3.1 - Khái niệm và các yêu cầu của xác thực

1. Khái niệm xác thực là gì?

a) Quá trình mã hóa thông tin để người khác không đọc được

b) Quá trình kiểm tra quyền truy cập của người dùng

c) Quá trình đảm bảo tính toàn vẹn và đáng tin cậy của thông tin

d) Quá trình lưu trữ thông tin một cách an toàn

2. Mã xác thực bản tin (MAC) là gì?

a) Một loại mã hóa thông tin

b) Địa chỉ vật lý của thiết bị mạng

c) Một hàm của bản tin và khóa bí mật tạo ra giá trị có chiều dài cố định có chức năng như một ký hiệu xác thực

d) Một phương pháp truyền thông tin qua mạng

3. Mục đích chính của xác thực dữ liệu là gì?

a) Mã hóa dữ liệu để bảo mật

b) Đảm bảo dữ liệu không bị thay đổi trong quá trình truyền

c) Tăng tốc độ truyền dữ liệu

d) Nén dữ liệu để tiết kiệm băng thông

4. Mã xác thực bản tin (MAC) cung cấp tính chất nào sau đây?

a) Tính bảo mật

b) Tính toàn vẹn và xác thực nguồn gốc

c) Tính sẵn sàng

d) Tính không thể chối bỏ

5. Hai chuẩn hàm MAC phổ biến là gì?

a) RSA và DSA

b) DES và AES

c) HMAC và CMAC

d) MD5 và SHA-1

6. Tại sao MAC được xem là an toàn hơn checksum thông thường?

a) Vì MAC có kích thước lớn hơn

b) Vì MAC sử dụng thuật toán phức tạp hơn

c) Vì MAC sử dụng khóa bí mật, kẻ tấn công không thể tạo ra MAC hợp lệ mà không biết khóa

d) Vì MAC được mã hóa bằng thuật toán mã hóa đối xứng

7. Trong mô hình MAC để chứng thực bản tin không có tính bảo mật, quá trình xác thực diễn ra như thế nào?

a) Bản tin được mã hóa trước khi tính MAC

b) Bản tin được gửi ở dạng rõ cùng với MAC, người nhận tính lại MAC và so sánh

c) Chỉ MAC được gửi, không gửi bản tin

d) Bản tin và MAC đều được mã hóa trước khi gửi

8. Phương pháp nào sau đây kết hợp cả tính bảo mật và xác thực?

a) Chỉ sử dụng MAC

b) Chỉ sử dụng mã hóa

c) Mã hóa bản tin và sử dụng MAC

d) Sử dụng checksum đơn giản

3.2 - Xác thực người sử dụng

1. Định danh (Identification) là gì?

a) Quá trình xác minh mật khẩu của người dùng

b) Quá trình người dùng cung cấp danh định của mình cho hệ thống

c) Quá trình mã hóa thông tin người dùng

d) Quá trình kiểm tra quyền truy cập của người dùng

2. Xác thực (Authentication) là gì?

a) Quá trình cấp quyền truy cập cho người dùng

b) Quá trình chứng minh định danh là hợp lệ và phù hợp với người dùng

c) Quá trình mã hóa thông tin người dùng

d) Quá trình tạo tài khoản mới cho người dùng

3. Có bao nhiêu phương pháp xác thực cơ bản?

a) 2 phương pháp

b) 3 phương pháp

1. "biết" - something you know
2. "có" - something you have
3. "là chính bạn " - something you

c) 4 phương pháp

d) 5 phương pháp

4. Phương pháp xác thực "Những gì bạn biết" (Something you know) bao gồm:

a) Vân tay và võng mạc

b) Mật khẩu và số PIN

c) Thẻ thông minh và token

d) Chứng chỉ số và khóa USB

5. Phương pháp xác thực "Những gì bạn có" (Something you have) bao gồm:

a) Mật khẩu và số PIN

b) Thẻ thông minh và token

c) Vân tay và võng mạc

d) Câu hỏi bảo mật và mật khẩu

6. Phương pháp xác thực "Những gì là chính bạn" (Something you are) bao gồm:

a) Mật khẩu và số PIN

b) Thẻ thông minh và token

c) Vân tay, võng mạc và nhận dạng khuôn mặt

d) Chứng chỉ số và khóa USB

7. Ưu điểm của phương pháp xác thực bằng mật khẩu là gì?

