

Câu 13. Hệ mật SHA-512 có thể sử dụng để tính giá trị băm của bản tin có độ dài tối đa bao nhiêu bit?

A. $2^{192}-1$

B. $2^{256}-1$

☒ C. $2^{128}-1$

D. $2^{512}-1$

Câu 14. A mật mã hóa bản rõ "dtvtbkhn" sử dụng hệ mật mã Affine với khóa mật mã là (14,4) rồi gửi cho B. Đây là bản mật mã A đã gửi đi?

A. LDPDZQJT

B. LDPOZOJT

C. LDPDZOJT

☒ D. Không có lựa chọn nào đúng

$$(P \times 14 + 4) \bmod 26$$

Câu 15. Các bit dùng để làm bit Parity trong hệ mật DES là?

A. 2, 4, 6, 8, 12, 14, 16, 18

☒ B. 8, 16, 24, 32, 40, 48, 56, 64

C. 2, 4, 8, 16, 24, 32, 48, 64

D. 4, 8, 16, 24, 32, 40, 48, 64

Câu 16. Thuật toán nào thực hiện theo các bước dưới đây:

1. p, q – two prime numbers, (private, chosen)
2. $n = p \cdot q$, (public, calculated)
3. e , with $\gcd(\Phi(n), e) = 1, 1 < e < \Phi(n)$, (public, chosen)
4. $d = e^{-1} \pmod{\Phi(n)}$, (private, calculated)

A. RC4

☒ B. RSA

C. Knapsack

D. ECC

Câu 17. Tập $\{1, 3, 6, 13, 27, 52\}$ là tập siêu tăng (superincreasing).

☒ A. Đúng

B. Sai

$$3 \bmod 11 = 3$$

Câu 18. Kết quả của phép tính sau: $3^{201} \bmod 11 = ?$

A. 10

B. 6

C. 5

☒ D. 3

$$3^{10} \cdot 3^2 \cdot 3$$

Câu 19. Biểu diễn tương ứng của đa thức $x^6 + x^4 + x^3 + x^2 + x$ trong $GF(2^8)$ là:

A. 01010111

B. 01001110

☒ C. 01011110

D. 11011010

Câu 20. Giá trị hàm Euler - Phi của 773 là?

A. 377

B. 770

C. 771

☒ D. 772

$$a \left(1 - \frac{1}{a}\right)$$

B. TỰ LUẬN (6 điểm)

Xét hệ mật AES-128 với khóa là HUSTCRYPTOGRAPHY và bản tin rõ (plaintext) là SUNSHINEINSUMMER. Hãy xác định:

- a. Ma trận khóa gốc và khối trạng thái (state) ứng với bản tin rõ với giả thiết các ký tự được mã hóa theo bảng mã ASCII và các phần tử ma trận thể hiện dưới dạng Hexa;
- b. Khối trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1;
- c. Cột đầu tiên (w_{04}) của khóa mở rộng cho vòng 1.

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
TRƯỜNG ĐIỆN - ĐIỆN TỬ

Đề số: 01 Tổng số trang: 2

Ký duyệt
CBGD phụ trách đề thi:

ĐỀ THI CUỐI KỲ 2022.1
Học phần: ET3310 - LÝ THUYẾT MẬT MÃ

Ngày thi: 08/03/2023

Thời gian làm bài: 60 phút

(Được sử dụng tài liệu, bản in bảng tra cứu, máy tính cầm tay. Nộp đề thi cùng với bài làm)

Trưởng nhóm chuyên môn:

A. TRẮC NGHIỆM (6 điểm, mỗi câu chọn 1 ý đúng duy nhất, làm vào giấy thi)

Câu 1. Tiến trình giải mật mã hóa chuyển đổi bản mật thành bản rõ thực hiện ở đâu?

- A. Máy phát dữ liệu
B. Máy nhận dữ liệu
C. Kênh truyền
D. Cả A,B,C

Câu 2. Hệ mật AES theo tiêu chuẩn FIPS PUB 197 có ba cấu hình khác nhau về số vòng (rounds) và ?

- A. Kích thước khối dữ liệu State
B. Kiểu dữ liệu đầu vào hệ mật
C. Độ dài khóa
D. Kiểu mật mã hóa từng vòng

Câu 3. Tiến trình thẩm định chữ ký số (Digital Signature) bên nhận sử dụng _____ ?

