# CÂU HỎI VÀ BÀI TẬP CHƯƠNG I
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi
1. Cho biết các nguyên tắc cốt lõi của an toàn thông tin
2. Hãy cho biết khác biệt giữa tấn công thụ động và tấn công chủ động
3. Liệt kê các loại tấn công thụ động, tấn công chủ động
4. Liệt kê và định nghĩa các cơ chế trong kiến trúc an ninh OSI
5. Liệt kê và định nghĩa các dịch vụ trong kiến trúc an ninh OSI

## II. Câu hỏi trắc nghiệm
**1. Hình thức tấn công thụ động chống lại nguyên tắc cốt lõi nào của an toàn thông tin?**
a. Bí mật
b. Toàn vẹn
c. Sẵn sàng
d. Xác thực

**2. Tấn công DOS (Denial of Service) thuộc loại tấn công nào trong kiến trúc an ninh OSI ?**
a. Tấn công từ xa (Remote Attack)
b. Tấn công chủ động (Active Attack)
c. Tấn công thụ động (Passive Attack)
d. Cả câu (a) và câu (b) đều đúng

**3. Cơ chế nào sau đây không cần thiết sử dụng để chống lại tấn công từ chối dịch vụ?**
a. Mã hóa dữ liệu (encipherment)
b. Quản lý định tuyến (routing control)
c. Trao đổi xác thực (authentication exchange)
d. Quản lý truy cập (access control)

**4. Cơ chế nào không sử dụng cho dịch vụ xác thực?**
a. Mã hóa dữ liệu (encipherment)
b. Chữ ký số (digital signature)
c. Trao đổi xác thực (authentication exchange)
d. Quản lý truy cập (access control)

**5. Cho biết Code Red thuộc vào loại mã độc nào sau đây:**
a. Virus
b. Trojan
c. Worm
d. Là một loại mã độc lai ghép

## III. Bài tập
1. Hãy xây dựng bảng tương tự như bảng 4.1([1]) mô tả mối quan hệ giữa các dịch vụ và các tấn công trong kiến trúc an ninh OSI
2. Hãy xây dựng bảng tương tự như bảng 4.1([1]) mô tả mối quan hệ giữa các cơ chế và các tấn công trong kiến trúc an ninh OSI

# CÂU HỎI VÀ BÀI TẬP CHƯƠNG II

## Môn: AN NINH MẠNG

-o0o-

## I. Câu hỏi

1. Hai hàm cơ bản của mô hình mã hóa là gì?
2. Các thành phần thiết yếu của mô hình mã hóa đối xứng là gì?
3. Bao nhiêu khóa là cần thiết để hai bên giao tiếp với nhau dùng mã hóa đối xứng?
4. Khác biệt giữa mã hóa khối và mã hóa dòng là gì?
5. Mã hóa hoán vị là gì?
6. Mã hóa nhân là gì?
7. Hay cho biết chiều dài khối và khóa sử dụng với DES.
8. Mục đích của các S-box trong DES là gì?
9. Bao nhiêu khóa được dùng với 3DES?
10. Có bao nhiêu chế độ hoạt động cho DES?

## II. Câu hỏi trắc nghiệm

**1. Hệ mã Cesar mã hóa $x \in [0; 25]$ thành $y = x + 3 \bmod 26$. Hãy cho biết nếu giá trị bản rõ là 10 thì giá trị bản mã tương ứng là:**

a. 5 b. 7 c. 13 d. 15

**2. Hệ mã Affine mã hóa $x \in [0; 25]$ thành $y = 3x + 5 \bmod 26$. Hãy cho biết nếu giá trị bản mã là 10 thì giá trị bản rõ tương ứng là:**

a. 9 b. 14 c. 19 d. 23

**3. Đối với mã hóa DES, trong các phát biểu sau phát biểu nào là sai?**

a. DES sử dụng khóa có chiều dài 64 bits.
b. Dữ liệu được mã hóa trong các khối có chiều dài 64 bits.
c. S-box là một hàm thay thế không tuyến tính làm tăng độ phức tạp của phép biến đổi.
d. DES dùng bộ tạo khóa để tạo ra các khóa con dùng cho mỗi vòng và chúng có chiều dài là 48 bits.

**4. Hệ mã Double DES(2DES) không an toàn do tấn công gì?**

a. Tấn công "man in the midle" c. Tấn công brute force
b. Tấn công "meet in the midle" d. Tấn công DOS

**5. Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt?**

a. ECB b. CBC c. CFB d. OFB

## III. Bài tập

1. Một affine cipher mã hóa $x \in [0; 255]$ thành $y = k_1x + k_2 \bmod 256$. Một khóa $(k_1, k_2)$ với $0 \leq k_1; k_2 \leq 255$ được gọi là hợp lệ nếu hàm $y = k_1x + k_2 \bmod 256$ là một ánh xạ một một. Hãy cho biết các giá trị $k_1$, $k_2$ hợp lệ và số lượng khóa $(k_1, k_2)$ hợp lệ.
2. Xem xét thay thế được định nghĩa trong dòng đầu tiên của S-box $\mathbf{S_1}$ trong bảng 3.3([1]). Hãy cho biết sơ đồ khối tương tự như hình 3.1([1]) mà tương ứng với thay thế này.
3. Tính toán giá trị các bit 1, 16, 33, 48 của đầu ra ở vòng thứ nhất của hàm giải mã DES. Giả sử khối mã hóa (ciphertext) và khóa (key) tất cả đều là các bit 1.
4. Điền vào phần còn lại của bảng sau:

| Mode | Encrypt | Decrypt |
|---|---|---|
| ECB | $C_j = E(K, P_j)\ j = 1,\ldots,N$ | $P_j = D(K, C_j)\ j = 1,\ldots, N$ |
| CBC | $C_1 = E(K, [P_1 \oplus IV])$<br><br>$C_j = E(K, [P_j \oplus C_{j-1}])\ j = 2,\ldots, N$ | $P_1 = D(K, C_1) \oplus IV$<br><br>$P_j = D(K, C_j) \oplus C_{j-1}\ j = 2,\ldots, N$ |
| CFB | | |
| OFB | | |
| CTR | | |

# CÂU HỎI VÀ BÀI TẬP CHƯƠNG III

**Môn: AN NINH MẠNG**

-o0o-

## I. Câu hỏi

1. b là ước số của a có nghĩa là gì?
2. Số nguyên tố là gì?
3. Hàm phi Euler là gì?
4. Căn nguyên thủy của một số là gì?
5. Các yếu tố chủ yếu của một hệ mã khóa công khai là gì?
6. Bao nhiêu khóa là cần thiết để hai bên giao tiếp với nhau dùng mã hóa khóa công khai?
7. Hãy cho biết vai trò của khóa công khai và khóa riêng.
8. Trình bày ba loại ứng dụng của mã hóa khóa công khai.
9. Mô tả chung chung một thủ tục hiệu quả để chọn một số nguyên tố.
10. Mô tả ngắn gọn lược đồ trao đổi khóa Diffie-Hellman.

| $\phi(n)$ | +0 | +1 | +2 | +3 | +4 | +5 | +6 | +7 | +8 | +9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0+ | | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 |
| 10+ | 4 | 10 | 4 | 12 | 6 | 8 | 8 | 16 | 6 | 18 |
| 20+ | 8 | 12 | 10 | 22 | 8 | 20 | 12 | 18 | 12 | 28 |
| 30+ | 8 | 30 | 16 | 20 | 16 | 24 | 12 | 36 | 18 | 24 |
| 40+ | 16 | 40 | 12 | 42 | 20 | 24 | 22 | 46 | 16 | 42 |
| 50+ | 20 | 32 | 24 | 52 | 18 | 40 | 24 | 36 | 28 | 58 |
| 60+ | 16 | 60 | 30 | 36 | 32 | 48 | 20 | 66 | 32 | 44 |
| 70+ | 24 | 70 | 24 | 72 | 36 | 40 | 36 | 60 | 24 | 78 |
| 80+ | 32 | 54 | 40 | 82 | 24 | 64 | 42 | 56 | 40 | 88 |
| 90+ | 24 | 72 | 44 | 60 | 46 | 72 | 32 | 96 | 42 | 60 |

## II. Câu hỏi trắc nghiệm

**1. Hãy cho biết kết quả của ($7^{2010}$ mod 13):**

a. 1
b. 12
c. 7
d. Các giá trị trên đều sai

**2. Cho biết giá trị hàm phi Euler ϕ(440) là:**

a. 439
b. 240
c. 160
d. Tất cả các câu trên đều sai

**3. Hãy cho biết kết quả của ($3^{2086}$ mod 440):**

a. 1 b. 3 c. 81 d. 289

**4. Đối với mã hóa khóa công khai, khóa nào được sử dụng để tạo chữ ký số trên một thông điệp:**

a. Khóa công khai của người nhận
b. Khóa riêng của người nhận
c. Khóa công khai của người gửi
d. Khóa riêng của người gửi

**5. Đối với mã hóa khóa công khai, khóa nào được sử dụng để mã hóa một thông điệp:**

a. Khóa công khai của người nhận
b. Khóa riêng của người nhận
c. Khóa công khai của người gửi
d. Khóa riêng của người gửi

**(Dữ liệu dùng cho câu 6 và 7)**
**Thực hiện mã hóa và giải mã với thuật toán RSA và p = 3; q = 11, e = 7; bản mã C = 5**

**6. Giá trị của d là:**

a. 7 b. 5 c. 3 d. 2

**7. Giá trị của bản rõ M tương ứng là:**

a. 26 b. 24 c. 5 d. 1

**(Dữ liệu dùng cho câu 10, 11, 12)**

**A và B dùng kỹ thuật trao đổi khóa Diffie-Hellman với q = 71 và $\alpha$ = 7.**

**8. Nếu A có khóa riêng $X_A$ = 5, hãy cho biết khóa công khai của A ($Y_A$)?**

a. 4 b. 5 c. 30 d. 51

**9. Nếu B có khóa riêng $X_B$ = 12, hãy cho biết khóa công khai của B ($Y_B$)?**

a. 4 b. 5 c. 30 d. 51

**10. Nếu A có khóa riêng $X_A$ = 5 và B có khóa riêng $X_B$ = 12, hãy cho biết khóa bí mật dùng chung giữa A và B($K_{AB}$)?**

a. 4
b. 5
c. 30
d. 51

## III. Bài tập

1. **Tìm các số nguyên dương x nhỏ nhất mà:**
   a. $5x \equiv 4 \pmod 3$
   b. $7x \equiv 6 \pmod 3$
   c. $9x \equiv 8 \pmod 3$

2. **Dùng thuật toán Euclid mở rộng tính nghịch đảo nhân của:**
   a. 1234 mod 4321
   b. 24140 mod 40902
   c. 550 mod 1769

3. **Dùng định lý Fermat tính $3^{201}$ mod 11.**

4. **Dùng định lý Euler tính $7^{1000}$ mod 10.**

5. **Tính các hàm phi Euler sau:**
   a. $\phi(41)$
   b. $\phi(27)$
   c. $\phi(231)$
   d. $\phi(440)$

6. **Dùng mã hóa RSA, cho biết bản mã C trong các trường hợp sau:**
   a. p = 3; q = 11, e = 7; M = 5
   b. p = 5; q = 11, e = 3; M = 9
   c. p = 7; q = 11, e = 17; M = 8
   d. p = 11; q = 13, e = 11; M = 7
   e. p = 17; q = 31, e = 7; M = 2.

7. **Với hệ mã khóa công khai RSA, bạn lấy được bản mã C = 10 gởi đến một người có khóa công khai (e,n) = (5, 35). Bản rõ M là gì ?**

8. **Xem xét lược đồ trao đổi khóa Diffie-Hellman với số nguyên tố q = 11 và $\alpha = 2$.**
   a. Chứng minh 2 là một căn nguyên thủy của 11.
   b. Nếu A có khóa công khai là $Y_A = 9$. Hãy cho biết khóa riêng của A($X_A$)?
   c. Nếu B có khóa công khai là $Y_B = 3$. Hãy tính toán khóa bí mật dùng chung giữa A và B($K_{AB}$)?

# CÂU HỎI VÀ BÀI TẬP CHƯƠNG IV

**Môn: AN NINH MẠNG**

-o0o-

## I. Câu hỏi

1. Cho biết các hướng tiếp cận nhằm cung cấp khả năng xác thực thông điệp.
2. Khác biệt giữa mã xác thực thông điệp(MAC) và hàm băm một chiều là gì?
3. Mã xác thực thông điệp dựa trên hàm băm được gọi là gì?
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:**
   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**
   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.
   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.

## 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.
   b. Tương tự như câu (a) cho hàm băm: $h = \left(\sum_{i=1}^{t} (a_i)^2\right) \bmod n$
   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.**

# CÂU HỎI CHƯƠNG V
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi

1. Kerberos xem xét và giải quyết vấn đề gì?
2. Bốn yêu cầu của Kerberos là gì ? Giải thích chi tiết.
3. Cho biết khác biệt giữa Kerberos version 4 và Kerberos version 5.
4. Mục đích của chuẩn X.509 là gì?
5. Chứng chỉ X.509 bị thu hồi như thế nào?

## II. Câu hỏi trắc nghiệm

**1. Một môi trường Kerberos đầy đủ dịch vụ bao gồm:**
   a. Một máy chủ Kerberos
   b. Một máy chủ Kerberos và một số máy trạm
   c. Một máy chủ Kerberos và một số máy chủ ứng dụng
   d. Một máy chủ Kerberos, một số máy trạm, một số máy chủ ứng dụng

**2. Đối với Kerberos, mỗi người dùng có:**
   a. Một vé TGT và một vé SGT cho tất cả các dịch vụ mà người dùng truy cập đến
   b. Một vé TGT và mỗi vé SGT cho mỗi dịch vụ mà người dùng truy cập đến
   c. Một vé SGT và mỗi vé TGT cho mỗi dịch vụ mà người dùng truy cập đến
   d. Mỗi vé SGT và mỗi vé TGT cho mỗi dịch vụ mà người dùng truy cập đến

**3. 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)

**4. 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.

**5. Thủ tục xác thực nào được dùng để dùng cho các kết nối có tương tác ?**
   a. Xác thực một chiều.
   b. Xác thực hai chiều.
   c. Xác thực ba chiều.
   d. Cả câu (b) và (c) đều đúng.

# CÂU HỎI CHƯƠNG VI
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi
1. Các dịch vụ được PGP cung cấp là gì?
2. Vì sao PGP tạo chữ ký trước khi thực hiện nén dữ liệu?
3. Cho biết thuật toán Radix-64 làm gì?
4. RFC 822 là gì?
5. S/MIME là gì?