a) Khó bị tấn công

b) Tiện lợi và chi phí thấp

c) Không thể đoán được

d) Không thể quên

8. Xác thực bằng sinh trắc học gồm mấy bước?

a) 1 bước

b) 2 bước

c) 3 bước 3 bước : thu thập dữ liệu sinh học -> so khớp -> quyết định

d) 4 bước

9. Định danh số hóa bao gồm những loại nào?

a) Định danh máy tính và định danh mạng

b) Định danh sinh trắc, định danh máy tính và định danh số

c) Định danh người dùng và định danh thiết bị

d) Định danh vật lý và định danh logic

10. So sánh các phương pháp xác thực về khả năng bị tấn công, phương pháp nào khó bị tấn công nhất?

a) Mật khẩu

b) Thẻ thông minh

c) Sinh trắc học

d) Tất cả đều như nhau

11. Giao thức xác thực Challenge/Response hoạt động như thế nào?

a) Người dùng gửi mật khẩu, máy chủ xác thực

b) Máy chủ gửi mật khẩu, người dùng xác thực

c) Máy chủ gửi một số ngẫu nhiên (nonce), người dùng trả lời bằng hàm của số đó và mật khẩu

d) Người dùng và máy chủ đồng thời gửi mật khẩu cho nhau

12. Nhược điểm của giao thức xác thực đơn giản là gì?

a) Quá phức tạp để triển khai

b) Mật khẩu có thể bị nghe lén khi truyền dưới dạng bản rõ

c) Yêu cầu nhiều tài nguyên máy tính

d) Không hỗ trợ nhiều người dùng cùng lúc

13. Trong xác thực người dùng sử dụng mật mã khóa đối xứng, ký hiệu KAB đại diện cho:

a) Khóa công khai của Alice

b) Khóa bí mật của Bob

c) Khóa chung (shared key) của Alice và Bob

d) Khóa của cơ quan chứng thực

14. Trong giao thức xác thực lẫn nhau cải tiến, tại sao cần sử dụng số nonce?

a) Để tăng tốc độ xác thực

b) Để ngăn chặn tấn công bằng cách lặp lại thông điệp (replay attack)

c) Để giảm kích thước thông điệp

d) Để mã hóa mật khẩu

15. Trong xác thực người dùng sử dụng mật mã khóa bất đối xứng, ký hiệu PUA và PRA lần lượt đại diện cho:

a) Mật khẩu người dùng và mật khẩu quản trị

b) Khóa chính và khóa phụ

c) Khóa công khai và khóa bí mật của Alice

d) Khóa bí mật và khóa công khai của Alice

16. Trong xác thực người dùng sử dụng mật mã khóa bất đối xứng, ký hiệu S=[M]PRA có ý nghĩa gì?

a) Mã hóa thông điệp M bằng khóa công khai của Alice

b) Giải mã thông điệp M bằng khóa công khai của Alice

c) Ký lên thông điệp M bằng khóa bí mật của Alice

d) Xác thực thông điệp M bằng khóa công khai của Alice

17. Phân tích lỗ hổng trong giao thức xác thực lẫn nhau cải tiến sau:

1. A → B: A, NA

2. B → A: B, NB, E(KAB, NA)

3. A → B: E(KAB, NB)

a) Không có lỗ hổng, giao thức này an toàn

b) Lỗ hổng là NA và NB có thể bị nghe lén

c) Lỗ hổng là kẻ tấn công có thể mạo danh B vì không có cơ chế xác thực B trong bước 2

d) Lỗ hổng là KAB có thể bị tính toán từ NA và NB

18. Trong tấn công giao thức xác thực lẫn nhau cải tiến, kẻ tấn công Mallory có thể thực hiện tấn công như thế nào?

a) Đoán mật khẩu của Alice và Bob

b) Chặn thông điệp giữa Alice và Bob, sau đó mạo danh Bob để giao tiếp với Alice

c) Tấn công từ điển vào khóa mã hóa

d) Phá vỡ thuật toán mã hóa đối xứng

19. So sánh hiệu quả bảo mật giữa xác thực sử dụng mật mã khóa đối xứng và xác thực sử dụng mật mã khóa bất đối xứng, phương pháp nào có ưu điểm vượt trội hơn về mặt bảo mật?

