Đề số 2 – Lần 1

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. Thuật toán mã hóa nào sau đây không phải là đối xứng ?
   a) Knapsack b) RC5 c) DES d) Đường cong Elliptic

2. Hãy chọn những đặc trưng của hàm băm H(x):
   a) Cho một mã *h*, việc tính *x* sao cho *H(x) = h* là khó
   b) Là hàm mã hoá đối xứng
   c) Dễ dàng trong tính toán *H(x)*
   d) Cho đầu ra là khối dữ liệu độ dài cố định
   e) Là mã hóa không đối xứng
   f) Sử dụng khóa mật
   g) Tác động lên thông điệp có độ dài bất kỳ
   h) Với một *x*, việc tìm *y* sao cho *H(x) = H(y)* là khó

3. Thuật toán nào sau đây là mã hóa dòng ?
   a) Knapsack b) RC4 c) RSA d) DES.

4. Các phương pháp Xác thực thông điệp để chống lại các loại tấn công nào ?
   a) Nghe trộm b) Giả mạo c) Phát lại thông điệp
   d) Từ chối dịch vụ e) Sửa đổi thông điệp f) Phân tích lưu lượng

5. Những dạng tấn công nào sau đây là tấn công thụ động ?
   a) Giả mạo b) Chặn giữ thông điệp c) Phân tích lưu lượng
   d) Phát lại thông điệp e) Nghe trộm f) Từ chối dịch vụ

6. Trong quản lý và phân phối khóa đối xứng, xác định những câu khẳng định đúng?
   a) Khóa phiên là khóa dùng để xác thực hai bên trao đổi thông tin.
   b) Khóa phiên thay đổi thường xuyên sau mỗi phiên làm việc
   c) Khóa chính dùng để mã hóa trao đổi khóa phiên
   d) Khóa phiên dùng để trao đổi khóa chính
   e) Khóa chính và khóa phiên là cặp khóa riêng và khóa công khai
   f) Khóa chính sẽ được thay đổi chậm hơn khóa phiên
   g) Khóa chính chỉ được dùng một lần

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

8. 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 thống kê với bản tin rõ
e) Khóa phải được sử dụng một lần

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

10. 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

11. Phương pháp xác thực bằng MAC sử dụng các thao tác nào:
a) Mã hóa và giải mã
b) Tính mã băm
c) Mã hóa
d) Giải mã

12. Trong các hệ mật sau, hệ nào không phải hệ mật khóa công khai ?
a) DES b) El-Gammal c) RC5 d) RSA

II. PHẦN TỰ LUẬN *(7 điểm)*

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

Câu 2. Trình bày vắn tắt các bước của quá trình trao đổi khóa Diffie-Hellman. Cho một ví dụ minh họa.

Câu 3. Phân tích các yếu tố trong sơ đồ phân phối khóa đối xứng tập trung (sử dụng KDC) có tác dụng chống lại các tấn công vào sơ đồ này.

Câu 4. Cho X, Y, K với các xác suất xuất hiện của xi, yi , ki :

X	0.25	0.25	0.125	0.0625	0.125	0.1875
Y	0.5	0.25	0.125	0.0625	0.03125	0.03125
K	0.125	0.0625	0.0625	0.125	0.25	0.375

1. Khảo sát tính mật của hệ.
2. Trường hợp nào thì độ an toàn của hệ mật là cao nhất có thể ?
3. Bản rõ : 80 kí tự; khóa 40 kí tự; mật: 100 kí tự. Hỏi đối phương cần thu nhận ít nhất bao nhiêu kí tự mã mật để có thể bẻ khóa?