## II. Câu hỏi trắc nghiệm
**1. Chọn phát biểu sai trong các phát biểu sau khi PGP được sử dụng trong một hệ thống E-mail:**
a. Hệ thống E-mail nói trên sẽ cung cấp các dịch vụ xác thực, bí mật, nén, tương thích e-mail và phân mảnh.
b. Nếu dùng dịch vụ bí mật thì thông điệp gởi đi sẽ có mã hóa ở một số khối dữ liệu.
c. Nếu chỉ dùng dịch vụ xác thực thì thông điệp gởi đi sẽ không có mã hóa ở bất kỳ khối dữ liệu nào.
d. Nếu dùng dịch vụ tương thích e-mail thì mỗi nhóm 3 byte dữ liệu nhị phân được ánh xạ thành 4 ký tự ASCII.

**2. Khi cần truyền một thông điệp và dùng cả hai dịch vụ bí mật và xác thực của PGP thì phần nào sẽ được mã hóa đối xứng bằng khóa phiên?**
a. Thông điệp.
b. Tóm tắt thông điệp.
c. Chữ ký số trên thông điệp.
d. Thông điệp và chữ ký số trên thông điệp.

**3. Khóa được sử dụng để mã hóa khóa phiên trong PGP khi dùng trên hệ thống E-mail là:**
a. Khóa công khai của người gởi.
b. Khóa riêng của người gởi.
c. Khóa công khai của người nhận.
d. Khóa riêng của người nhận.

**4. Chế độ hoạt động của PGP khi thực hiện mã hóa đối xứng là:**
a. CBC b. ECB c. CFB d. OFB

**5. Thuật toán mã hóa nào sau đây là phù hợp với mã hóa đối xứng của PGP:**
a. DES
b. 3DES với 2 khóa
c. AES
d. Cả câu (b) và (c) đều đúng

# CÂU HỎI CHƯƠNG VIII
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi
1. Cho biết ba mục tiêu thiết kế của bức tường lửa.
2. Các thông tin nào được sử dụng cho một bộ lọc gói.
3. Phân biệt bộ lọc gói không trạng thái và bộ lọc gói có trạng thái.
4. Điểm yếu của bộ lọc gói là gì?
5. Trình bày điểm khác biệt giữa ba cấu hình bức tường lửa trong hình 20.2([1]).

## II. Câu hỏi trắc nghiệm
**1. Cho biết mục tiêu nào sau đây là mục tiêu thiết kế một bức tường lửa?**
a. Tất cả thông tin từ bên trong ra bên ngoài và ngược lại phải đi qua bức tường lửa.
b. Tất cả thông tin di chuyển bên trong một mạng cục bộ phải đi qua bức tường lửa.
c. Chỉ các loại thông tin được cấp quyền thông qua chính sách an ninh cục bộ mới được phép đi qua bức tường lửa.
d. Các câu (a) và (c) đều đúng.
e. Các câu (a), (b) và (c) đều đúng.

**2. Chọn phát biểu sai khi nói về bộ lọc gói (packet filter ):**
a. Nó không xem xét dữ liệu ở tầng ứng dụng trong mô hình TCP/IP.
b. Nó không thể ngăn chặn các cuộc tấn công sử dụng các lỗ hổng ứng dụng cụ thể.
c. Nó có khả năng phát hiện các tấn công dạng giả mạo địa chỉ ở tầng mạng
**d.** Chức năng ghi nhật ký (logging) của nó bị hạn chế.

**3. Chọn phát biểu sai trong các phát biểu sau khi nói về các loại bức tường lửa.**
a. Packet fiter quyết định lọc gói dựa trên thông tin các trường trong IP và TCP header.
b. Circuit-level gateway cho phép thiết lập một kết nối TCP end to end.
c. Application-level gateway còn được gọi là proxy server.
d. Application-level gateway an toàn hơn Packet fitering router.

**4. Cho biết cấu hình bức tường lửa nào sau đây có khả năng ngăn chặn các vi phạm an ninh mạng khi bộ lọc gói trên bộ định tuyến kết nối với Internet bị thương tổn hay đã thỏa hiệp.**
a. single-homed bastion host
b. dual-homed bastion host
c. screened subnet
d. Câu (b) và (c) đều đúng

**5. Cách thức để hạn chế tấn công SYN-Flooding trên bức tường lửa là:**
a. Cho phép nhận một lượng nhất định gói SYN trong một giây.
b. Chặn những IP kết nối thất bại nhiều lần.
c. Chỉ cho phép gói SYN trên một số port nhất định.
d. Tất cả đều đúng.

# CÂU HỎI CHƯƠNG IX
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi
1. Cho biết ba loại thâm nhập bất hợp pháp.
2. Ba lợi ích có thể được cung cấp bởi một hệ thống phát hiện xâm nhập là gì?
3. Phân biệt hai hướng tiếp cận để phát hiện thâm nhập bất hợp pháp.
4. Phân biệt hai hệ thống phát hiện thâm nhập bất hợp pháp.
5. Cho biết các vấn đề nảy sinh đối với các hệ thống ngăn chặn bất hợp pháp (IPS).

## II. Câu hỏi trắc nghiệm
**1. Hướng phát hiện thâm nhập bất hợp pháp nào liên quan đến việc thu thập hành vi người dùng hợp pháp trong một khoảng thời gian và sau đó phân tích đánh giá:**
a. Phát hiện dựa trên thống kê
b. Phát hiện dựa trên quy tắc
c. Lai tạo
d. Các câu trên đều sai

**2. Cho biết phát biểu sai trong các phát biểu sau khi nói đến hệ thống phát hiện thâm nhập bất hợp pháp:**
a. Để xây dựng hệ thống phát hiện thâm nhập bất hợp pháp ta có hai hướng tiếp cận là rule-based detection và behavior-based detection.
b. Nếu hệ thống phát hiện một xâm nhập đủ nhanh, kẻ xâm nhập có thể được xác định trước khi bị thiệt hại.
c. Một hệ thống phát hiện thâm nhập bất hợp pháp hiệu quả có thể kết hợp với bức tường lửa để ngăn chặn ngay các xâm nhập.
d. Nó cho phép ta thu thập thông tin về các kỹ thuật xâm nhập đã được sử dụng để tăng cường cho công tác phòng chống xâm nhập.

**3. Đối với việc khởi tạo một IDS, sau khi đã xác định mục tiêu ta phải làm gì tiếp theo?**
a. Chọn đáp ứng thích hợp
b. Xét các ngưỡng
c. Hiện thực chính sách
d. Chọn thành phần, hệ thống để theo dõi

**4. Nếu một tổ chức muốn bảo vệ một máy chủ tránh bị người dùng hợp pháp phá hoại, hệ thống phát hiện thâm nhập bất hợp pháp nào là lựa chọn tốt nhất?**
a. NIDS
b. HIDS
c. Lai tạo
d. Các câu trên đều sai

**5. Nếu một tổ chức muốn phát hiện các tấn công với chi phí thấp thì hệ thống phát hiện thâm nhập bất hợp pháp nào là lựa chọn tốt nhất?**
a. NIDS
b. HIDS
c. Lai tạo
d. Các câu trên đều sai

# CÂU HỎI CHƯƠNG X
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi
1. Mạng riêng ảo là gì?
2. Các chức năng của mạng riêng ảo là gì?
3. Trình bày cơ chế hoạt động của VPN
4. Các vấn đề chính của User VPN là gì?
5. Liệt kê các thành phần chính của VPN.

## II. Câu hỏi trắc nghiệm
**1. VPN là viết tắt của:**
a. Virtual Public Network
b. Virtual Private Network
c. Virtual Protocol Network
d. Virtual Perimeter Network

**2. Lợi ích chính của VPN so với các mạng chuyên dụng như frame relay, leased line hay dial-up truyền thống là gì?**
a. Hiệu suất mạng tốt hơn
b. Ít bị lỗi hơn
c. Giảm chi phí
d. Cải thiện an ninh

**3. Trong VPN, thuật ngữ "tunneling" đề cập đến:**
a. Một tính năng tùy chọn làm tăng hiệu suất mạng.
b. Đóng gói các gói tin bên trong các gói tin của một giao thức khác để tạo và duy trì mạch ảo
c. Phương pháp quản trị hệ thống sử dụng để phát hiện tin tặc trên mạng
d. Một chiến lược tiếp thị để bán các sản phẩm VPN

**4. Những giao thức nào sau đây là giao thức VPN tunneling?**
a. PPTP
b. L2TP
c. IPSec
d. Tất các các câu trên đều đúng

**5. Khác biệt giữa Firewall và VPN là gì?**
a. Firewall có thể cấu hình còn VPN thì không cấu hình được.
b. Firewall là một loại mới của VPN.
c. Firewall chặn các thông điệp còn VPN thì mở ra con đường cho các thông điệp hợp lệ đi qua.
d. Không có khác biệt giữa Firewall và VPN.

# CÂU HỎI CHƯƠNG XI
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi
1. Biện pháp nào được sử dụng nhằm giảm nguy cơ từ mối đe dọa AP giả mạo.
2. Mã hóa trong WEP dùng thuật toán gì?
3. Phân biệt chế độ WPA doanh nghiệp và WPA cá nhân.
4. Mã hóa trong WPA2 dùng thuật toán gì?
5. So sánh các chuẩn an ninh WLAN

## II. Câu hỏi trắc nghiệm
**1. WEP được viết tắt là:**
a. Wireless Encryption Protocol
b. Wireless Encryption Privacy
c. Wired Equivalent Privacy
d. Wired Equivalent Protocol

**2. Điểm yếu thật sự của WEP trong vấn đề mã hóa là:**
a. Dùng thuật toán RC4
b. Dùng khóa chung quá ngắn
c. Thuật toán lập lịch khóa của RC4
d. Không xác thực người dùng

**3. Tiêu chuẩn an ninh mạnh mẽ hơn được phát triển bởi IEEE để giải quyết các lỗ hổng chuẩn WLAN IEEE 802.11 là:**
a. IEEE 802.16.2
b. IEEE 802.11e
c. IEEE 802.11i
d. IEEE 802.11n

**4. Khác biệt giữa WPA và WPA2 là:**
a. WPA mã hóa dùng RC4, WPA2 mã hóa dùng AES.
b. WPA mã hóa dùng RC4 với TKIP/MIC, WPA2 mã hóa dùng AES.
c. WPA xác thực dùng PSK, WPA2 xác thực dùng 802.1x/EAP.
d. WPA xác thực dùng ICV, WPA2 xác thực dùng 802.1x/EAP.

**5. Chọn phát biểu sai trong các phát biểu sau:**
a. WPA là một tập con của IEEE 802.11i
b. AES là mã hóa đối xứng.
c. WPA2 cho phép các client AES và TKIP được hoạt động trên cùng WLAN.
d. IEEE 802.11i thực thi an ninh trên port.

# ĐÁP ÁN CÂU HỎI VÀ BÀI TẬP CHƯƠNG I
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi

1. C-I-A (bí mật - Confidentiality, toàn vẹn - Integrity, sẵn sàng - Availability).

2. Tấn công thụ động lấy trộm thông tin nhưng không làm thay đổi nội dung dòng dữ liệu hay tạo dòng dữ liệu sai lệch.Trong khi đó tấn công chủ động làm thay đổi nội dung dòng dữ liệu hay tạo dòng dữ liệu sai lệch.

3. Tấn công thụ động: lấy nội dung của thông điệp, Phân tích lưu lượng. Tấn công chủ động: giả mạo, phát lại, thay đổi nội dung thông điệp, từ chối dịch vụ.

4. Các cơ chế trong kiến trúc an ninh OSI bao gồm:
   - Các cơ chế an ninh cụ thể: mã hóa, chữ ký số, kiểm soát truy cập, toàn vẹn dữ liệu, trao đổi xác thực, chèn thông tin trong lưu thông, điều khiển định tuyến, công chứng.
   - Các cơ chế an ninh phổ biến.

5. Các dịch vụ trong kiến trúc an ninh OSI bao gồm:
   - Dịch vụ xác thực
   - Dịch vụ kiểm soát truy cập
   - Dịch vụ bí mật dữ liệu, dòng thông tin
   - Dịch vụ toàn vẹn dữ liệu
   - Dịch vụ chống thoái thác
   - Dịch vụ sẵn sàng

## II. Câu hỏi trắc nghiệm

1. a  2. b  3. a  4. d  5. c

## III. Bài tập

1.

| | Lấy nội dung thông điệp | Phân tích lưu lượng | Giả mạo | Phát lại | Thay đổi nội dung thông điệp | Từ chối dịch vụ |
|---|---|---|---|---|---|---|
| Xác thực | | | x | | | |
| Kiểm soát truy cập | | | x | | | |
| Bí mật dữ liệu, dòng thông tin | x | x | | | | |
| Toàn vẹn dữ liệu | | | | x | x | |
| Chống thoái thác | | | x | | | |
| Sẵn sàng | | | | | | x |

2.

| | Lấy nội dung thông điệp | Phân tích lưu lượng | Giả mạo | Phát lại | Thay đổi nội dung thông điệp | Từ chối dịch vụ |
|---|---|---|---|---|---|---|
| Mã hóa | x | | | | | |
| Chữ ký số | | | x | x | x | |
| Kiểm soát truy cập | x | x | x | x | | x |
| Toàn vẹn dữ liệu | | | x | x | | |
| Trao đổi xác thực | | | x | x | | x |
| Chèn thông tin trong lưu thông | | x | | | | x |
| Điều khiển định tuyến | x | x | | | | x |
| Công chứng | | | x | x | x | |

# ĐÁP ÁN CÂU HỎI VÀ BÀI TẬP CHƯƠNG II
## Môn: AN NINH MẠNG
-o0o-

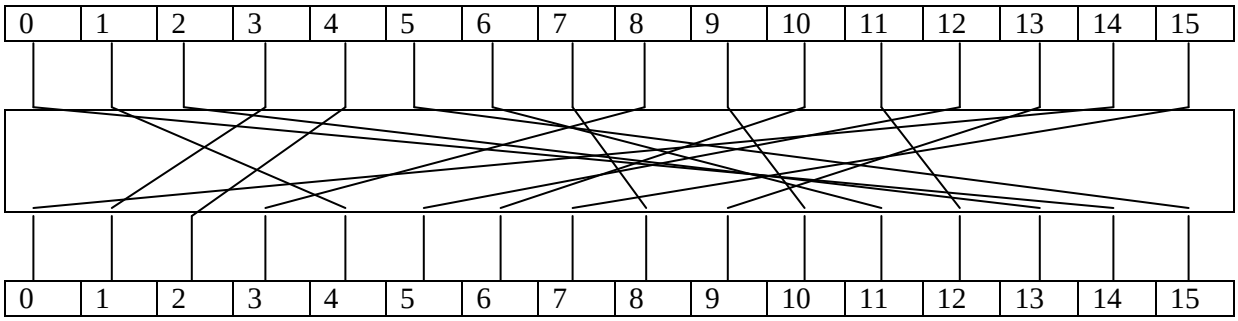
## I. Câu hỏi

1. Encryption algorithm, decryption algorithm.
2. Plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.
3. Một khóa
4. Mã hóa dòng xử lý các thông điệp theo từng bit hay byte tại mỗi thời điểm. Mã hóa khối xử lý các dòng thông điệp theo từng khối(ví dụ 64 bits) tại mỗi thời điểm.
5. Sắp xếp lại thứ tự các ký tự mà không thay đổi không thay đổi các ký tự trong bản rõ.
6. Một mã thay thế theo sau một mã hoán vị.
7. Khối có chiều dài 64 bits và khóa có chiều dài 56 bits.
8. S-box trong DES là hàm thay thế không tuyến tính làm tăng độ phức tạp của việc biến đổi.
9. 3DES có thể dùng 3 khóa riêng biệt cho 3 giai đoạn. Một thay thế khác là dùng 2 khóa, một khóa được dùng cho cả giai đoạn 1 và giai đoạn 3.
10. 5 chế độ hoạt động: ECB, CBC, CFB, OFB, CTR.