a) Xác thực sử dụng mật mã khóa đối xứng luôn an toàn hơn

b) Xác thực sử dụng mật mã khóa bất đối xứng luôn an toàn hơn

c) Xác thực sử dụng mật mã khóa bất đối xứng có ưu điểm về quản lý khóa và khả năng chống chối bỏ, nhưng xác thực sử dụng mật mã khóa đối xứng có ưu điểm về tốc độ và hiệu quả

d) Cả hai phương pháp đều có mức độ bảo mật như nhau

20. Phân tích tại sao việc kết hợp nhiều phương pháp xác thực (xác thực đa yếu tố) lại hiệu quả hơn việc chỉ sử dụng một phương pháp xác thực?

a) Vì xác thực đa yếu tố dễ sử dụng hơn

b) Vì xác thực đa yếu tố nhanh hơn

c) Vì kẻ tấn công phải vượt qua nhiều rào cản bảo mật khác nhau, mỗi rào cản yêu cầu kỹ năng và công cụ tấn công khác nhau

d) Vì xác thực đa yếu tố tiết kiệm chi phí hơn

3.3 - Xác thực dữ liệu

1. Xác thực dữ liệu là gì?

a) Quá trình mã hóa dữ liệu để bảo mật

b) Quá trình đảm bảo tính toàn vẹn và nguồn gốc của dữ liệu

c) Quá trình nén dữ liệu để tiết kiệm không gian lưu trữ

d) Quá trình sao lưu dữ liệu để phòng mất mát

2. Checksum trong truyền dữ liệu có tác dụng gì?

a) Mã hóa dữ liệu

b) Phát hiện lỗi trong quá trình truyền dữ liệu

c) Nén dữ liệu

d) Tăng tốc độ truyền dữ liệu

4. Hàm băm (Hash function) được sử dụng để làm gì trong xác thực dữ liệu?

a) Mã hóa dữ liệu

b) Tạo ra một giá trị có kích thước cố định đại diện cho dữ liệu gốc

c) Nén dữ liệu

d) Tăng kích thước dữ liệu để dễ truyền

5. Đặc điểm của đầu ra của hàm băm là gì?

a) Có kích thước lớn hơn dữ liệu đầu vào

b) Có kích thước bằng dữ liệu đầu vào

c) Có kích thước cố định, thường nhỏ hơn dữ liệu đầu vào

d) Có kích thước thay đổi tùy theo dữ liệu đầu vào

6. Ứng dụng của hàm băm trong việc lưu trữ mật khẩu là gì?

a) Mã hóa mật khẩu để người dùng không đọc được

b) Lưu trữ giá trị băm của mật khẩu thay vì mật khẩu gốc

c) Tạo mật khẩu mạnh hơn

d) Nén mật khẩu để tiết kiệm không gian lưu trữ

7. Trong xác thực dữ liệu, redundancy (dư thừa) có vai trò gì?

a) Làm tăng kích thước dữ liệu không cần thiết

b) Thêm thông tin để phát hiện sự thay đổi của dữ liệu

c) Làm chậm quá trình truyền dữ liệu

d) Tăng độ phức tạp của dữ liệu

8. Mã xác thực bản tin (MAC) khác với checksum thông thường ở điểm nào?

a) MAC có kích thước nhỏ hơn

b) MAC không thể phát hiện lỗi

c) MAC sử dụng khóa bí mật trong quá trình tính toán

d) MAC chỉ áp dụng cho dữ liệu văn bản

9. Công thức tính MAC là gì?

a) MAC = M + K (M là thông điệp, K là khóa bí mật)

b) MAC = C(M, K) (M là thông điệp, K là khóa bí mật, C là hàm tính MAC)

c) MAC = M × K (M là thông điệp, K là khóa bí mật)

d) MAC = C(K) (K là khóa bí mật, C là hàm tính MAC)

