CÂU HỎI ÔN TẬP HỌC PHẦN

BẢO MẬT THÔNG TIN

Mã học phần: 0101001455 **Bộ môn: KHOA HỌC MÁY TÍNH**

Số tín chỉ: 2

Hình thức thi: Trắc nghiệm **Thời gian thi: 60 phút**

Đề thi gồm: 40 câu

Không được sử dụng tài liệu

NỘI DUNG

Chương 1: Giới thiệu
Chương 2: Mã hóa đối xứng cổ điển
Chương 3: Mã hóa đối xứng hiện đại
Chương 4: Mật mã khóa công khai
Chương 5: Xác thực và chữ ký số
Chương 6: An toàn thư điện tử
Chương 7: An toàn IP
Chương 8: An toàn Web

Chương 1: Giới thiệu về Bảo Mật Thông Tin

1. An toàn hệ thống thông tin là gì? Hãy giải thích các thuộc tính an ninh cơ bản cần đảm bảo trong một hệ thống thông tin.
2. Bảo mật thông tin khác với an toàn thông tin như thế nào? Hãy nêu ví dụ minh họa cho từng khái niệm.
3. Trình bày các phương pháp bảo mật thông tin trên máy tính. Vì sao việc bảo vệ thông tin trên máy tính trở nên quan trọng trong thời đại công nghệ số?
4. Phân biệt giữa an toàn hệ thống và an toàn thông tin. Đưa ra các yếu tố cần thiết để đảm bảo mỗi loại an toàn này.
5. Theo bạn, "an toàn" trong lĩnh vực bảo mật thông tin có nghĩa là gì? Hãy giải thích với ví dụ thực tiễn.
6. Trình bày khái niệm an toàn máy tính và mối quan hệ của nó với an toàn mạng.
7. Vì sao an toàn mạng được xem là một thành phần quan trọng của an toàn thông tin? Hãy giải thích.
8. Phân tích các loại hình tấn công vào yếu tố con người và đề xuất các biện pháp phòng chống.
9. Tấn công trung gian (Man-in-the-Middle) là gì? Hãy trình bày cách thức và hậu quả của loại hình tấn công này.
10. Hãy mô tả cách thức và mục tiêu của một cuộc tấn công từ chối dịch vụ (DoS). Nêu giải pháp ngăn chặn.
11. SQL Injection là gì? Phân tích cách tấn công này hoạt động và nêu các biện pháp phòng ngừa.
12. Logic bomb là gì? Hãy giải thích cách thức hoạt động và nguy cơ của loại mã độc này.
13. Theo bạn, các tệp nào dễ bị nhiễm virus nhất? Vì sao? Đưa ra các biện pháp hạn chế rủi ro.
14. Trình bày các bước cần thực hiện để xử lý một máy tính bị nhiễm virus mà không có phần mềm antivirus.
15. Hãy phân tích cách tạo mật khẩu mạnh và nêu lý do tại sao mật khẩu phức tạp lại quan trọng.
16. Tấn công DDoS khác với DoS ở điểm nào? Hãy giải thích tại sao DDoS lại khó phòng chống hơn.
17. Phân tích cách một cuộc tấn công IP flood hoạt động. Hãy đề xuất các biện pháp bảo vệ hệ thống trước kiểu tấn công này.
18. Theo bạn, chiều dài tối thiểu của mật khẩu nên là bao nhiêu để đảm bảo an toàn? Giải thích ý nghĩa của việc này.
19. Quy trình xác thực người dùng khi họ đăng nhập vào một mạng máy tính cần bao gồm những bước nào? Tại sao xác thực lại quan trọng?
20. Hãy mô tả một tình huống thực tế mà việc không sử dụng mật khẩu mạnh dẫn đến hậu quả nghiêm trọng. Nêu các bài học rút ra từ tình huống này