## II. Câu hỏi trắc nghiệm

1. c  2. c  3. a  4. b  5. a

## III. Bài tập

1. $k_1$ nguyên tố cùng nhau với 256 vậy $k_1$ là các số lẻ và $\leq k_1 \leq 255$. $k_2$ là tùy ý và $\leq k_2 \leq 255$. Số lượng khóa ($k_1$, $k_2$) hợp lệ là 128 x 256 = 32.768
2. 

3. 1, 1, 0, 1
4.

| Mode | Encrypt | Decrypt |
|---|---|---|
| ECB | $C_j = E(K, P_j)$ $j = 1, \ldots, N$ | $P_j = D(K, C_j)$ $j = 1, \ldots, N$ |
| CBC | $C_1 = E(K, [P_1 \oplus IV])$<br>$C_j = E(K, [P_j \oplus C_{j-1}])$ $j = 2, \ldots, N$ | $P_1 = D(K, C_1) \oplus IV$<br>$P_j = D(K, C_j) \oplus C_{j-1}$ $j = 2, \ldots, N$ |
| CFB | $C_1 = P_1 \oplus S_s(E[K, IV])$<br>$C_j = P_j \oplus S_s(E[K, C_{j-1}])$ | $P_1 = C_1 \oplus S_s(E[K, IV])$<br>$P_j = C_j \oplus S_s(E[K, C_{j-1}])$ |
| OFB | $C_1 = P_1 \oplus S_s(E[K, IV])$<br>$C_j = P_j \oplus S_s(E(K, [C_{j-1} \oplus P_{j-1}]))$ | $P_1 = C_1 \oplus S_s(E[K, IV])$<br>$P_j = C_j \oplus S_s(E(K, [C_{j-1} \oplus P_{j-1}]))$ |
| CTR | $C_j = P_j \oplus E[K, Counter + j - 1]$ | $P_j = C_j \oplus E[K, Counter + j - 1]$ |

# ĐÁP ÁN CÂU HỎI VÀ BÀI TẬP CHƯƠNG III

**Môn: AN NINH MẠNG**

-o0o-

## I. Câu hỏi

1. b là ước số của a nghĩa là a = mb với a, b, m là số nguyên.
2. Số nguyên tố là số chỉ chia hết cho 1 và chính nó.
3. Là số các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n.
4. a và n là nguyên tố cùng nhau, n > 0 và nếu ϕ(n) là số nguyên dương nhỏ nhất sao cho $\mathbf{a}^{\phi(n)} \equiv 1 \mod n$ thì a được gọi là căn nguyên thủy của n.
5. Public key, private key, plaintext, encrypt algorithm, ciphertext, decrypt algorithm.
6. 2 cặp khóa tức là bốn khóa.
7. Khóa công khai dùng để mã hóa dữ liệu hoặc xác minh chữ ký số. Khóa riêng dùng để giải mã dữ liệu hoặc ký(tạo chữ ký số).
8. Mã hóa/giải mã; chữ ký số; trao đổi khóa.
9. 

Bước 1: Lấy một số nguyên dương lẻ ngẫu nhiên.

Bước 2: Lấy một số nguyên dương a ngẫu nhiên mà $a < n$.

Bước 3: Thực hiện phép kiểm tra xác xuất như dùng Miller-Rabin. Nếu n là hợp số thì lặp lại bước 1, nếu không tăng số lần kiểm tra lên 1.

Bước 4: Nếu n đã thành công qua một số lượng kiểm tra thì chấp nhận n nếu không lặp lại bước 2.

10. Hai bên tạo cặp khóa công khai, khóa riêng và trao đổi khóa công khai cho nhau. Các khóa này được thiết kế sao cho hai bên có thể tính được một khóa bí mật duy nhất dựa trên khóa riêng của mỗi bên và khóa công khai của bên kia.

## II. Câu hỏi trắc nghiệm

| | | | | |
|---|---|---|---|---|
| 1. b | 3. d | 5. a | 7. a | 9. a |
| 2. c | 4. d | 6. c | 8. d | 10. c |

## III. Bài tập

1. 
   a. x = 2
   b. x = 3
   c. Không có giá trị x nào thỏa mãn.
2. 
   a. 3239
   b. Không có phần tử nghịch đảo nhân
   c. 550
3. 3
4. 1
5. 
   a. 40
   b. 18
   c. 120
   d. 160
6. **Dùng mã hóa RSA, cho biết bản mã C trong các trường hợp sau:**
   a. C = 36
   b. C = 14
   c. C = 57
   d. C = 106
   e. C = 2
7. M = 5
8. 
   a. Nếu kiểm tra 2^*n* với $n < 10$ thì không có giá trị nào $\equiv 1 \mod 11$.
   b. 6
   c. 3

# ĐÁP ÁN CÂU HỎI VÀ BÀI TẬP CHƯƠNG IV
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi

1. Mã hóa thông điệp, MAC, hàm băm.

2. Mã xác thực thông điệp(MAC) tạo ra mã xác thực thông điệp có chiều dài cố định và có dùng khóa. Hàm băm một chiều tạo ra một giá trị băm có chiều dài cố định(không có khả năng xác thực thông điệp) và không dùng khóa.

3. HMAC

4.
   a. Nó phải có khả năng xác minh tác giả và ngày giờ tạo ra chữ ký.
   b. Nó phải có khả năng xác thực nội dung tại thời điểm ký.
   c. Nó có khả năng được xác minh bởi bên thứ ba để giải quyết tranh chấp.

5. Kích thước chữ ký nhỏ hơn; tất cả các tính toán cho ký và xác minh đều nhỏ hơn so với RSA.

## II. Câu hỏi trắc nghiệm

1. b  2. b  3. c  4. d  5. a

## III. Bài tập

1.
   a. Chỉ thỏa mãn các yêu cầu từ 1 đến 3. Các yêu cầu 4, 5, 6 không được thỏa mãn.
   b. Thỏa mãn các yêu cầu từ 1 đến 3. Yêu cầu 4 được thỏa mãn khi n là 1 hợp số đủ lớn. Yêu cầu 5, 6 không được thỏa mãn vì h(M) = h(-M)
   c. 955

2. Khóa riêng của người dùng sẽ được khám phá.

# ĐÁP ÁN CÂU HỎI CHƯƠNG V
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi

1. Vấn đề mà Kerberos xem xét và giải quyết là: trong môi trường phân bố mở, người dùng ở các máy trạm muốn truy cập các dịch vụ trên các máy chủ phân bố trên toàn bộ mạng. Bên cạnh đó chúng ta còn mong muốn các máy chủ có thể hạn chế truy cập chỉ cho người có thẩm quyền và được phép xác thực các yêu cầu dịch vụ. Trong môi trường này, một máy trạm không thể được tin cậy để xác định người sử dụng một cách chính xác với các dịch vụ mạng.

2. An toàn, tin cậy, trong suốt, khả mở.

3. Kerberos version 5 đã khắc phục một số hạn chế về môi trường và một số thiếu sót về kỹ thuật trong Kerberos version 4.

4. X.509 định nghĩa một khung làm việc cho việc cung cấp dịch vụ xác thực bởi thư mục X.500 đến người dùng của nó. Thư mục này có thể phục vụ như kho lưu trữ các chứng chỉ khóa công khai. Mỗi chứng chỉ bao gồm khóa công khai của người dùng và nó được ký bằng khóa riêng của một nhà phát hành chứng chỉ tin cậy. Ngoài ra, X.509 còn định nghĩa các giao thức xác thực thay thế dựa trên việc sử dụng chứng chỉ khóa công khai.

5. Chủ sở hữu của chứng chỉ có thể gởi yêu cầu thu hồi đến nhà phát hành chứng chỉ hoặc nhà phát hành chứng chỉ thu hồi các chứng chỉ đã hết hạn sử dụng.

## II. Câu hỏi trắc nghiệm

1. d  2. b  3. c  4. d  5. d

# ĐÁP ÁN CÂU HỎI CHƯƠNG VI

**Môn: AN NINH MẠNG**

-o0o-

## I. Câu hỏi

1. Xác thực, bí mật, nén, tương thích với E-mail và phân mảnh.

2. Thích hợp cho việc lưu trữ thông điệp không nén cùng chữ ký để xác minh trong tương lai. Ngoài ra việc ký trước khi nén cũng không chịu ảnh hưởng khi các phiên bản PGP thay đổi thuật toán nén.

3. Thuật toán Radix-64 chuyển đổi một dòng 8 bits dạng nhị phân thành dòng các ký tự ASCII có thể in được. Một nhóm 3 bytes được ánh xạ thành 4 ký tự ASCII.

4. RFC 822 định nghĩa định dạng thông điệp văn bản được gởi khi sử dụng với E-mail.

5. S/MIME là cải tiến an toàn của MIME trên hệ thống E-mail.

## II. Câu hỏi trắc nghiệm

1. c 2. d 3. c 4. c 5. d

# ĐÁP ÁN CÂU HỎI CHƯƠNG VII
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi

1. IPSec, SSL, các dịch vụ an toàn cho ứng dụng xác định.

2. SSL handshake protocol; SSL change cipher spec protocol; SSL alert protocol; SSL record protocol.

3. Một kết nối SSL là một liên kết truyền thông ngang hàng, ngắn hạn và cung cấp một loại dịch vụ. Nhiều kết nối tồn tại trên cùng một phiên. Một phiên bắt tay bằng giao thức SSL Handshake xác định một tập hợp các tham số liên quan đến mật mã và được chia xẻ cho nhiều kết nối.

4. Cardholder: chủ thẻ; Merchant: bán hàng; Issuer: đơn vị phát hành thẻ; Acquirer: tổ chức chi trả đại diện; Payment gateway: cổng thanh toán là một chức năng của tổ chức chi trả đại diện hoặc một bên thứ ba; CA: đơn vị cấp chứng chỉ.

5. Chữ ký đôi nhằm liên kết hai thông điệp được gửi đến hai nơi nhận khác nhau tuy nhiên không bên nào biết thông tin chi tiết của bên kia nhưng phải biết chúng được liên kết với nhau. Đối với giao dịch điện tử an toàn, chữ ký đôi được dùng để ký trên hai tài liệu gồm: thông tin đặt hàng (order information-OI), thông tin thanh toán (payment information-PI).

## II. Câu hỏi trắc nghiệm

1. d 2. a 3. d 4. c 5. b

# CÂU HỎI CHƯƠNG VIII
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi

1.
   a. Tất cả thông tin từ bên trong ra bên ngoài và ngược lại phải đi qua nó.
   b. Chỉ những lưu thông mạng có quyền được phép đi qua. Các lưu thông mạng có quyền được định nghĩa bởi chính sách an ninh cục bộ.
   c. Bản thân nó phải miễn dịch

2. Source IP address, destination IP address, source port, destination port, IP protocol field, interface.

3. Một bộ lọc gói tin không trạng thái đưa ra những quyết định lọc trên cơ sở từng gói tin riêng lẻ mà không xem xét bối cảnh lớp cao hơn. Một bộ lọc gói kiểm tra trạng thái thắt chặt các quy tắc giao thông cho TCPbằng cách tạo một bảng của các kết nối TCP đang được thiết lập. Các bộ lọc gói tin này sẽ chỉ cho phép các gói tin phù hợp với một trong những kết nối đang được thiết lập.

4. Không xem xét dữ liệu ở tầng cao hơn; chức năng nhật ký bị giới hạn; không hỗ trợ các lược đồ xác thực người dùng; không phát hiện giả mạo địa chỉ IP; dễ dàng cho phép lưu thông các loại thông tin mà bị cấm dựa trên chính sách an ninh thông tin của tổ chức.

5. Cấu hình single – home bastion bao gồm 2 hệ thống: một bộ lọc gói và một bastion host; bastion host diễn tả các chức năng xác thực và đại diện. Với cấu hình này khi bộ lọc gói bị thỏa hiệp, lưu thông có thể đi trực tiếp từ Internet vào các máy tính trong mạng nội bộ. Cấu hình dual-home bastion ngăn chặn hành vi vi phạm an ninh như vậy. Trong cấu hình screened subnet firewall, hai bộ lọc gói được dùng, một giữa bastion host và Internet, một giữa bastion host và mạng nội bộ. Cấu hình này tạo ra một mạng con cô lập bao gồm bastion host hoặc một hay nhiều máy chủ khác và các modem cho việc dial-in.

## IV. Câu hỏi trắc nghiệm

1. d  2. c  3. b  4. d  5. d

# ĐÁP ÁN CÂU HỎI CHƯƠNG IX
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi

1.
   a. Thâm nhập bất hợp pháp từ bên ngoài đến một số hệ thống máy tính bên trong.
   b. Thâm nhập bất hợp pháp từ người dùng hợp pháp đến dữ liệu, các chương trình, tài nguyên không được cấp quyền.
   c. Thâm nhập bất hợp pháp từ người kiểm soát hệ thống và sử dụng quyền này để né tránh hay ngăn chặn hệ thống kiểm soát truy cập và kiểm toán

2.
   a. Ngăn chặn truy cập và thao tác trái phép và giảm thiểu thiệt hại nếu phát hiện nhanh chóng.
   b. Hệ thống phát hiện xâm nhập hiệu quả có thể phục vụ như một bộ ngăn chặn.
   c. Thu thập thông tin để cải thiện an ninh trong tương lai.