10. HMAC là gì?

a) Một loại thuật toán mã hóa

b) Một loại MAC dựa trên hàm băm

c) Một loại giao thức truyền dữ liệu

d) Một loại chuẩn bảo mật mạng

11. CMAC là gì?

a) Một loại thuật toán mã hóa

b) Một loại MAC dựa trên mã khối

c) Một loại giao thức truyền dữ liệu

d) Một loại chuẩn bảo mật mạng

12. Các thuật toán hàm băm phổ biến bao gồm:

a) DES, AES, RSA

b) HMAC, CMAC, PMAC

c) MD5, SHA-1, SHA-2, SHA-3

d) RSA, DSA, ECDSA

13. Ứng dụng của hàm băm trong đấu giá trực tuyến là gì?

a) Mã hóa giá đấu giá để người khác không biết

b) Cung cấp giá trị băm của giá đấu giá cho trọng tài, đảm bảo người tham gia không thể thay đổi giá sau khi đã nộp

c) Tạo mã xác thực cho người tham gia đấu giá

d) Kiểm tra tính hợp lệ của người tham gia đấu giá

14. Ứng dụng của hàm băm trong việc download dữ liệu là gì?

a) Mã hóa dữ liệu trước khi download

b) Kiểm tra tính toàn vẹn của file sau khi download bằng cách so sánh giá trị băm

c) Tăng tốc độ download

d) Nén dữ liệu trước khi download

15. Tính chống trùng mạnh (Strong collision resistance) của hàm băm có nghĩa là gì?

a) Không thể tìm được giá trị gốc từ giá trị băm

b) Với một giá trị x, không thể tìm $y \neq x$ sao cho $H(x)=H(y)$

c) Không thể tìm được cặp giá trị x, y bất kỳ ($x \neq y$) sao cho $H(x)=H(y)$

d) Hàm băm luôn tạo ra các giá trị khác nhau cho mọi đầu vào

3.4 - Chữ ký số, chứng thư số và PKI

1. Chữ ký số (Digital signature) là gì?

a) Một hình ảnh chữ ký được quét và lưu trữ

b) Một chuỗi dữ liệu liên kết với một thông điệp và thực thể tạo ra thông điệp, đảm bảo tính toàn vẹn và xác thực

c) Một loại mật khẩu dùng để đăng nhập hệ thống

d) Một phương pháp mã hóa thông điệp

2. Mục đích chính của chữ ký số là gì?

a) Mã hóa thông điệp

b) Xác thực nguồn gốc, đảm bảo tính toàn vẹn và chống chối bỏ

c) Nén thông điệp

d) Tăng tốc độ truyền thông điệp

3. Trong chữ ký số, khóa nào được sử dụng để tạo chữ ký?

a) Khóa công khai của người gửi

b) Khóa bí mật của người gửi

c) Khóa công khai của người nhận

d) Khóa bí mật của người nhận

4. Trong chữ ký số, khóa nào được sử dụng để xác thực chữ ký?

a) Khóa bí mật của người gửi

b) Khóa công khai của người gửi

c) Khóa bí mật của người nhận

d) Khóa công khai của người nhận

5. Chứng thư số (Digital certificate) là gì?

a) Một loại chữ ký số

b) Một tài liệu điện tử liên kết khóa công khai với một thực thể cụ thể, được ký bởi một bên thứ ba tin cậy (CA)

c) Một loại khóa bí mật

d) Một phương pháp xác thực người dùng

6. CA là viết tắt của:

a) Certificate Association

b) Certification Authority

c) Cryptographic Agency

d) Certificate Administration

7. PKI là viết tắt của:

a) Private Key Infrastructure

b) Public Key Infrastructure

c) Personal Key Identification

d) Public Key Identification

8. Thành phần nào trong PKI chịu trách nhiệm tạo và quản lý chứng thư số?

a) RA (Registration Authority)

b) CA (Certification Authority)

c) CRA (Certificate Repository and Archive)

d) SS (Security Server)

