

**Đề số 1 – 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.*

- Mã Hill thực hiện bằng những phép biến đổi nào ?  
☒ a) Phép thế                      b) Phép hoán vị                      c) Gama xoring
- Trong các hệ mật sau, hệ nào không phải hệ mật khóa công khai ?  
a) RSA                      ☒ b) RC5                      c) El-Gammal                      ☒ d) DES
- Những dạng tấn công nào sau đây là tấn công thụ động ?  
☒ a) Nghe trộm                      b) Chặn giữ thông điệp                      c) Phát lại thông điệp  
☒ d) Phân tích lưu lượng                      e) Giả mạo                      f) Từ chối dịch vụ
- Trong quản lý và phân phối khóa đối xứng, xác định những câu khẳng định đúng?  
a) Khóa chính chỉ được dùng một lần  
☒ b) Khóa phiên thay đổi thường xuyên sau mỗi phiên làm việc  
c) Khóa phiên dùng để trao đổi khóa chính  
d) Khóa chính và khóa phiên là cặp khóa riêng và khóa công khai  
☒ e) Khóa chính dùng để mã hóa trao đổi khóa phiên  
f) Khóa chính sẽ được thay đổi chậm hơn khóa phiên  
☒ g) Khóa phiên là khóa dùng để xác thực hai bên trao đổi thông tin.
- Thuật toán nào sau đây là mã hóa dòng ?  
a) Knapsack                      b) RC4                      c) RSA                      d) DES.
- 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
- 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
- Thuật toán mã hóa nào sau đây không phải là đối xứng ?  
a) DES                      ☒ b) Knapsack                      c) RC5                      ☒ d) Đường cong Elliptic
- 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. Các phương pháp Xác thực thông điệp để chống lại các loại tấn công nào ?  
 a) Nghe trộm ☐ b) Sửa đổi thông điệp ☐ c) Phát lại thông điệp ☐  
 d) Phân tích lưu lượng ☐ e) Giả mạo ☐ f) Từ chối dịch vụ ☐
11. 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 ☐
12. Hãy chọn những đặc trưng của hàm băm  $H(x)$ :  
 a) Là hàm mã hoá đối xứng ☐  
 b) Tác động lên thông điệp có độ dài bất kỳ ☐  
 c) Là mã hóa không đối xứng ☐  
 d) Cho đầu ra là khối dữ liệu độ dài cố định ☐  
 e) Cho một mã  $h$ , việc tính  $x$  sao cho  $H(x) = h$  là khó ☐  
 f) Sử dụng khóa mật ☐  
 g) Dễ dàng trong tính toán  $H(x)$  ☐  
 h) Với một  $x$ , việc tìm  $y$  sao cho  $H(x) = H(y)$  là khó ☐

## II. PHẦN TỰ LUẬN (7 điểm)

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

**Câu 2.** Trình bày vắn tắt các bước của thuật toán RSA. Cho một ví dụ minh họa.

**Câu 3.** Trong sơ đồ quản lý khóa công khai, Public Key Authority gửi lại thông tin:  $E_{K_{Rpa}}(K_{Ub}|Request|Time_1)$  cho bên yêu cầu A. Những thông tin này là gì, giải thích. Khi nhận được thì bên A sẽ làm gì ?

**Câu 4.** Cho X, Y, K với các xác suất xuất hiện của  $x_i, y_i, k_i$  :

X	0.5	0.25	0.125	0.0625	0.03125	0.03125
Y	0.25	0.25	0.125	0.0625	0.125	0.1875
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 : 40 kí tự; khóa 20 kí tự; mật: 50 kí tự. Hỏi đối phương cần thu nhận ít nhất bao nhiêu kí tự mã mật để có thể bẻ khóa?