3. Phát hiện dựa trên thống kê thông thường liên quan đến việc thu thập dữ liệu liên quan hành vi người dùng hợp pháp trong một khoảng thời gian. Sau đó phân tích, đánh giá và áp dụng các kết quả thống kê để xác định một hành vi không phải là hành vi của người dùng hợp pháp khi nó vượt qua một ngưỡng nào đó. Phát hiện dựa trên quy tắc liên quan đến nỗ lực để xác định một tập quy tắc có thể được sử dụng để quyết định một hành vi là một thâm nhập bất hợp pháp.

4. NIDS: Hệ thống phát hiện thâm nhập bất hợp pháp trên mạng; HIDS: Hệ thống phát hiện thâm nhập bất hợp pháp trên máy chủ.

5. Từ chối dịch vụ và tính sẵn sàng.

## II. Câu hỏi trắc nghiệm

1. a  2. a  3. d  4. b  5. a

# ĐÁP ÁN CÂU HỎI CHƯƠNG X
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi

1. Là một loại mạng riêng sử dụng môi trường truyền thông công cộng như Internet, thay vì dùng đường thuê bao (leased line) để truyền thông.

2. Bí mật, toàn vẹn, xác thực, quản lý truy cập.

3. VPN tạo ra một kết nối ảo điểm – điểm thông qua mạng công cộng. Nó vận chuyển các gói tin đã được đóng gói bằng một giao thức khác.

4.
   a. Nguy cơ vi phạm an toàn khá lớn khi người dùng kết nối đồng thời đến các trang Web khác hay thỏa hiệp với một chương trình virus/trojan/worm.
   b. Xác thực người dùng.
   c. Tải trên mạng.
   d. Liên quan đến việc sử dụng NAT

5. Các thành phần chính của VPN là VPN Server, thuật toán mã hóa, hệ thống xác thực và giao thức VPN như IPSec, SSL, …

## II. Câu hỏi trắc nghiệm

1. b  2. c  3. b  4. d  5. c

# ĐÁP ÁN CÂU HỎI CHƯƠNG XI
## Môn: AN NINH MẠNG
-o0o-

## I. Câu hỏi

1. Xác thực lẫn nhau tức là dùng WPA hoặc WPA2.

2. RC4.

3. WPA doanh nghiệp xác thực dùng 802.1x/EAP còn WPA cá nhân xác thực dùng PSK (Pre Shared Key).
4. AES
5.

| | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| **Mã hóa** | RC4 | RC4 với TKIP/MIC | AES |
| **Quay vòng khóa** | Không | Các khóa phiên động | Các khóa phiên động |
| **Phân phối khóa** | Gõ bằng tay vào mỗi thiết bị | Phân phối tự động | Phân phối tự động |
| **Xác thực** | Dùng khóa WEP | Có thể dùng 802.1x & EAP | Có thể dùng 802.1x & EAP |

## II. Câu hỏi trắc nghiệm

1. c 2. c 3. c 4. b 5. d

# Giua ky 2009

Đề kiểm tra giữa kỳ (Học kỳ I) (2009)
Môn: **Mật Mã & An Ninh Mạng**
Thời gian: 30 phút
(Không được dùng tài liệu)

**Câu 1:** DDOS thuộc loại tấn công nào:
=> Active Attack

**Câu 2:** Việc tránh sử dụng trái phép tài nguyên:
=> Access Control

**Câu 3:** Việc bảo vệ nhằm chống lại sự từ chối của một trong các bên của 1 giao tiếp
=> Non-Repudiation

**Câu 4:** Khóa trong mã hóa đối xứng phải được biết bởi ai?
=> Bên nhận và gửi (a và b đúng)

**Câu 5:** Cesar thuộc vào mã hóa đối xứng truyền thống nào:
=> Substitution Cipher (mã thay thế)

**Câu 6:** Trong 3 loại MH đối xứng (Trans, Subs, Product), mã hóa nào dẫn xuất của 2 loại kia:
=> Product Cipher (mã nhân)

**Câu 7:** Hãy dùng mã hóa Playfair để mã hóa chuỗi ……
=> ……

**Câu 8:** Dùng mã hóa Vigenère với key là chuỗi sau ……
=> ……

**Câu 9:** Dùng định lý Fermat: 3^(……) mod 11
=> ……

**Câu 10:** Giá trị hàm Euler Totient: O(70) là: (phi của 70)
=> 24

**Câu 11:** Đối với phương pháp MH công khai, khóa nào được sử dụng khi cần MH data trước gửi
=> Khóa công khai của người nhận

**Câu 12:** Đối với phương pháp MH công khai, khóa nào tạo chữ ký số trên 1 message
=> Khóa riêng của người gửi

**Câu 13:** Đối với lược đồ MH công khai RSA, khóa công khai được diễn tả là:
=> (e, n)

**Câu 14:** Đối với lược đồ MH công khai RSA, cho biết khóa d quan hệ với e như thế nào
=> $e.d \equiv 1 \bmod o(n)$ và $0 < d < n$

**Câu 15:** Đối với lược đồ MH công khai RSA, cho n = 187, e = 3. Chọn d
=> 107

**Câu 16:** Đối với lược đồ MH công khai RSA, cho n = 187, e = 7, d = 23. Cho biết MH của M = 88
=> 11

**Câu 17:** Sun Java hỗ trợ JCA bao gồm
=> Provider, Service

**Câu 18:** Trong JCA, method getInstance() dùng để
=> Xác định dẫn xuất liên quan đến 1 phương pháp mã hóa

**Câu 19:** Trong JCA, giả sử có 2 provider cùng hỗ trợ 1 phương pháp mã hóa. Khi người dùng gọi MH, provider nào được chọn?
=> Tùy thuộc vào giá trị "preference order" của 1 provider
=> Người dùng chọn provider nào thì dùng provider đó

**Câu 20:** Chọn SAI khi lập trình mã hóa RSA sử dụng service Cipher trong JCA
=> Lớp SecretKey dùng để sinh khóa cho RSA

---

*Chép lại đề và đáp án: HLND (email: hoanglenghiaduc@gmail.com)*

# Cuoi ky 2009

**1.** Chọn phát biểu sai khi nói về bộ lọc gói (packet filtering router)
- a. Nó không xem xét dữ liệu ở tầng ứng dụng trong mô hình TCP/IP
- b. Nó không có khả năng phát hiện các tấn công giả mạo địa chỉ ở tầng mạng
- c. Nó không có khả năng phát hiện các tấn công dựa trên các lỗ hổng của các tầng từ tầng vận chuyển trở lên
- d. Nó hầu như không hỗ trợ các lược đồ xác thực người dùng cao cấp

**2.** Cho biết cấu hình bức tường lửa nào sau đây có khả năng phòng tránh các tấn công khi bộ lọc gói trên bộ định tuyến kết nối với Internet bị thương tổn hay đã tắt
- a. Single-Homed Bastion Host
- b. Dual- Homed Bastion Host.
- c. Screened-subnet Firewall
- d. Câu b và c đều đúng

**3.** Chọn phát biểu sai trong các phát biểu sau khi nói về các loại bức tường lửa
- a. Packet filtering router quyết định lọc gói dựa trên thông tin các trường trong mỗi gói
- b. Application-level gateway còn được gọi là proxy server.
- c. Application-level gateway an toàn hơn Packet filtering router
- d. Curcuit-level gateway cho phép thiết lập một kết nối TCP end to end ?

**4.** Chọn phát biểu sai khi nói về virus và worm
- a. Cả virus và worm đều có khả năng lây lan và tạo bản sao
- b. Cả virus và worm đều được đính kèm trong một chương trình
- c. Worm có khả năng tái tạo chính nó
- d. Virus có khả năng phát tán bản sao từ máy tính này sang máy tính khác

**5.** Cho biết thành phần tham gia trong giao dịch điện tử an toàn (SET- Secure Electronic Transaction) có trách nhiệm thanh toán các khoản mua hành của chủ thẻ
- a. Cardholder
- b. Merchant
- c. Issuer ?
- d. Acquier ?

**6.** Cho biết phát biểu sai về dual signature trong các phát biểu sau:
- a. Mục đích của dual signature là để liên kết hai thông điệp dành cho hai nơi
- b. Dual signature được đăng ký trên hai tài liệu nối với nhau và mỗi tài liệu
- c. Đối với giao dịch điện tử an toàn, dual signature được dùng để ký trên… thẻ thanh toán (Payment information- PI), và thông tin đặt hàng (Order information- OI).
- d. Đối với giao dịch điện tử an toàn, dual signature được dùng nhằm để…được hash code của tài liệu đặt hàng

**7.** Chế độ nào của IPsec không bảo vệ IP header
- a. Tunnel
- b. Transport
- c. Cả 2 câu a và b đều đúng
- d. Cả 2 câu a và b đều sai

**8.** Các giao thức được thiết kế bởi IETF nào an toàn cho gói dữ liệu ở tầng mạng trong mô hình mạng OSI
- a. IPsec
- b. SSL
- c. PGP
- d. Cả 3 câu trên đều đúng

**9.** Tham số nào của sự kết hợp bảo mật SA (Security Association) gồm các thông số xác thực, khóa, và thời gian sống của khóa
- a. Security Parameters Index (SPI)
- b. AH Information
- c. ESP Information
- d. Cả câu b và c đều đúng

**10.** Giao thức IKE (Internet Key Exchange) tạo các kết hợp bảo mật (SA- Security Association) nào sau đây
- a. PGP
- b. SSL
- c. IPsec
- d. Cả câu b và c đều đúng

**11.** Cho biết tấn công nào gây nguy hiểm cho sự an toàn của phương pháp trao đổi thông tin không chứng thực lẫn nhau
- a. Ciphertext attack
- b. Plaintext attack

c. Secret-text attack
d. Các câu trên đều đúng

**12.** SSL không cung cấp dịch vụ nào sau đây:
a. Authenticaiton
b. Confidentiality
c. Message Integrity
d. Compression

**13.** SSL không có khả năng chống lại dạng tấn công nào sau đây:
a. Man-in-the-middle-attack
b. IP Spoofing
c. SYN flooding
d. Cả 3 câu trên đều đúng

**14.** Giao thức nào của IPsec cung cấp dịch vụ xác thực và dịch vụ mã hóa thông tin trong Internet trong mô hình TCP/IP
a. AH
b. ESP
c. SSL
d. Cả ba câu trên đều đúng

**15.** Trong PGP, để gửi e-mail, người dùng cần có một bộ khóa, cho biết đó là bộ khóa nào:
a. Bộ khóa công khai
b. Bộ khóa riêng
c. Bộ khóa phiên
d. Cả 3 câu đều đúng

**16.** Chọn phát biểu sai khi nói về bức tường lửa
a. Tất cả truy cập mạng từ bên ngoài vào bên trong phải đi qua bức tường lửa
b. Tất cả truy cập mạng từ bên trong ra bên ngoài không nhất thiết phải qua bức tường lửa
c. Tất cả truy cập được phép được định nghĩa thông qua một chính sách thiết lập bởi người dùng.
d. Bức tường lửa chính nó phải là miễn dịch

**17.** Với SHA-512 cho biết phương trình để tính giá trị $W_{17}$
a. $W1 \oplus \sigma0(W2) \oplus W10 \oplus \sigma1(W15)$
b. $W0 \oplus \sigma0(W2) \oplus W10 \oplus \sigma1(W15)$
c. $W1 \oplus \sigma1(W2) \oplus W10 \oplus \sigma0(W15)$
d. $W0 \oplus \sigma1(W2) \oplus W10 \oplus \sigma0(W15)$

**18.** Chữ ký số (digital signature) sử dụng với các dịch vụ nào sau đây:
a. Xác thực (Authentication)
b. Không thể thoái thác (Nonrepudiation)
c. Tính toàn vẹn (Integrity)
d. Cả 3 câu đều đúng

**19.** Chọn phát biểu sai trong các phát biểu sau khi nói về các phiên SSL (SSL session):
a. Một kết nối SSL có một hoặc nhiều phiên SSL. (1 session có thể chia sẻ giữa nhiều connection)
b. Một kết nối SSL định nghĩa một bộ các tham số liên quan đến việc tạo phiên SSL
c. Kết nối SSL được sử dụng để tránh tốn kém trong việc thực hiện bảo mật cho mỗi phiên SSL.
d. Các câu trên đều sai

**20.** Cho biết giao thức nào sau đây không có trong kiến trúc SSL:
a. SSL Record Protocol
b. SSL Message Protocol
c. SSL Alert Protocol
d. SSL Change Cihper Spec Protocol

**21.** Cho biết tham số nào sau đây được định nghĩa trong mã hóa phía client và giải mã phía server:
a. Client Write Key
b. Server Write Key
c. Server Read Key
d. Client Read Key

| 1. | 2. | 3. | 4. | 5. | 6. | 7. | 8. | 9. | 10. | 11. | 12. | 13. | 14. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| 15. | 16. | 17. | 18. | 19. | 20. | 21. |
|---|---|---|---|---|---|---|

1, 6, 10, 12, 19

# Giua ky 2010

Đề kiểm tra giữa kỳ (Học kỳ II) (2010)
Môn: **Mật Mã & An Ninh Mạng**
Thời gian: 30 phút
(Không được dùng tài liệu)

**Câu 1:** Việc tránh sử dụng trái phép tài nguyên:
=> Access Control

**Câu 2:** Việc bảo vệ nhằm chống lại sự từ chối của một trong các bên của 1 giao tiếp
=> Non-Repudiation

**Câu 3:** Thông điệp sau khi được chuyển từ thông điệp ban đầu với 1 thuật toán mã hóa
=> Ciphertext

**Câu 4:** Khóa trong mã hóa đối xứng phải được biết bởi ai?
=> Bên nhận và gửi (a và b đúng)

**Câu 5:** Cho biết giải thuật MH Cesar như sau: ký tự A biến thành D. Hàm giải mã là:
=> (y + 23) % 26
Lưu ý: không chọn đáp án (y – 3) % 26 vì nếu y < 3 sẽ ra kết quả âm không có trong bảng ký tự

**Câu 6:** Chọn kết quả sau khi mã hóa Cesar chuỗi BREAK
=> ……

**Câu 7:** Hãy dùng mã hóa Playfair để mã hóa chuỗi …… với key = DETHIGIUAKY
=> ……

**Câu 8:** Đối với MH khối, có bao nhiêu cách (phép biến đổi) để MH 1 khối có chiều dài N bits?
=> $2^N!$

**Câu 9:** Chọn câu SAI
=> DES sử dụng cấu trúc mã hóa Feistel với số lượng vòng là 32

**Câu 10:** Dùng định lý Fermat: $3^{2011}$ mod 11
=> 3

**Câu 11:** Dùng Fermat và Euler mở rộng: $2^{1990}$ mod 77
=> 23

**Câu 12:** Giá trị hàm Euler Totient: O(210) là: (phi của 210)
=> 48

**Câu 13:** Đối với phương pháp MH công khai, khóa nào được sử dụng khi cần MH data trước gửi
=> Khóa công khai của người nhận