Chương 2: Mã hóa đối xứng cổ điển

1. Trình bày khái niệm mã hóa và giải mã. Vì sao mã hóa lại quan trọng trong việc bảo mật thông tin?

2. Mật mã học là gì? Hãy giải thích vai trò của ngành khoa học này trong việc bảo vệ thông tin.
3. Phá mã là gì? Phân biệt giữa phá mã và giải mã.
4. Phân tích các yếu tố ảnh hưởng đến độ an toàn của một hệ mật mã. Hãy nêu ví dụ minh họa.
5. So sánh tốc độ mã hóa và giải mã giữa hệ mật mã công khai và hệ mật mã bí mật hiện đại.
6. So sánh độ an toàn của hệ mật mã công khai và hệ mật mã bí mật hiện đại. Điều gì quyết định tính ưu việt của một loại hệ mật?
7. Trình bày các phương pháp mà người thám mã có thể sử dụng để tìm bản rõ hoặc khóa bí mật.
8. Mật mã dịch vòng là gì? Hãy giải thích cách hoạt động và ứng dụng của loại mật mã này.
9. Trong bảng chữ cái tiếng Anh, mật mã dịch vòng có bao nhiêu cách chọn khóa? Giải thích cách tính.
10. Trình bày nguyên tắc hoạt động của mật mã hoán vị. So sánh với mật mã dịch vòng.
11. Trong mật mã hoán vị, tại sao số cách chọn khóa lại liên quan đến hoán vị của các ký tự? Hãy giải thích chi tiết.
12. Hệ mật mã Hill hoạt động như thế nào? Trình bày điều kiện cần của ma trận khóa K để hệ mật mã này hoạt động chính xác.
13. Giải thích vai trò của định thức ma trận K trong hệ mật mã Hill. Tại sao định thức này phải nguyên tố cùng nhau với 26?
14. Cho một ma trận vuông cấp **m**, hãy trình bày cách kiểm tra xem ma trận đó có thể làm khóa cho hệ mật mã Hill hay không.
15. So sánh mật mã Hill với mật mã dịch vòng và mật mã hoán vị. Điểm mạnh và hạn chế của từng loại mật mã là gì?
16. Trình bày quy trình giải mã một bản mã sử dụng mật mã dịch vòng. Hãy đưa ra một ví dụ minh họa.
17. Giải thích cách giải mã bản mã khi sử dụng mật mã hoán vị. Hãy nêu một ví dụ cụ thể.
18. Làm thế nào để tính toán ma trận nghịch đảo $\mathbf{K}^{-1}$ trong hệ mật mã Hill? Hãy trình bày các bước thực hiện.
19. Trong mật mã hoán vị, điều gì xảy ra nếu sử dụng khóa sai khi giải mã? Hãy phân tích hệ quả và nêu ví dụ.
20. Vì sao việc chọn khóa trong các hệ mật mã phải đảm bảo tính an toàn? Hãy đưa ra các tiêu chí để chọn một khóa mật mã an toàn.

Chương 3: Mã hóa đối xứng hiện đại

1. Giải thích cấu trúc và nguyên lý hoạt động của thuật toán mã hóa DES.
2. So sánh sự khác biệt giữa chế độ hoạt động ECB và CBC trong DES. Nêu ưu, nhược điểm của từng chế độ.
3. Giải thích vì sao hệ mã Double DES (2DES) không an toàn và mô tả tấn công "meet-in-the-middle".

4. Trình bày mục đích của S-box trong DES và tại sao nó là yếu tố quan trọng trong việc tăng cường độ phức tạp của thuật toán.
5. Mô tả quy trình tạo các khóa con trong thuật toán DES.
6. Giải thích khái niệm mã hóa khối và mã hóa dòng. So sánh ưu, nhược điểm của hai phương pháp này.
7. Giải thích nguyên nhân DES sử dụng khóa có chiều dài 56 bits thay vì 64 bits.
8. Trình bày các bước cơ bản trong quá trình mã hóa và giải mã sử dụng DES.
9. Phân tích các phương pháp tấn công phá mã DES, bao gồm vét cạn khóa, vi sai, và tuyến tính.
10. Trình bày quy trình mã hóa sử dụng thuật toán 3DES và giải thích cách nó cải thiện độ an toàn so với DES.
11. Mô tả các chế độ hoạt động của thuật toán mã hóa khối (ECB, CBC, OFB, CFB).
12. So sánh thuật toán mã hóa AES và DES về cấu trúc, độ dài khóa và độ an toàn.
13. Trình bày các bước chính trong quy trình mã hóa và giải mã của AES.
14. Giải thích tại sao chính phủ Mỹ sử dụng AES thay thế cho DES.
15. Phân tích vai trò và ý nghĩa của các khóa vòng trong thuật toán AES.
16. So sánh các loại tấn công vào hệ mật mã khối như brute force, vi sai, và tuyến tính.
17. Giải thích tầm quan trọng của việc sử dụng kênh bảo mật trong phân phối khóa đối xứng.
18. Tại sao thuật toán mã hóa khối cần xử lý dữ liệu theo từng khối có độ dài xác định?
19. Mô tả các yếu tố quyết định độ an toàn của một thuật toán mã hóa.
20. Phân tích các điểm yếu của DES khiến nó dễ bị tấn công bằng các phương pháp hiện đại.

