xác suất :
P(X = 0) = P(X = 1) = 0.5;
P(K = 1) = P(K = 2) = P(K = 3) = P(K = 4) = 0.25

Tính các xác suất tấn công vào hệ xác thực trên. Từ đó đưa ra kết luận về tính xác thực của hệ.