**Câu 14:** Đối với phương pháp MH công khai, khóa nào tạo chữ ký số trên 1 message
=> Khóa riêng của người gửi

**Câu 15:** Đối với lược đồ MH công khai RSA, cho n = 187, e = 3. Chọn d
=> 107

**Câu 16:** Đối với lược đồ MH công khai RSA, cho n = 187, e = 7, d = 23. Cho biết MH của M = 88
=> 11

**Câu 17:** Cần có tối thiểu bao nhiêu thay đổi trong 1 văn bản cho trước (nhằm tạo ra các phiên bản) sao cho xác suất tồn tại 2 phiên bản có giá trị hash như nhau là 0.5 (hash của 1 văn bản có chiều dài là 128bit)
=> 64
($\sqrt{(2^{128})} = 2^{64}$ các phiên bản => cần thay đổi 64 bit)

**Câu 18:** Chiều dài hash được tính bằng bit của SHA-1
=> 160

**Câu 19:** Chữ ký số dùng cho dịch vụ nào
=> Xác thực
=> Chống khoái thác

**Câu 20:** Chọn câu SAI về lược đồ tạo chữ ký số
=> Lược đồ DSA tạo chữ ký có chiều dài 512 bit

---

*Chép lại đề và đáp án: HLND (email: hoanglenghiaduc@gmail.com)*

# Ôn Tập 2

1. **Hình thức tấn công thụ động chống lại nguyên tắc cốt lõi nào của an toàn thông tin ?**
   a. Bí mật
   b. Toàn vẹn
   c. Sẵn sàng
   d. Xác thực
2. **Tấn công DOS (Denial of Service) thuộc loại tấn công nào trong kiến trúc an ninh OSI ?**
   a. Tấn công từ xa (Remote Attack)
   b. Tấn công chủ động (Active Attack)
   c. Tấn công thụ động (Passive Attack)
   d. Cả câu (a) và câu (b) đều đúng
3. **Cơ chế nào sau đây không cần thiết sử dụng để chống lại tấn công từ chối dịch vụ?**
   a. Mã hóa dữ liệu (encipherment)
   b. Quản lý định tuyến (routing control)
   c. Trao đổi xác thực (authentication exchange)
   d. Quản lý truy cập (access control)
4. **Cơ chế nào không sử dụng chodịch vụ xác thực?**
   a. Mã hóa dữ liệu (encipherment)
   b. Chữ ký số (digital signature)
   c. Trao đổi xác thực (authentication exchange)
   d. Quản lý truy cập (access control)
5. **Cho biết Code Red thuộc vào loại mã độc nào sau đây:**
   a. Virus
   b. Trojan
   c. Worm
   d. Là một loại mã độc lai ghép

1. **Hệ mã Cesar mã hóa x∈[0; 25] thành y = x + 3 mod 26. Hãy cho biết nếu giá trị bản rõ là 10 thì giá trị bản mã tương ứng là:**
   a. 5 b. 7 c. 13 d. 15
2. **Hệ mã Affine mã hóa x∈[0; 25] thành y = 3x + 5 mod 26. Hãy cho biết nếu giá trị bản mã là 10 thì giá trị bản rõ tương ứng là:**
   a. 9 b. 14 c. 19 d. 23
3. **Đối với mã hóa DES, trong các phát biểu sau phát biểu nào là sai?**
   a. DES sử dụng khóa có chiều dài 64 bits.
   b. Dữ liệu được mã hóa trong các khối có chiều dài 64 bits.
   c. S-box là một hàm thay thế không tuyến tính làm tăng độ phức tạp của phép biến đổi.
   d. DES dùng bộ tạo khóa để tạo ra các khóa con dùng cho mỗi vòng và chúng có chiều dài là 48 bits.
4. **Hệ mã Double DES(2DES) không an toàn do tấn công gì?**
   a. Tấn công "man in the midle"
   b. Tấn công "meet in the midle"
   c. Tấn công brute force
   d. Tấn công DOS
5. **Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt?**
   a. ECB
   b. CBC
   c. CFB
   d. OFB

4. **Hãy cho biết kết quả của ($7^{2010}$ mod 13):**
   a. 1
   b. 12
   c. 7
   d. Các giá trị trên đều sai

5. **Cho biết giá trị hàm phi Euler ϕ(440) là:**
   a. 439
   b. 240
   c. 160
   d. Tất cả các câu trên đều sai

6. **Hãy cho biết kết quả của ($3^{2086}$ mod 440):**
   a. 1 b. 3 c. 81 d. 289

7. **Đối với mã hóa khóa công khai, khóa nào được sử dụng để tạo chữ ký số trên một thông điệp:**
   a. Khóa công khai của người nhận
   b. Khóa riêng của người nhận
   c. Khóa công khai của người gửi
   d. Khóa riêng của người gửi

8. **Đối với mã hóa khóa công khai, khóa nào được sử dụng để mã hóa một thông điệp:**
   a. Khóa công khai của người nhận
   b. Khóa riêng của người nhận
   c. Khóa công khai của người gửi
   d. Khóa riêng của người gửi

**(Dữ liệu dùng cho câu 6 và 7)**
**Thực hiện mã hóa và giải mã với thuật toán RSA và p = 3; q = 11, e = 7; bản mã C = 5**

9. **Giá trị của d là:**
   a. 7 b. 5 c. 3 d. 2

10. **Giá trị của bản rõ M tương ứng là:**
    a. 26 b. 24 c. 5 d. 1

**(Dữ liệu dùng cho câu 10, 11, 12)**
**A và B dùng kỹ thuật trao đổi khóa Diffie-Hellman với q = 71 và α = 7.**

11. **Nếu A có khóa riêng $X_A = 5$, hãy cho biết khóa công khai của A ($Y_A$)?**
    a. 4 b. 5 c. 30 d. 51

12. **Nếu B có khóa riêng $X_B = 12$, hãy cho biết khóa công khai của B ($Y_B$)?**
    a. 4 b. 5 c. 30 d. 51

13. **Nếu A có khóa riêng $X_A = 5$ và B có khóa riêng $X_B = 12$, hãy cho biết khóa bí mật dùng chung giữa A và B($K_{AB}$)?**
    a. 4
    b. 5
    c. 30
    d. 51

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

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

**15. 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**

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

**16. 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

**17. 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

**18. 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.
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.

**19. Một môi trường Kerberos đầy đủ dịch vụ bao gồm:**
a. Một máy chủ Kerberos
b. Một máy chủ Kerberos và một số máy trạm
c. Một máy chủ Kerberos và một số máy chủ ứng dụng
d. Một máy chủ Kerberos, một số máy trạm, một số máy chủ ứng dụng

**20. Đối với Kerberos, mỗi người dùng có:**
a. Một vé TGT và một vé SGT cho tất cả các dịch vụ mà người dùng truy cập đến
b. Một vé TGT và mỗi vé SGT cho mỗi dịch vụ mà người dùng truy cập đến
c. Một vé SGT và mỗi vé TGT cho mỗi dịch vụ mà người dùng truy cập đến
d. Mỗi vé SGT và mỗi vé TGT cho mỗi dịch vụ mà người dùng truy cập đến

**21. 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)

**22. 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.

**23. Thủ tục xác thực nào được dùng để dùng cho các kết nối có tương tác ?**
a. Xác thực một chiều.
b. Xác thực hai chiều.
c. Xác thực ba chiều.
d. Cả câu (b) và (c) đều đúng.

**24. Chọn phát biểu sai trong các phát biểu sau khi PGP được sử dụng trong một hệ thống E-mail:**

a. Hệ thống E-mail nói trên sẽ cung cấp các dịch vụ xác thực, bí mật, nén, tương thích e-mail và phân mảnh.
b. Nếu dùng dịch vụ bí mật thì thông điệp gởi đi sẽ có mã hóa ở một số khối dữ liệu.
c. Nếu chỉ dùng dịch vụ xác thực thì thông điệp gởi đi sẽ không có mã hóa ở bất kỳ khối dữ liệu nào.
d. Nếu dùng dịch vụ tương thích e-mail thì mỗi nhóm 3 byte dữ liệu nhị phân được ánh xạ thành 4 ký tự ASCII.

**25. Khi cần truyền một thông điệp và dùng cả hai dịch vụ bí mật và xác thực của PGP thì phần nào sẽ được mã hóa đối xứng bằng khóa phiên?**

a. Thông điệp.
b. Tóm tắt thông điệp.
c. Chữ ký số trên thông điệp.
d. Thông điệp và chữ ký số trên thông điệp.

**26. Khóa được sử dụng để mã hóa khóa phiên trong PGP khi dùng trên hệ thống E-mail là:**

a. Khóa công khai của người gởi.
b. Khóa riêng của người gởi.
c. Khóa công khai của người nhận.
d. Khóa riêng của người nhận.

**27. Chế độ hoạt động của PGP khi thực hiện mã hóa đối xứng là:**

a. CBC
b. ECB
c. CFB
d. OFB

**28. Thuật toán mã hóa nào sau đây là phù hợp với mã hóa đối xứng của PGP:**

a. DES
b. 3DES với 2 khóa
c. AES
d. Cả câu (b) và (c) đều đúng

**29. SSL có không có khả năng chống lại loại tấn công nào sau đây:**

a. Password Sniffing
b. Man-in-the-Middle
c. Replay
d. SYN Flooding

**30. Cho biết giao thức nào sau đây không có trong SSL:**

a. SSL Message Protocol.
b. SSL Record Protocol.
c. SSL Handshake Protocol.
d. SSL Change Cipher Spec Protocol.

**31. Chọn phát biểu sai trong các phát biểu sau khi nói về kết nối SSL(SSL connection) và phiên SSL(SSL session):**

a. Một kết nối SSL có một hoặc nhiều phiên SSL.
b. Một kết nối SSL định nghĩa một bộ các tham số liên quan đến mã hóa và được chia sẻ giữa nhiềuphiên SSL.
c. Kết nối SSL được sử dụng để tránh tốn kém trong việc đàm phán các tham số liên quan đến bảo mật cho mỗi phiên SSL.
d. Các câu trên đều sai.

**32. Cho biết phát biểu sai về chữ ký đôi(dual signature) trong các phát biểu sau:**

a. Mục đích của dual signature là để liên kết hai thông điệp dành cho hai nơi nhận khác nhau.
b. Đối với giao dịch điện tử an toàn, dual signature được dùng để ký trên hai tài liệu gồm thông tin thanh toán (payment information – PO) và thông tin đặt hàng (order information – OI).
c. Đối với giao dịch điện tử an toàn, dual signature được dùng nhằm để ngân hàng không thể biết được mã băm của tài liệu đặt hàng.
d. Dual signature được dùng để ký trên hai tài liệu nối với nhau và mỗi tài liệu này có mã băm riêng.

**33. Cho biết thành phần tham gia trong giao dịch điện tử an toàn (SET- Secure Electronic Transaction) có trách nhiệm thanh toán các khoản mua hàng của chủ thẻ.**

a. Cardholder.
b. Issuer.
c. Merchant.
d. CA.

**34. Cho biết mục tiêu nào sau đây là mục tiêu thiết kế một bức tường lửa?**

a. Tất cả thông tin từ bên trong ra bên ngoài và ngược lại phải đi qua bức tường lửa.
b. Tất cả thông tin di chuyển bên trong một mạng cục bộ phải đi qua bức tường lửa.
c. Chỉ các loại thông tin được cấp quyền thông qua chính sách an ninh cục bộ mới được phép đi qua bức tường lửa.
d. Các câu (a) và (c) đều đúng.
e. Các câu (a), (b) và (c) đều đúng.

**35. Chọn phát biểu sai khi nói về bộ lọc gói (packet filter ):**

a. Nó không xem xét dữ liệu ở tầng ứng dụng trong mô hình TCP/IP.
b. Nó khôngthểngăn chặncác cuộc tấn côngsử dụngcác lỗ hổngứng dụngcụ thể.
c. Nó có khả năng phát hiện các tấn công dạng giả mạo địa chỉ ở tầng mạng
**d.** Chức năng ghi nhật ký (logging) của nó bị hạn chế.

**36. Chọn phát biểu sai trong các phát biểu sau khi nói về các loại bức tường lửa.**

a. Packet fiter quyết định lọc gói dựa trên thông tin các trường trong IP và TCP header.
b. Circuit-level gateway cho phép thiết lập một kết nối TCP end to end.
c. Application-level gateway còn được gọi là proxy server.
d. Application-level gateway an toàn hơn Packet fitering router.

**37. Cho biết cấu hình bức tường lửa nào sau đây có khả năng ngăn chặn các vi phạm an ninh mạng khi bộ lọc gói trên bộ định tuyến kết nối với Internet bị thương tổn hay đã thỏa hiệp.**

a. single-homed bastion host
b. dual-homed bastion host
c. screened subnet
d. Câu (b) và (c) đều đúng

**38. Cách thức để hạn chế tấn công SYN-Flooding trên bức tường lửa là:**
a. Cho phép nhận một lượng nhất định gói SYN trong một giây.
b. Chặn những IP kết nối thất bại nhiều lần.
c. Chỉ cho phép gói SYN trên một số port nhất định.
d. Tất cả đều đúng.

**39. Hướng phát hiện thâm nhập bất hợp pháp nào liên quan đến việc thu thập hành vi người dùng hợp pháp trong một khoảng thời gian và sau đó phân tích đánh giá:**
a. Phát hiện dựa trên thống kê
b. Phát hiện dựa trên quy tắc
c. Lai tạo
d. Các câu trên đều sai

**40. Cho biết phát biểu sai trong các phát biểu sau khi nói đến hệ thống phát hiện thâm nhập bất hợp pháp:**
a. Để xây dựng hệ thống phát hiện thâm nhập bất hợp pháp ta có hai hướng tiếp cận là rule-based detection và behavior-based detection.
b. Nếu hệ thống phát hiện một xâm nhập đủ nhanh, kẻ xâm nhập có thể được xác định trước khi bị thiệt hại.
c. Một hệ thống phát hiện thâm nhập bất hợp pháp hiệu quả có thể kết hợp với bức tường lửa để ngăn chặn ngay các xâm nhập.
d. Nó cho phép ta thu thập thông tin về các kỹ thuật xâm nhập đã được sử dụngđể tăng cường cho công tác phòng chống xâm nhập.