Chương 4: Mật mã khóa công khai

1. Chứng minh và tính kết quả của $(72010 \bmod 13)$.
2. Tính giá trị $\phi(440)$ trong hàm phi Euler và giải thích cách tính.
3. Cho thuật toán RSA với $p=3, q=11, e=7$:
   a. Tính giá trị nnn và $\phi(n)$.
   b. Xác định giá trị d, biết $d \cdot e \equiv 1 \bmod \phi(n)$.
4. Với thuật toán RSA trên, giải mã bản mã $C=5$. Tìm bản rõ M.
5. Giải thích lý do độ an toàn của RSA phụ thuộc vào việc phân tích thừa số nguyên tố của các số lớn.

6. Trình bày quy trình trao đổi khóa Diffie-Hellman.
7. Với $q=71, \alpha=7, X_A=5$, tính khóa công khai Y_A của A.
8. Giải thích cách tính khóa bí mật dùng chung K_{AB} giữa hai bên A và B trong Diffie-Hellman.

9. Phân tích điểm mạnh và điểm yếu của Diffie-Hellman trong trao đổi khóa bảo mật.
10. Trình bày quy trình ký số và xác thực chữ ký trong hệ thống RSA.

11. So sánh tốc độ và kích thước khóa giữa RSA và DES.
12. Nêu và phân tích các ứng dụng chính của hệ mật mã khóa công khai.
13. Tại sao RSA không được sử dụng để mã hóa dữ liệu lớn? Đề xuất phương pháp thay thế khi cần.
14. Giải thích tại sao kích thước khóa trong RSA phải lớn để đảm bảo an toàn.
15. Trình bày ý nghĩa và vai trò của khóa công khai và khóa riêng trong RSA.

16. Một file dữ liệu cần được bảo mật lưu trên đĩa cứng. Hãy đề xuất thuật toán phù hợp và giải thích.
17. Khi mã hóa bản rõ x=12 với khóa công khai n=77, e=7 hãy tính bản mã thu được.
18. Cho biết quy trình mã trước ký sau trong giao tiếp bảo mật. Minh họa bằng ví dụ cụ thể.
19. Phân tích bài toán (y=77,p=13, q=17, e=37):
    a. Tính $\phi(n)$, khóa riêng d.
    b. Giải mã yyy để tìm bản rõ.

20. Người A chọn các thông số p=17, q=3, e=5:
    a. Tính khóa công khai của A.
    b. b. Xác định giá trị khóa riêng.

Chương 5: Xác thực và chữ ký số

1. Hàm băm mật mã cần đáp ứng những tính chất nào để đảm bảo tính an toàn? Trình bày và giải thích từng tính chất đó.
2. Hãy giải thích cách thức mà chữ ký số đảm bảo tính toàn vẹn và tính xác thực của một thông điệp. Đưa ra ví dụ minh họa.
3. Giải thích quy trình tạo và xác minh chữ ký số trong hệ mã RSA. Khóa nào được sử dụng ở mỗi bước?
4. So sánh thuật toán MD5 và SHA về kích thước giá trị băm và tính ứng dụng trong thực tế.
5. Phân biệt giữa hàm băm không có khóa và hàm băm có khóa. Đưa ra một ví dụ ứng dụng thực tế cho từng loại.
6. Chữ ký số khác gì so với chữ ký điện tử thông thường? Trình bày sự khác biệt và các tình huống sử dụng cụ thể.
7. Giải thích tại sao thuật toán RSA không được sử dụng để mã hóa dữ liệu lớn mà chỉ được áp dụng trong việc bảo mật khóa và tạo chữ ký số.
8. Nếu có một hàm băm với giá trị băm dài 128 bits, giải thích tại sao xác suất để có hai thông điệp có cùng giá trị băm bằng 0.5 khi sửa đổi một số lượng bit nhất định.
9. Trình bày các bước chi tiết trong quá trình sử dụng thuật toán SHA-1 để kiểm tra tính toàn vẹn của một thông điệp.