9. Quá trình tạo chữ ký số thường bao gồm bước nào?

a) Mã hóa toàn bộ thông điệp bằng khóa bí mật

b) Tính giá trị băm (message digest) của thông điệp, sau đó mã hóa giá trị băm bằng khóa bí mật của người gửi

c) Mã hóa thông điệp bằng khóa công khai của người nhận

d) Tính giá trị băm của thông điệp và gửi kèm theo thông điệp

10. Quá trình xác thực chữ ký số bao gồm bước nào?

a) Giải mã chữ ký bằng khóa bí mật của người gửi

b) Tính giá trị băm của thông điệp nhận được, giải mã chữ ký bằng khóa công khai của người gửi, sau đó so sánh hai giá trị băm

c) Giải mã chữ ký bằng khóa công khai của người nhận

d) So sánh chữ ký số với chữ ký mẫu

11. Thuật toán chữ ký số nào dựa trên bài toán phân tích ra thừa số nguyên tố?

a) DSA (Digital Signature Algorithm)

b) RSA (Rivest–Shamir–Adleman)

c) ECDSA (Elliptic Curve Digital Signature Algorithm)

d) ElGamal

12. Chuẩn chứng thư số phổ biến nhất hiện nay là gì?

a) PGP (Pretty Good Privacy)

b) X.509

c) SSL/TLS

d) S/MIME

13. Nội dung chính của một chứng thư số X.509 bao gồm:

a) Chỉ có khóa công khai và tên người dùng

b) Tên chủ sở hữu, khóa công khai, thời hạn hiệu lực, tên CA, chữ ký của CA, số hiệu chứng thư

c) Chỉ có khóa bí mật và tên người dùng

d) Chỉ có chữ ký số của người dùng

14. Vai trò của RA (Registration Authority) trong PKI là gì?

a) Tạo và ký chứng thư số

b) Xác minh thông tin nhận dạng của người yêu cầu cấp chứng thư trước khi chuyển yêu cầu tới CA

c) Lưu trữ và phân phối chứng thư số

d) Thu hồi chứng thư số hết hạn

15. Mô hình PKI phân cấp (Hierarchical PKI) có đặc điểm gì?

a) Chỉ có một CA duy nhất

b) Có một CA gốc (Root CA) và nhiều CA cấp dưới, tạo thành cấu trúc cây

c) Các CA tin tưởng lẫn nhau theo mô hình mạng lưới

d) Không có CA nào, người dùng tự quản lý khóa

16. Tại sao cần phải thu hồi chứng thư số?

a) Vì chứng thư số quá cũ

b) Vì khóa bí mật tương ứng có thể đã bị lộ, hoặc thông tin trong chứng thư không còn chính xác

c) Vì người dùng không muốn sử dụng nữa

d) Vì CA muốn cấp chứng thư mới

17. Cho biết khóa bí mật d=7, n=33, và bản băm của thông điệp là H(m)=4. Chữ ký số được tạo ra là:

a) 11

b) 16 `S = 4 ^ 7 mod 33 = 16`

c) 28

d) 13

18. Cho khóa công khai của người gửi là (e=3,n=33), khoá bí mật của bên nhận (d=11, n=33) và chữ ký số S=16, người nhận kiểm tra bằng cách tính:

a) 16^3 mode 33

b) 16^11 mode 33

c) 3^16 mode 33

d) 11^16 mode 33

19. Nếu chữ ký RSA S=20, khoá công khai của bên gửi (e=3,n=33), giá trị xác minh là bao nhiêu?

a) 4

b) 26

c) 7

d) 16

20. Trong chữ ký RSA, bước nào sau đây không cần thiết trong quá trình tạo chữ ký?

a) Băm thông điệp

b) Tính S=H(m)^d mod n

c) Giải mã chữ ký

d) Sử dụng khóa bí mật