**41. Đối với việc khởi tạo một IDS, sau khi đã xác định mục tiêu ta phải làm gì tiếp theo?**
a. Chọn đáp ứng thích hợp
b. Xét các ngưỡng
c. Hiện thực chính sách
d. Chọn thành phần, hệ thống để theo dõi

**42. Nếu một tổ chức muốn bảo vệ một máy chủ tránh bị người dùng hợp pháp phá hoại, hệ thống phát hiện thâm nhập bất hợp phápnào là lựa chọn tốt nhất?**
a. NIDS
b. HIDS
c. Lai tạo
d. Các câu trên đều sai

**43. Nếu một tổ chức muốn phát hiện các tấn công với chi phí thấp thì hệ thống phát hiện thâm nhập bất hợp phápnào là lựa chọn tốt nhất?**
a. NIDS
b. HIDS
c. Lai tạo
d. Các câu trên đều sai

**C10:**

**44. VPN là viết tắt của:**

a. Virtual Public Network
b. Virtual Private Network
c. Virtual Protocol Network
d. Virtual Perimeter Network

**45. Lợi ích chính của VPN so với các mạng chuyên dụng như frame relay, leased line hay dial-up truyền thống là gì?**

a. Hiệu suất mạng tốt hơn
b. Ít bị lỗi hơn
c. Giảm chi phí
d. Cải thiện an ninh

**46. Trong VPN, thuật ngữ "tunneling" đề cập đến:**

e. Một tính năng tùy chọn làm tăng hiệu suất mạng.
f. Đóng gói các gói tin bên trong các gói tin của một giao thức khác để tạo và duy trì mạch ảo
g. Phương pháp quản trị hệ thống sử dụng để phát hiện tin tặc trên mạng
h. Một chiến lược tiếp thị để bán các sản phẩm VPN

**47. Những giao thức nào sau đây là giao thức VPN tunneling?**

a. PPTP
b. L2TP
c. IPSec
d. Tất các các câu trên đều đúng

**48. Khác biệt giữa Firewall và VPN là gì?**

a. Firewall có thể cấu hình còn VPN thì không cấu hình được.
b. Firewall là một loại mới của VPN.
c. Firewall chặn các thông điệp còn VPN thì mở ra con đường cho các thông điệp hợp lệ đi qua.
d. Không có khác biệt giữa Firewall và VPN.

**C11:**

**49. WEP được viết tắt là:**

Wireless Encryption Protocol
Wireless Encryption Privacy
Wired Equivalent Privacy
Wired Equivalent Protocol

**50. Điểm yếu thật sự của WEP trong vấn đề mã hóa là:**

a. Dùng thuật toán RC4
b. Dùng khóa chung quá ngắn
c. Thuật toán lập lịch khóa của RC4
d. Không xác thực người dùng

**51. Tiêu chuẩn an ninh mạnh mẽ hơn được phát triển bởi IEEE để giải quyết các lỗ hổng chuẩn WLAN IEEE 802.11 là:**

a. IEEE 802.16.2
b. IEEE 802.11e
c. IEEE 802.11i
d. IEEE 802.11n

**52. Khác biệt giữa WPA và WPA2 là:**

a. WPA mã hóa dùng RC4, WPA2 mã hóa dùng AES.
b. WPA mã hóa dùng RC4 với TKIP/MIC, WPA2 mã hóa dùng AES.
c. WPA xác thực dùng PSK, WPA2 xác thực dùng 802.1x/EAP.
d. WPA xác thực dùng ICV, WPA2 xác thực dùng 802.1x/EAP.

**53. Chọn phát biểu sai trong các phát biểu sau:**

a. WPA là một tập con của IEEE 802.11i
b. AES là mã hóa đối xứng.
c. WPA2 cho phép các client AES và TKIP được hoạt động trên cùng WLAN.
d. IEEE 802.11i thực thi an ninh trên port.

**1**. Hình thức tấn công thụ động chống lại nguyên tắc cốt lõi nào của an toàn thông tin? **Bí mật**

**2.** Tấn công DOS (Denial of Service) thuộc loại tấn công nào trong kiến trúc an ninh OSI **? Tấn công chủ động**

**3.** Cơ chế nào sau đây không cần thiết sử dụng để chống lại tấn công từ chối dịch vụ**? Mã hóa dữ liệu (encipherment).**

**On tap**

**4.** Cơ chế nào không sử dụng cho dịch vụ xác thực? **Quản lý truy cập (access control)**

**5.** biết Code Red thuộc vào loại mã độc nào sau đây: **Worm**

**6**. Hệ mã Cesar mã hóa $x \in [0; 25]$ thành $y = x + 3 \bmod 26$. Hãy cho biết nếu giá trị bản rõ là 10 thì giá trị bản mã tương ứng là: **13**

**7**. Hệ mã Affine mã hóa $x \in [0; 25]$ thành $y = 3x + 5 \bmod 26$. Hãy cho biết nếu giá trị bản mã là 10 thì giá trị bản rõ tương ứng là: **19**

**8**. Đối với mã hóa DES, trong các phát biểu sau phát biểu nào là sai? **DES sử dụng khóa có chiều dài 64 bits.**

**9**. Hệ mã Double DES(2DES) không an toàn do tấn công gì? **Tấn công "meet in the middle"**

**10**. Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt? **ECB**

**11**. Hãy cho biết kết quả của ($7^{2010} \bmod 13$): **12 . $a^{p-1} \bmod p = 1$.**

**12**. Cho biết giá trị hàm phi Euler $\phi(440)$ là: **160 . $440 = 2^3.5.11$ => $o(440) = 2^2.(2-1).4.10 = 160$.**

**13**. Hãy cho biết kết quả của ($3^{2086} \bmod 440$) : **289 . $a^{o(n)} \bmod n = 1$.**

**14**. Đối với mã hóa khóa công khai, khóa nào được sử dụng để tạo chữ ký số trên một thông điệp : Khóa riêng của người gửi

**15**. Đối với mã hóa khóa công khai, khóa nào được sử dụng để mã hóa một thông điệp : Khóa công khai của người nhận.

(Dữ liệu dùng cho câu 16 và 17)Thực hiện mã hóa và giải mã với thuật toán RSA và p = 3; q = 11, e = 7; bản mã C = 5

**16.** Giá trị của d là :**3 . Tính n = p*q = 33. o(n) = (p-1).(q-1) = 20 . Mà e.d mod o(n) = 1 => d =3**

**17.** Giá trị của bản rõ M tương ứng là: . **26 . ( $M = C^d \bmod n$ và $C = M^e \bmod n$ )**

(Dữ liệu dùng cho câu 18, 19, 20) A và B dùng kỹ thuật trao đổi khóa Diffie-Hellman với q = 71 và $\alpha = 7$.

**18**. Nếu A có khóa riêng $X_A = 5$, hãy cho biết khóa công khai của A ($Y_A$)? **51 . $Y_A = \alpha^{Xa} \bmod q$**

**19.** Nếu B có khóa riêng $X_B = 12$, hãy cho biết khóa công khai của B ($Y_B$)? **4**

**20**. Nếu A có khóa riêng $X_A = 5$ và B có khóa riêng $X_B = 12$, hãy cho biết khóa bí mật dùng chung giữa A và B($K_{AB}$)

**30 . $K = Y_A^{Xb} \bmod q = Yb^{Xa} \bmod q$**

**21**. DAA(Data Authentication Algorithm) tạo ra mã xác thực thông điệp có kích thước là: **64 bits**

**22**. 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 : **64**

**23**. Mã xác thực thông điệp dựa trên hàm băm MD5 tạo ra mã xác thực thông điệp có kích thước là : **c.128 bytes**

**24**. 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**

**25**. 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**

**26**. Hướng phát hiện thâm nhập bất hợp pháp nào liên quan đến việc thu thập hành vi người dùng hợp pháp trong một khoảng thời gian và sau đó phân tích đánh giá:

**a. Phát hiện dựa trên thống kê** b. Phát hiện dựa trên quy tắc. c. Lai tạo. d. Các câu trên đều sai

**27.** Cho biết phát biểu sai trong các phát biểu sau khi nói đến hệ thống phát hiện thâm nhập bất hợp pháp:

**Nếu hệ thống phát hiện một xâm nhập đủ nhanh, kẻ xâm nhập có thể được xác định trước khi bị thiệt hại**

**28**. Đối với việc khởi tạo một IDS, sau khi đã xác định mục tiêu ta phải làm gì tiếp theo?

a. Chọn đáp ứng thích hợp b. Xét các ngưỡng

c. Hiện thực chính sách **d. Chọn thành phần, hệ thống để theo dõi**

**29.** Nếu một tổ chức muốn bảo vệ một máy chủ tránh bị người dùng hợp pháp phá hoại, hệ thống phát hiện thâm nhập bất hợp pháp nào là lựa chọn tốt nhất?

a. NIDS **b. HIDS** c. Lai tạo. d. Các câu trên đều sai.

**30.** Nếu một tổ chức muốn phát hiện các tấn công với chi phí thấp thì hệ thống phát hiện thâm nhập bất hợp pháp nào là lựa chọn tốt nhất?

**a. NIDS** b.HIDS c.Lai tạo d.Tất cả đều sai

**31.** Một môi trường Kerberos đầy đủ dịch vụ bao gồm :

a.Một máy chủ Kerberos

b.Một máy chủ Kerberos và một số máy trạm

c.Một máy chủ Kerberos và một số máy chủ ứng dụng

**d.Một máy chủ Kerberos, một số máy trạm, một số máy chủ ứng dụng**

**32**. Đối với Kerberos, mỗi người dùng có:

a.Một vé TGT và một vé SGT cho tất cả các dịch vụ mà người dùng truy cập đến

**b.Một vé TGT và mỗi vé SGT cho mỗi dịch vụ mà người dùng truy cập đến**

c.Một vé SGT và mỗi vé TGT cho mỗi dịch vụ mà người dùng truy cập đến

d.Mỗi vé SGT và mỗi vé TGT cho mỗi dịch vụ mà người dùng truy cập đến

**33.** 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)

**34.** 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.**

**35.**Thủ tục xác thực nào được dùng để dùng cho các kết nối có tương tác ?

a.Xác thực một chiều. b.Xác thực hai chiều. c.Xác thực ba chiều. **d.Cả câu (b) và (c) đều đúng**

**36.** Chọn phát biểu sai trong các phát biểu sau khi PGP được sử dụng trong một hệ thống E-mail:

a.Hệ thống E-mail nói trên sẽ cung cấp các dịch vụ xác thực, bí mật, nén, tương thích e-mail và phân mảnh.

b.Nếu dùng dịch vụ bí mật thì thông điệp gởi đi sẽ có mã hóa ở một số khối dữ liệu.

**c.Nếu chỉ dùng dịch vụ xác thực thì thông điệp gởi đi sẽ không có mã hóa ở bất kỳ khối dữ liệu nào.**

d.Nếu dùng dịch vụ tương thích e-mail thì mỗi nhóm 3 byte dữ liệu nhị phân được ánh xạ thành 4 ký tự ASCII

**37.** Khi cần truyền một thông điệp và dùng cả hai dịch vụ bí mật và xác thực của PGP thì phần nào sẽ được mã hóa đối xứng bằng khóa phiên ?

a.Thông điệp. b.Tóm tắt thông điệp.

c.Chữ ký số trên thông điệp. **d.Thông điệp và chữ ký số trên thông điệp**

**38.** Khóa được sử dụng để mã hóa khóa phiên trong PGP khi dùng trên hệ thống E-mail là:

a.Khóa công khai của người gởi. b.Khóa riêng của người gởi.

**c.Khóa công khai của người nhận.** d.Khóa riêng của người nhận

**39.** Chế độ hoạt động của PGP khi thực hiện mã hóa đối xứng là: **CFB**

**40.** Thuật toán mã hóa nào sau đây là phù hợp với mã hóa đối xứng của PGP: **3DES với 2 khóa và AES**

**41.** SSL có không có khả năng chống lại loại tấn công nào sau đây: **SYN flooding**

**42.** Cho biết giao thức nào sau đây không có trong SSL: **SSL message protocol**

**43.** Chọn phát biểu sai trong các phát biểu sau khi nói về kết nối SSL(SSL connection) và phiên SSL(SSL session):

a.Một kết nối SSL có một hoặc nhiều phiên SSL.

b.Một kết nối SSL định nghĩa một bộ các tham số liên quan đến mã hóa và được chia sẻ giữa nhiều phiên SSL.

c.Kết nối SSL được sử dụng để tránh tốn kém trong việc đàm phán các tham số liên quan đến bảo mật cho mỗi phiên SSL.