10. Phân tích ưu và nhược điểm của DSA so với RSA khi áp dụng trong thực tế.
11. Một thông điệp được băm bằng MD5 và giá trị băm đó được mã hóa bằng khóa riêng của người gửi. Hãy giải thích quy trình này nhằm mục đích gì.
12. Giả sử bạn được giao nhiệm vụ xác thực một tập tin phần mềm tải về từ internet. Bạn sẽ sử dụng MD5 như thế nào để đảm bảo tính toàn vẹn của tập tin?
13. Hãy mô tả các bước thực hiện mã hóa chữ ký số với thông điệp gốc trong sơ đồ ký số.
14. Xác thực chữ ký số của một người khác cần sử dụng khóa nào? Tại sao?
15. So sánh sự khác biệt giữa các hàm băm có khóa và không có khóa trong việc ứng dụng tạo mã xác thực thông điệp (MAC).
16. Trình bày cách mà thuật toán SHA hỗ trợ trong việc tạo chữ ký số. Nêu các đặc điểm của thuật toán này.
17. Nếu một ứng dụng yêu cầu tính toán giá trị băm với kích thước 256 bits, thuật toán băm nào sẽ phù hợp hơn, và tại sao?
18. Trình bày và giải thích quá trình phân loại các hàm băm mật mã. Phân loại này dựa trên tiêu chí nào?
19. Một tổ chức muốn bảo mật một tài liệu sao cho chỉ những người nhận được khóa bí mật mới có thể mở xem. Giải thích cách sử dụng thuật toán băm kết hợp với khóa bí mật để đạt được mục tiêu này.
20. Trong tình huống thực tế, làm thế nào để sử dụng MAC để kiểm tra tính toàn vẹn và tính xác thực của dữ liệu trong hệ thống mạng?

Chương 6: An toàn thư điện tử

1. Trình bày các dịch vụ mà giao thức PGP cung cấp.
2. Giải thích vì sao khi dùng PGP trong hệ thống Email, dịch vụ tương thích với email lại yêu cầu ánh xạ các dữ liệu nhị phân thành ký tự ASCII.
3. Khi sử dụng cả hai dịch vụ bí mật và xác thực của PGP, hãy mô tả quy trình mã hóa thông điệp và chữ ký số.
4. Khóa được sử dụng để mã hóa khóa phiên trong PGP là gì? Giải thích vai trò của khóa này.
5. Phân tích chế độ hoạt động của PGP khi thực hiện mã hóa đối xứng và nêu lý do chọn chế độ đó.
6. Các thuật toán mã hóa đối xứng nào được sử dụng trong PGP? Vì sao các thuật toán này được lựa chọn?
7. PGP hỗ trợ những loại xác thực nào trong quá trình bảo mật thư điện tử?
8. Vì sao PGP thực hiện tạo chữ ký trước khi nén dữ liệu? Trình bày lợi ích của phương pháp này.
9. Mô tả ba cách sử dụng phổ biến của mã hóa PGP và ý nghĩa của chúng trong bảo mật thông tin.
10. Phân tích ưu điểm của mã hóa PGP và ứng dụng trong thực tế.
11. Trình bày nhược điểm chính của mã hóa PGP và cách khắc phục.
12. So sánh mã hóa bất đối xứng và đối xứng trong S/MIME. Đâu là trường hợp thích hợp để sử dụng mỗi phương pháp?