**d.Các câu trên đều sai**

**44.** Cho biết phát biểu sai về chữ ký đôi(dual signature) trong các phát biểu sau:

**Đối với giao dịch điện tử an toàn, dual signature được dùng nhằm để ngân hàng không thể biết được mã băm của tài liệu đặt hàng**

**45.** Cho biết thành phần tham gia trong giao dịch điện tử an toàn (SET- Secure Electronic Transaction) có trách nhiệm thanh toán các khoản mua hàng của chủ thẻ: **Issuer**

**46.** Cho biết mục tiêu nào sau đây là mục tiêu thiết kế một bức tường lửa? 2 mục tiêu

**Tất cả thông tin từ bên trong ra bên ngoài và ngược lại phải đi qua bức tường lửa**

**Chỉ các loại thông tin được cấp quyền thông qua chính sách an ninh cục bộ mới được phép đi qua bức tường lửa**

**47.** Chọn phát biểu sai khi nói về bộ lọc gói (packet filter ):

**Nó có khả năng phát hiện các tấn công dạng giả mạo địa chỉ ở tầng mạng**

**48**. Chọn phát biểu sai trong các phát biểu sau khi nói về các loại bức tường lửa.

**Circuit-level gateway cho phép thiết lập một kết nối TCP end to end** (thực sự có 2 kết nối)

**49.** Cho biết cấu hình bức tường lửa nào sau đây có khả năng ngăn chặn các vi phạm an ninh mạng khi bộ lọc gói trên bộ định tuyến kết nối với Internet bị thương tổn hay đã thỏa hiệp? **screened subnet và dual-homed bastion host**

**50.** Cách thức để hạn chế tấn công SYN-Flooding trên bức tường lửa là:

a. Cho phép nhận một lượng nhất định gói SYN trong một giây

b. Chặn những IP kết nối thất bại nhiều lần

c. Chỉ cho phép gói SYN trên một số port nhất định

**d. Tất cả đều đúng**

**51**.VPN là viết tắt của: **Virtual Private Network**

**52**.Lợi ích chính của VPN so với các mạng chuyên dụng như frame relay,leased line hay dial-up truyền thống là gì

a. Hiệu suất mạng tốt hơn b.Ít bị lỗi hơn **c.Giảm chi phí** d.Cải thiện an ninh

**53**.Trong VPN thuật ngữ "tunneling" đề cập đến: **Đóng gói các gói tin bên trong các gói tin của một giao thức khác để tạo và duy trì mạch ảo**

**54**.Những giao thức nào sau đây là giao thức VPN tunneling

a.PPTP b.L2TP c.IPSec **d. Tất cả đều đúng**

**55.** Khác biệt giữa Firewall và VPN là gì : **Firewall chặn các thông điệp còn VPN thì mở đường cho các thông điệp hợp lệ đi qua.**

**56**.WEP được viết tắt của**: Wired Equivalent Privacy**

**57.**Điểm yếu thật sự của WEP trong vấn đề mã hóa là: **Thuật toán lập trình khóa của RC4**

**58.**Tiêu chuẩn an ninh mạnh mẽ hơn được phát triển bởi IEEE để giải quyết các lỗ hổng chuẩn WLAN IEEE 802.11 là : **IEEE 802.11 1i**

**59.**Khác biệt giữa WPA và WPA2 là : **WPA mã hóa dùng RC4 với TKIP/MIC, WPA2 mã hóa dùng AES.**

**60.**Chọn phát biểu sai trong các phát biểu sau:

a.WPA là một tập con của IEEE 802.1 1i b.AES là mã hóa đối xứng

c.WPA2 cho phép các client AES và TKIP được hoạt động trên cùng WLAN **d.IEEE 802.1 1i thực thi an toàn trên port**

**---**

Chế độ nào của IPSec không bảo vệ IP header : **Transport**

Các giao thức được thiết kế bởi IETF nào an toàn cho gói dữ liệu ở tầng mạng trong mô hình OSI : **IPSec** ,

Tham số nào của sự kết hợp bảo mật SA gồm các thông số xác thực,khóa, và thời gian sống của khóa : **AH Information, ESP Information**

Giao thức IKE tạo các kết hợp bảo mật nào sau đây :**SSL và IPSec**

SSL không cung cấp dịch vụ nào sau đây : **Compresion ( key point**)

Giao thức nào của IPSec cung cấp dịch vụ xác thực và mã hóa thông tin trong Internet trong mô hình TCP/IP: **ESP**

**Trac nghiem an ninh mang**
**03/04/2010 16:00**
**Đinh Xuân Dụy**

# *TRƯỜNG KHÁC*

1.Yêu cầu  để đảm bảo sử dụng mã  hóa đối xứng là
a.Có thuật tóan encryption tốt,có một khóa bí mật được biết bởi người nhận/gởi  và kênh truyền bí mật  để phân phát key
b.Có một kênh truyền phù hợp và một khóa bí mật được biết bởi người nhận/gởi
c.Có thuật tóan encryption tốt và có một khóa bí mật được biết bởi người nhận/gởi
d.Tất cả đều đúng
2.Các thuật tóan nào sau đây là thuật tóan mã  hóa đối xứng
a.Triple –DES, RC4, RC5, Blowfish
b.Triple –DES, RC4, RC5, IDEA
c.RC4, RC5, IDEA, Blowfish
d.IDEA, Blowfish, AES, Elliptic Cure
3.Các phát biểu sau đây phát biểu nào đúng
a. Hầu hết các thuật tóan mã hóa đối xứng đều dựa trên cấu trúc thuật tóan Feistel
b.Tấn công thông điệp thì thời gian giải mã tỷ lệ với kích thước khóa
c.Hầu hết các thuật tóan mã hóa khối đều đối xứng
d.Tất cả đều đúng
**4.Cơ  chế bảo mật SSL hoạt  động trên tầng**
**a.Network, Transport**
b.Network, Session
c.Application, Session
d.Tất cả đều sai
**5.Keberos là  dịch vụ ủy thác**
a. Xác thực trên Web
b. Xác thực X.509
c. Xác thực trên Server
d. Xác thực trên các máy trạm với nhau
**6.PGP là  giao thức để xác thực**
a. Quyền đăng cập vào hệ thống máy chủ Window
b. Bảo mật cho thư  điện tử
c. Thực hiện mã hóa thông điệp theo thuật tóan RSA
d. Địa chỉ của máy trạm khi kết nối vào Internet
**7. Công cụ/cơ chế bảo mật cho mạng không dây là**
a. SSL
b. TSL
c. Giao thức PGP
d. WEP
**8. Giao thứ  SSL và TSL hoạt động ở tầng nào của mô  hình OSI**
a. Network
b. Sesion

c. Transport
d. **Từ tầng Trasport trở lên**
**9. Giao thức SSL dùng để**
a. Cung cấp bảo mật cho dữ liệu lưu thông trên dịch vụ HTTP
b. Cung cấp bảo mật cho thư điện tử
c. **Cung cấp bảo mật cho Web**
d. Cung cấp bảo mật cho xác thực người dùng vào các hệ thống vận hành trên Flatform Window
**10.Chức năng chính của Virus là**
a. Lây nhiễm và sinh sản
b. Sống ký sinh và lây nhiễm
c. Tự phát triển độc lập và lây nhiễm
**d. Tất cả đều đúng**
**11.Hoạt động của virus có 4 giai đoạn**
a. Nằm im, lây nhiễm, tàn phá và tự hủy
b. Lây nhiễm, tấn công, hủy diệt và tự hủy
**c. Nằm im, lây nhiễm, khởi sự và tàn phá**
d. Lây nhiễm, khởi sự, tàn phát, kích hoạt lại
**12.Các dạng sau đây, dạng nào là của virus**
a.sealth, cư trú bộ nhớ, macro, đa hình, file
b.stealth, cư trú bộ nhớ, macro, lưỡng tính, file
c.virus ký sinh, file, boot secctor, stealth, cư trú bộ nhớ, macro
**d.virus ký sinh, cư trú bộ nhớ, boot secctor, Stealth, đa hình, macro**
**13. Virus Macro chỉ có khả năng tấn công vào các file**
a. MS.Exel, MX Word, MS.Outlook Mail
**b. MS.Exel, MX Word, MS.Power Point**
c. MS.Exel, MX Word,Yahoo Mail
d.Tất cả các loại file
**14. Các giao thức bảo mật trên Internet như SSL, TLS và SSH hoạt động ở tầng nào trên mô hình OSI**
a.Tầng Network
b.Tầng Transport
**c.Từ tầng Transport trở lên đến tầng 7**
d.Tầng Session
**15. Kỹ thuật tấn công phổ biến trên Web là**
a. Chiếm hữu phiên làm việc.
b.Tràn bộ đệm.
**c.Từ chối dịch vụ (DoS)**
d.Chèn câu truy vấn SQL.
**16. Các lỗ hổng bảo mật trên hệ thống là do**
a. Dịch vụ cung cấp
b. Bản thân hệ điều hành
c. Con người tạo ra
**d. Tất cả đều đúng**

**17. Cho biết câu nào đúng trong các câu sau**

a. Tất cả Firewall đều có chung thuộc tính là cho phép phân biệt hay đối xử khả năng từ chối hay truy nhập dựa vào địa chỉ nguồn

b. Chức năng chính của Firewall là kiểm sóat luồng thông tin giữa mạng cần bảo vệ và Internet thông qua các chính sách truy nhập đã được thiết lập

c. Hệ thống Firewall thường bao gồm cả phần cứng lẫn phần mềm

**d. Tất cả đều đúng**

**18. Loại Firewall nào sau đây cho phép hoạt động ở lớp phiên ( session) của mô hình OSI**

a. Packet filtering firewall

b. Circuit level firewall

c. Application level firewall

**d. Stateful multilayer inspection firewall**

**19.Những giao thức WAN nào có thể được định hình trên một kết nối tuần tự không đồng bộ (Chọn 2)**

a. PPP

b. ATM

c. HDLC

d. SDLC

**20. Khi thuê một giải pháp VPN, những loại tấn công nào bạn cần phải xét đến ?**

a. Denial of Service (DoS) attacks, Internet Viruses..

b. Distributed Denial of Service (DDoS) attacks.

c. Data confidentiality, IP Spoofing.

**d. Network mapping, Internet Viruses.**

**21. Các phát biểu sau đây phát biểu là là đúng nhất**

a.Fire wal là một vành đai phòng thủ cho máy tính hoặc hệ thống trước những tấn công

**b.Là một điểm chặn của trong quá trình điều khiển và giám sát.**

c. Là một phần mềm hoặc phần ứng có khả năng ngăn chặn tấn công từ bên trong và bên ngoài vào hệ thống.

d.Là một giải pháp giúp hệ thống phát hiện và ngăn chặn các truy cập trái phép

**22. Bảo mật thư điện tử là nhằm đảm bảo**

**a.Tính tin cẩn (confidentiality), Tính xác nhận,Toàn vẹn thông điệp(integrity), Sự thối thác ban đầu (non-repudiation of origin)**

b. Tính xác nhận,Toàn vẹn thông điệp(integrity), Sự thối thác ban đầu (non-repudiation of origin), tính bền vững

c.Sự thối thác ban đầu (non-repudiation of origin), tính bền vững, tính ổn khi gởi và nhận

d.Tất cả đều đúng

23. Các giao thức được để bảo mật thư điện tử là

a.GPG, S/MINE

b.SHA-1, S/MINE

**c.CAST-128 / IDEA/3DES**

d. Keboros, X.509

24. Chữ ký điện tử (digital signature) sử dụng thuật tóan nào sau đây

a. RSA,MD5

b. RSA,MD5, Keboros

**c. MD5, SHA,RSA**

d.Không dùng thuật tóan nào nêu trên

**25. Chữ ký điện tử là**

**a.Là một chuỗi đã được mã hóa theo thuật tóan băm và đính kèm với văn bản gốc trước khi gởi.**

b.Đoạn dữ liệu ngắn đính kèm với văn bản gốc để chứng thực tác giả của văn bản và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc.

c.a và b đều đúng

d.Tất cả cả đều sai

**26. Các bước mã hóa của chứ ký điện tử**

**a.Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, Sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên, sau đó gộp digital signature vào message ban đầu.**

b.Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên, sau đó gộp digital signature vào message ban đầu và nén dữ liệu gởi đi.

c.Chỉ sử dụng giải thuật băm để thay đổi thông điệp cần truyền đi và sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên.

d.Tất cả đều đúng

27. Các bước kiểm tra của chứ ký điện tử

**a. Gồm các bước**

**1.Dùng public key của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của message,**

**2.Dùng giải thuật (MD5 hoặc SHA) băm message đính kèm, So sánh kết quả thu được ở bước 1 và 2.**

**3.Nếu trùng nhau, ta kết luận message này không bị thay đổi trong quá trình truyền và message này là của người gửi.**

b.Chỉ có bước 1 và 2

c.Gồm các bước

1.Dùng public key của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của message,

2.Dùng giải thuật (MD5 hoặc SHA) băm message đính kèm, So sánh kết quả thu được ở bước 1 và 2.

3.Nén dữ liệu rồi gởi đi

d.Không có bước nào ở trên là đúng

**28. Việc xác thực người dùng khi đăng cập vào hệ thống Window XP, 2000 hoặc 2003 sử dụng giải thuật**

a.RSA

b.Keberos

c.MD5

**d.SHA**

**29. Để thực hiện tấn công bằng Trojan, kẻ tấn công chỉ cần**

**a.Tạo 1 file chạy (*.exe, *.com) vận hành trên máy nạn nhân là đủ**

b. Cho máy nạn nhân lây nhiễm một loại virus bất kỳ nào đó.

c. Thực hiện đồng thời 2 file, một file vận hành trên máy nạn nhân, file còn lại hoạt động điều khiển trên máy kẻ tấn công.

d. Không có điều nào đúng.

**30. Giao thức bảo mật IPSec hoạt động ở tầng**

a. Chỉ ở tầng transport ở mô hình OSI

b.Từ tầng 4 tới tầng 7 ở mô hình OSI

**c.Network Layer ở mô hình OSI**

d.Tất cả đều sai

**31. Cho biết phát biểu sau đây phát biểu nào là đúng nhất về registry**

**a.Regỉstry là một cơ sở dữ liệu dùng để lưu trữ thông tin về những sự thay đổi, những lựa chọn, những thiết lập từ người sử dụng Windows.**

b.Regỉstry là một phần mềm tiện ích hỗ trợ cho người dùng thay đổii cấu hình Window khi cần thiết

c. Regỉstry là một thành phần của hệ điều hành Window

d. Tất cả đều đúng

**32.Có bao nhiêu kiểu dữ liệu trong Registry**

a. 5 b. 4 c. 6 d. 7

33. Các kiểu dữ liệu dùng trong registry là

a.interger, real,text,string

b.HKEY_CLASSES_ROOT, -USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG, HKEY_DYN_DATA

c.HKEY_CLASSES_ROOT, -USER, HKEY_LOCAL_MACHINE, REG_BINARY

d.REG_BINARY, REG_DWORD, REG_EXPAND_SZ, REG_MULTI_SZ, REG_SZ

34. Để ẩn tất cả các ổ đĩa trong registry (A,B,C,D…) thì biến REG_DWORD trong Userkey và Systemkey có giá trị là bao nhiêu

a. 65656000

b. 67188270

c. 67108863

d.Tất cả đều sai

35. Để sử dụng xác thực Keberos V5 ở tất cả máy trạm Window98, người ta thực hiện :

a. Update window 98 lên XP hoặc Window 2000

b. Cài đặt tiện ích Distributed Security Client trên tất cả các máy chạy Window 98

c. Chỉ cần cài đặt Active Directory trên Server hệ thống

d. Không thể thực hiện được

36. Khi cài đặt Window 2000 Server trên hệ thống NTFS, nhưng không thấy có hiển thị mục Security ở Security tables vì ?

a. Update Window 2000 mà không remote trước khi cài đặt

b. Cài đặt Window 2000 nhiều lần trên Server

c. Bản Window 2000 không có bản quyền

d. Tất cả đều đúng
37. Dịch vụ  Active Directory thực hiện các chức năng sau
a. Tổ chức và  xây dựng các domain; xác thực và cấp quyền cho các  đối tượng
b. Duy các hoạt động của các dịch vụ bảo mật cho Window Server và xác thực, cấp quyền cho các đối tượng
c. Chỉ thực hiện việc xác thực và cấp các quyền cho users và groups
d. Quản lý tài nguyên và người dùng; xác thực và cấp các quyền cho users và groups; giám sát hoạt động của các user
38. Thuật tóan thực hiện trong cơ chế bảo mật IP (IP Sec) ở Window sử dụng là
*a.MD5 và SHA1*
b. Kerberos và DES
c. DES hoặc 3DES (triple DES).
d.Tất cả đều sai
39.  Trong Window 98,XP Registry được lưu trữ ở đâu ?
a.Được lưu trong file Classes.dat trong thư mục Windows
b.Được lưu trong thư  mục "Windows System32 Config
c.Trong 2 file: user.dat và system.dat trong thư mục Windows
d.Tất cả đều sai
40. Để thực hiện sửa đổi cấu hình trên registry ta thực hiện như sau:
a. Gõ regedit vào cửa sổ Run
b. Bấm Ctrl+ Esc+ r  rồi bấm Enter
c. a và b đúng
d.Tất cả đều sai
41.Quy trình crack một sản phẩm phần mềm đơn giản gồm mấy bước
a. 3  b.4  c.5  d.3 hoặc 4
**42. Hai giao thức  sử dụng trong IPSec (IPSec Protocol) gồm**
a.IP Authentication Header, TCP/IP
b.TCP/IP, IP Encapsulating Security Payload
**c.IP Authentication Header, IP Encapsulating Security Payload**
d.Tất cả đều đúng
43. Các  điểm khác nhau cơ bản giữa dịch vụ  X.509 và Kerberos là
**a. Dựa trên mã hóa  đối xứng**
b. Được sử dụng trong dịch vụ mail
c. Xác thực nhiều chiều
d. Tất cả đều đúng
44. Các chức năng cơ bản của kỹ thuật tấn công Sniffer
a. Tự động chụp các tên người sử dụng (Username) và mật khẩu không được mã hoá, Chuyển đổi dữ liệu trên đường truyền, phân tích những lỗi đang mắc phải trên hệ thống lưu lượng của mạng.
b. Bắt gói tin trên  đường truyền, phân tích lỗi và giải mã gói tin
c.  Bắt gói tin trên  đường truyền, mã hóa vag giải mã dữ liệu
d.Tất cả đều đúng
45. Các bước tấn công của Web Server theo trình tự  sau :
a. Thăm dò, Scan, Giành quyền truy cập, Duy trì truy cập, Xóa vết

**b. Scan, Thăm dò, Giành quyền truy cập, Duy trì truy cập, Xóa vết**

c. Thăm dò, Scan, Duy trì truy cập, Giành quyền truy cập, Xóa vết

d. Giành quyền truy cập, Duy trì truy cập, Scan, Thăm dò

**46. Hiện tượng này do loại chương trình nguy hiểm nào gây ra : Làm mất một số file, làm phân mãnh ổ đĩa, gây tác hại vào những ngày, tháng đặc biệt v.v…**

a. Virrus,Zombie b. Worm, Virus **c. Logicbomb, Virus** d.Trapdoors, Trojan

47.Để đánh giá điểm mạnh của hệ thống IDS người ta dựa vào các yếu tố sau :

a.Khởi sự, Cách thực hiện, biểu hiện mà nó ghi nhận

b.Khởi sự, giám sát vị trí, những đặc trưng ghép nối hoặc tích hợp

c. Cách thực hiện, biểu hiện mà nó ghi nhận, những đặc trưng ghép nối hoặc tích hợp

d.Tất cả đều đúng

48. Hai cơ chế chính của hệ thống IDS Trigger để phát hiện khi có một kẻ xâm nhập tấn công mạng là :

**a.Phát hiện biểu hiện không bình thường, phát hiện sử dụng không đúng**

b.Phát hiện hiện tượng trùng lặp, phát hiện không bình thường

c. Phát hiện thay đổi, phát hiện sử dụng bất bình thường

d.Tất cả đều đúng

49.Mục tiêu là phân tích mật mã là gì?

**a. Để xác định thế mạnh của các thuật toán một**

b. Để tăng cường chức năng thay thế trong một thuật toán mật mã

c. Để giảm chức năng transposition trong một thuật toán mật mã

d. Để xác định hoán vị sử dụng

50. Điều gì sẽ xãy ra khi một thông báo đã được sửa đổi?

a. Khoá công cộng đã được thay đổi

b. Chìa khóa cá nhân đã được thay đổi

c. Thông điệp số đã được thay đổi

d.Tin nhắn đã được mã hóa đúng cách

51.Mà hóa nào sau đây là một tiêu chuẩn dùng để phát triển cho việc tạo ra thông điệp an toàn?

a. Data Encryption Standard

**b. Digital Signature Standard**

c. Secure Hash Algorithm

d. Chữ kí dữ liệu tiêu chuẩn

52.Nếu kẻ tấn công lấy trộm một mật khẩu có chứa một chiều mật khẩu đã mật mã, loại tấn công, cô sẽ thực hiện để tìm mật khẩu đã mật mã?

a. Tấn công Man-in-the-middle

**b. Tấn công Birthday**

c. Tấn công Denial of Service

d. Tấn công Dictionary

53.Lợi thế của RSA là gì so với DSS?

**a.Nó có thể cung cấp cho chữ ký số và mã hóa các chức năng**

b.Nó sử dụng nguồn tài nguyên ít hơn và mã hóa nhanh hơn bởi vì nó sử dụng các phím đối xứng

c.Nó là một thuật toán mật mã khối so với một thuật toán mật mã dòng

d.Nó sử dụng một lần mã hóa pad

54.Những gì được sử dụng để tạo ra một chữ ký điện tử?
a. Khóa riêng của người nhận
b. Khóa công khai của người gửi
**c. Khóa riêng của người gửi**
d. Khóa công khai của người nhận
55. Phương thức nào sau đây là tốt nhất mô tả một chữ ký điện tử?
a. Một phương thức chuyển giao một chữ ký viết tay vào một tài liệu điện tử
b. Một phương pháp mã hóa thông tin bí mật
c. Một phương pháp để cung cấp một chữ ký điện tử và mã hóa
**d. Một phương pháp để cho những người nhận của tin nhắn chứng minh nguồn gốc và sự toàn vẹn của một tin nhắn**
**56. Sử dụng nhiêu bit với DES để có hiệu quả?**
**a.56** b.64 c.32 d.16
**57.Các yếu tố ảnh hưởng đến quá trình mã hóa**
**a. Thuật toán mã hóa, giải mã, và tính an toàn của kênh truyền**
b. Thời gian thực hiện mã hóa và giải mã
c. Thực hiện mã hóa khối, mở rộng số bít xử lý
d. Tất cả đều sai
**58. Đối với Firesall lọc gói, hình thức tấn công nào sau đây được thực hiện**
a. Nhái địa chỉ IP, tấn công giữa, tấn công biên
**b. Nhái địa chỉ IP, tấn công đường đi nguồn, tấn công từng mẫu nhỏ**
c. Nhái địa chỉ IP, tấn công vượt firewall,tấn công từng mẫu nhỏ
d. Nhái địa chỉ IP, tấn công vượt firewall, tấn công đường đi nguồn
**59.Ai là người tham gia vào việc phát triển đầu tiên hệ thống mã hóa khóa công?**
a. Adi Shamir
b. Ross Anderson
c. Bruce Schneier
**d. Martin Hellman**
**60. DES là viết tắt của từ nào ?**
a. Data encryption system
**b. Data encryption standard**
c. Data encoding standard
d. Data encryption signature
**61. Các phát biểu sau đây, phát biểu nào tốt nhất mô tả một hacker mũ trắng?**
**A. Chuyên gia bảo mật**
B. Cựu Hacker mũ đen
C. Cựu Hacker mũ xám
D. Hacker hiểm độc
**62. Giai đoạn đầu của hacking là gì?**
A. Duy trì truy cập
B. Gaining truy cập
C. Trinh sát
**D. Dò tìm (Scanning)**

**63. Khi một hacker cố gắng tấn công một máy chủ qua Internet nó được gọi là loại tấn công?**

**A. Tấn công  từ xa**

B. Tấn công truy cập vật lý

C. Truy cập  địa phương

D. Tấn công tấn công nội

**64. Công cụ nào sau đây đúng là một công cụ để thực hiện footprinting không bị phát hiện?**

**A. Whois search**

B. Traceroute

C. Ping sweep

D. Host scanning

**65. Bước tiếp theo sẽ được thực hiện sau khi footprinting là gì?**

A. Scanning

**B. Enumeration**

C. System hacking

D. Active information gathering

**66. Footprinting là gì**?

A. đo dấu vết của một hacker có đạo đức

**B. tích luỹ dữ liệu bằng cách thu thập thông tin về một mục tiêu**

C. quét một mạng lưới mục tiêu để phát hiện hệ điều hành các loại

D. sơ đồ bố trí vật lý của một mạng của mục tiêu

67. Lý do tốt nhất để thực hiện một chính sách bảo mật là gì?

**A. Tăng an ninh.**

B. Nó làm cho khó hơn việc thi hành bảo mật.

C. Hạn chế quyền hạn của nhân viên

D. Làm giảm an ninh.

68. FTP sử dụng cổng gì ?

**A. 21**

B. 25

C. 23

D. 80

69. Cổng nào được HTTPS sử dụng?

**A. 443**

B. 80

C. 53

D. 21

70. Trojan Horse là gì?

**A. một chương trình độc hại mà lấy cắp tên người dùng và mật khẩu của bạn**

B. gây hại như mã giả mạo hoặc thay thế mã hợp pháp

C. Một người sử dụng trái phép những người thu truy cập vào cơ sở dữ liệu người dùng của bạn và cho biết thêm mình như một người sử dụng

D. Một máy chủ đó là phải hy sinh cho tất cả các hacking nỗ lực để đăng nhập và giám sát các hoạt động hacking

71. John muốn cài đặt một ứng dụng mới vào máy chủ của Windows 2000.
Ông muốn đảm bảo rằng các ứng dụng bất kỳ ông sử dụng chưa được cài Trojan.
Ông có thể làm gì để giúp đảm bảo điều này?
**A. So sánh chữ ký MD5 của tập tin với một trong những công bố trên các phương tiện truyền thông phân tán**
B. Xin các ứng dụng thông qua SSL
C. So sánh chữ ký virus của file với một trong những công bố trên các phương tiện truyền thông
D. Cài đặt các ứng dụng từ đĩa CD-ROM
72. Hầu hết các lỗi SQL Injection đều là do (chọn 2 phương án)
**a. câu lệnh SQL sai**
b. trình duyệt Web không hỗ trợ
**c. User làm cho câu lệnh SQL sai**
d. Sử dụng Hệ quản trị CSDL không có bản quyền
73. Chính sách bảo mật là
a. Cơ chế mặc định của hệ điều hành
b. phương thức xác định các hành vi "phù hợp" của các đối tượng tương tác với hệ thống
**c. các tập luật được xây dựng nhằm bảo vệ các tấn công bất hợp pháp từ bên ngoài**
d. Tất cả đều đúng
74. Các loại mục tiêu của chiến tranh thông tin
a. Website, E-commerce server
b. Internet Relay Chat (IRC), Domain Name System (DNS)
c. ISP, Email server
**d. Tất cả đều đúng**
75. Khi thực hiện triển khai HIDS khó khăn gặp là
**a. Chi phí lắp đặt cao, khó bảo quản và duy trì**
b. Giới hạn tầm nhìn mạng, phải xử lí với nhiều hệ điều hành khác trên mạng.
c. Thường xuyên phải cập nhật bảng vá lỗi
d. Thường xuyên cài đặt lại phải khi hệ thống mạng thay đổi hệ điều hành

# GIUA KY 2010

Đề thi giữa kì I mật mã & an ninh mạng 2010 (time: 30', khong tai lieu)

1) Cơ chế nào không sử dụng cho việc chống lại từ chối dịch vụ (Deny of Service)
   a. Mã hóa
   b. Quản lý định tuyến (routing control)
   c. Trao đổi xác thực
   d. Quản lý truy cập (access control)
2) Cơ chế nào không sử dụng cho xác thực
   a. Mã hóa
   c. Chữ kí số
   b. Trao đổi xác thực
   d. Quản lý truy cập
3) Tấn công Deny of Service (DOS) thuộc loại nào sau đây
   a. Remote control
   c. Active control
   b. Passive control
   d. Tất cả đều sai
4) Mã hóa thay thế một kí tự bằng một kí tự khác thuộc loại nào
   a. Transposition
   c. Polyanlphabetic substitution
   b. Monoalphabetic substitution
   d. Tất cả đều sai

Xét hàm affine cipher sau $y = k_1x + k_2 \pmod{256}$ với $x \in [0, 255]$, $0 \leq k_1, k_2 \leq 255$, x, $k_1$, $k_2$ là số nguyên. Một yêu cầu đối với hàm mã hóa là ánh xạ một một.

5) Với giá trị nào của $k_1$ thì khóa ($k_1$, $k_2$) hợp lệ
   a. 2
   c. 14
   b. 8
   d. Tất cả đều sai
6) Có tất cả bao nhiêu khóa hợp lệ:
   a. 128
   c. 32768
   b. 256
   d. 65536
7) Tính số dư khi chia $7^{2010}$ cho 13
8) Tính output bit thứ 1 và 16 của vòng thứ nhất của DES decryption. Giả sử ciphertext và key gồm toàn bit 1.
   a. 0, 0
   c. 0, 1
   b. 1, 0
   d. 1, 1
9) Chọn phát biểu sai về DES → key 64 bit
10) Tính $\phi(440)$
11) Tìm phần dư $3^{2086} \bmod 440$
12) Trong mã hóa công khai, khóa nào được sử dụng để tạo chữ kí số
13) Trong mã hóa công khai, khóa nào được sử dụng khi mã hóa data trước khi gửi.

Trao đổi key Diffie-Hellman, cho q = 71, a = 7

14) Nếu A có khóa riêng là $X_A = 5$, khóa công khai của A ($Y_A$) là
15) Nếu B có private key $X_B = 12$, public key của B ($Y_B$) là
16) Nếu A, B có khóa riêng lần lượt là 5 và 12 thì khóa bí mật dùng chung là

Mã hóa RSA, p = 3, q = 11, e = 7, C = 5

17) d = ?
18) M = ?
19) Các hướng tiếp cận xác thực thông điệp
   a. Mã hóa
   d. b, c đúng
   b. Hash function
   e. a, b, c đều đúng
   c. Mã xác thực thông điệp
20) Cần thay đổi bao nhiêu chỗ trong 1 văn bản cho trước (nhằm tạo ra các phiên bản) sao cho xác suất tồn tại 2 phiên bản có giá trị hash như nhau là 0.5 nếu hash có chiều dài 128 bit
   a. 128
   c. $2^{128}$
   b. 64
   d. $2^{64}$