13. Khóa nào được sử dụng để mã hóa khóa trong S/MIME, và tại sao lại chọn loại khóa này?
14. Giải thích ý nghĩa và chức năng của S/MIME trong bảo mật thư điện tử.
15. So sánh S/MIME với các giao thức bảo mật khác như PGP, SSL, hoặc IPSec.
16. Ý nghĩa của cụm từ "Pretty Good Privacy" trong PGP, và tại sao giao thức này được đặt tên như vậy?
17. Mô tả vai trò của Internet Engineering Task Force (IETF) trong việc phát triển các chuẩn bảo mật như S/MIME.
18. Trình bày cách thức sử dụng khóa để giải mã khóa trong S/MIME khi nhận email được mã hóa.
19. Phân tích các ưu điểm của mã hóa S/MIME và vai trò của chúng trong bảo mật dữ liệu.
20. Chứng minh khả năng tương thích của S/MIME với các email client khác nhau. Vì sao điều này quan trọng trong việc bảo mật email?

Chương 7: An toàn IP

1. Trình bày các giao thức làm việc trên lớp IP để bảo vệ thông tin IP trên mạng. Hãy giải thích mục đích và cách thức hoạt động của từng giao thức.
2. Giao thức nào không phải là một giao thức đường hầm nhưng sử dụng các giao thức đường hầm để bảo mật thông tin trên mạng? Hãy giải thích tại sao?
3. Mô tả cách thức hoạt động của giao thức bảo mật IPSec tại tầng nào trong mô hình OSI và lý do tại sao nó hoạt động ở tầng đó.
4. Phân biệt giữa các chế độ hoạt động của IPSec: Tunnel Mode và Transport Mode. Mỗi chế độ này bảo vệ thông tin như thế nào?
5. Giải thích chế độ Tunnel của IPSec và cách nó bảo vệ các gói tin IP, bao gồm việc bảo vệ thông tin nào trong gói tin.
6. So sánh giữa chế độ Transport và Tunnel của IPSec. Mỗi chế độ bảo vệ các phần nào của gói tin và có tác động gì đến hiệu suất mạng?
7. IPSec có những mục tiêu bảo mật nào? Hãy phân tích chi tiết về các mục tiêu này và cách IPSec đạt được chúng.
8. Giải thích cơ chế của IPSec trong việc xác thực và bảo vệ thông tin trong giao tiếp qua mạng.
9. Khi sử dụng IPSec trong mạng, giao thức AH và ESP cung cấp các dịch vụ bảo mật nào? Hãy phân tích chi tiết từng dịch vụ.
10. Mô tả cách thức hoạt động của IPSec khi cung cấp dịch vụ bảo mật cho các giao thức TCP/IP và tầm quan trọng của việc mã hóa thông tin trong môi trường mạng.
11. IPSec hoạt động với mấy chế độ bảo mật và các chế độ này có tác dụng gì đối với bảo mật thông tin trong mạng?
12. Phân tích sự khác biệt giữa các dịch vụ bảo mật mà IPSec cung cấp. Giải thích vì sao mỗi dịch vụ lại quan trọng trong bảo mật mạng.
13. Mô tả các dịch vụ bảo mật mà IPSec cung cấp và tác động của các dịch vụ này đối với các giao thức và dữ liệu truyền qua mạng.

14. Chế độ vận chuyển của IPSec không bảo vệ toàn bộ IP packet. Giải thích tại sao và trong trường hợp nào chế độ này là phù hợp.
15. Chế độ đường hầm của IPSec bảo vệ toàn bộ IP packet. Trình bày chi tiết về cách thức hoạt động của chế độ này và ứng dụng thực tế của nó.
16. Giải thích các dịch vụ bảo mật của IPSec như tính toàn vẹn thông điệp, xác thực thực thể và tính bí mật. Cách thức hoạt động của từng dịch vụ trong IPSec.
17. IPSec cung cấp dịch vụ kiểm soát truy cập như thế nào? Hãy phân tích vai trò của cơ sở dữ liệu SAD trong việc kiểm soát truy cập.
18. Dịch vụ xác thực thực thể của IPSec giúp làm gì trong quá trình truyền thông tin qua mạng? Hãy mô tả cách thức xác thực này hoạt động.
19. Dịch vụ tính toàn vẹn thông điệp trong IPSec bảo vệ như thế nào? Giải thích cách thức tóm tắt dữ liệu được tạo ra và kiểm tra.
20. Giải thích dịch vụ tính bí mật và chống tấn công phát lại của IPSec. Cách mà thông điệp được bảo mật và xác thực thông qua AH và ESP.

Chương 8: An toàn Web

1. Mô tả các giao thức bảo mật trên Internet như SSL, TLS và SSH. Những giao thức này hoạt động ở tầng nào trên mô hình OSI và vì sao chúng lại hoạt động ở tầng đó?
2. Giải thích chức năng và mục đích sử dụng của giao thức SSL trong bảo mật thông tin trên Internet.
3. So sánh giao thức TLS với SSL. Tại sao TLS được đề nghị sử dụng bổ sung vào SSL trong các giao thức bảo mật?
4. Giao thức SSH được sử dụng để cung cấp dịch vụ bảo mật cho các phiên làm việc trên thiết bị đầu cuối hệ thống UNIX từ xa. Hãy mô tả chi tiết cách thức hoạt động của SSH.
5. Giao thức SSL, TLS và SSH đều đóng vai trò bảo mật thông tin trong các hệ thống mạng. Hãy phân tích vai trò của mỗi giao thức trong việc mã hóa và bảo vệ dữ liệu.
6. Trong giao thức SSL, có bao nhiêu khóa và vector ban đầu được yêu cầu để đảm bảo tính toàn vẹn và tính bảo mật của thông điệp? Giải thích vì sao cần các yếu tố này.
7. Một phiên trong giao thức SSL là gì? Trình bày các đặc điểm và mục đích của một phiên SSL trong quá trình bảo mật giao tiếp giữa client và server.
8. Trong giao dịch điện tử an toàn (SET), ai là người chịu trách nhiệm thanh toán các khoản mua hàng của chủ thẻ và tại sao?
9. Trong giao dịch điện tử an toàn (SET), ai là thành phần chịu trách nhiệm thực hiện các giao dịch thanh toán của người dùng thẻ tín dụng?
10. Chức năng và vai trò của Merchant trong giao dịch điện tử an toàn (SET) là gì? Hãy mô tả quá trình thực hiện giao dịch thanh toán của Merchant.
11. Trong giao dịch SET, Issuer là ai và có vai trò gì trong việc xử lý giao dịch thanh toán?
12. Payment Gateway trong giao dịch SET có vai trò như thế nào trong việc đảm bảo an toàn giao dịch thanh toán trực tuyến?

13. Chứng nhận của CA (Certification Authority) trong giao dịch SET giúp đảm bảo điều gì cho các bên tham gia? Hãy giải thích quá trình cấp chứng nhận này.
14. Trình bày các bước thực hiện một giao dịch SET điển hình, từ khi khách hàng đặt hàng cho đến khi giao hàng được thực hiện.
15. Chữ ký song song trong SET có vai trò gì trong việc bảo mật giao dịch? Giải thích sự khác biệt giữa chữ ký song song và chữ ký thông thường.
16. Phân tích quy trình xử lý thanh toán (Payment Processing) trong SET. Các thủ tục chính của quá trình này là gì và tại sao chúng lại quan trọng?
17. Thủ tục xác thực thanh toán trong quá trình xử lý thanh toán của SET có vai trò gì? Mô tả cách thức người bán hàng xác thực tính hợp lệ của người mua qua cửa thanh toán.
18. Giải thích thủ tục "Thực hiện thanh toán" trong SET và cách thức người bán hàng thực hiện giao dịch thanh toán với cửa thanh toán.
19. Trong yêu cầu mua hàng của xử lý thanh toán trong SET, có bao nhiêu bản tin được sử dụng? Hãy mô tả nội dung và mục đích của từng bản tin.
20. Khi thực hiện yêu cầu mua hàng trong xử lý thanh toán SET, bản tin nào có nhiệm vụ gửi thông tin cho người mua? Trình bày chi tiết về bản tin này và vai trò của nó trong giao dịch.