- A. Khóa công khai B. Khóa bí mật C. A và B D. Khóa vòng

Câu 4. Biểu diễn tương ứng với đa thức $x^7 + x^5 + x^2 + x + 1$ trong $GF(2^8)$

- A. 10010011 B. 11000110 C. 10100110 D. 10100111

Câu 5. Hệ mật Triple DES hoạt động sử dụng bao nhiêu khóa?

- A. 2 B. 3 C. 4 D. 5

Câu 6. Hệ mật AES hoạt động ở cấu hình khóa có độ dài 192 bit thực hiện bao nhiêu vòng (rounds)?

- A. 10 B. 12 C. 14 D. 16

Câu 7. Thao tác "Dịch hàng (Shift rows)" được thực hiện tại bước _____ trong mỗi round của hệ mật AES.

- A. 1 B. 2 C. 3 D. 4

Câu 8. Đa thức tối giản nào được sử dụng trong mã AES là đa thức nào dưới đây?

- A. $x^4 + x^3 + x + 1$ B. $x^{16} + x^5 + x^3 + x + 1$
C. $x^8 + x^4 + x^3 + x + 1$ D. $x^6 + x^3 + x + 1$

Câu 9. Khóa nào được sử dụng để chuyển bản rõ thành bản mật trong hệ mật bất đối xứng?

- A. Khóa công khai B. Khóa bí mật C. A và B D. Khóa vòng

Câu 10. Thuật toán Diffie-Helman algorithm được sử dụng cho những ứng dụng nào ?

- A. Digital Signature B. Encryption
C. Key Exchange D. Authentication

Câu 11. Phần phi tuyến của mã AES là S-box được tính toán trong trường hữu hạn nào?

- A. $GF(2^4)$ B. $GF(2^8)$ C. $GF(2^{16})$ D. $GF(2^{32})$

Câu 12. Xác định nghịch đảo nhân của $(x^2 + x + 1) \bmod (x^4 + x^3 + 1)$

- A. $x^2 + 1$ B. $x^3 + x^2 + x$ C. $x^3 + x + 1$ D. $x^3 + x^2 + 1$

Câu 13. Tập $\{1, 3, 4, 9, 15, 25\}$ là tập siêu tăng (superincreasing).

- A. Đúng B. Sai

3 Lit MR

Câu 14. Thuật toán nào thực hiện theo các bước dưới đây:

1. p, q – two prime numbers, (private, chosen)
2. $n = p \cdot q$, (public, calculated)
3. e , with $\gcd(\Phi(n), e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
4. $d = e^{-1} \pmod{\Phi(n)}$, (private, calculated)

A. DHKE

B. AES

☒ C. RSA

D. ECC

Câu 15. Các bit dùng để làm bit Parity trong hệ mật DES là?

A. 2, 4, 6, 8, 12, 14, 16, 18

B. 2, 4, 8, 16, 24, 32, 48, 64

☒ C. 8, 16, 24, 32, 40, 48, 56, 64

D. 4, 8, 16, 24, 32, 40, 48, 64

Câu 16. Hệ mật SHA-512 có thể sử dụng để tính giá trị băm của bản tin có độ dài tối đa bao nhiêu bit?

A. $2^{256}-1$

☒ B. $2^{128}-1$

C. $2^{512}-1$

D. $2^{192}-1$

Câu 17. Giá trị hàm Euler - Phi của 787 là?

A. 878

B. 784

C. 785

☒ D. 786

Câu 18. Kết quả của phép tính sau: $3^{201} \pmod{11} = ?$

☒ A. 3

B. 5

C. 6

D. 10

Câu 19. Lựa chọn nào ứng với bản mật khi mật mã hóa bản rõ "dvtbkhk" sử dụng hệ mật mã Affine với khóa mật mã là (18,6)?

A. LDPDZQJT

B. LDPDZOJT

C. LDPOZOJT

D. Không có lựa chọn nào đúng

Câu 20. Chế độ ECB (Electronic Code Book) áp dụng cho hệ mật nào?

A. Hệ mật Caesar

B. Hệ mật dòng

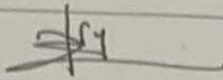

☒ C. Hệ mật khối

D. Hệ mật bất đối xứng

B. TỰ LUẬN (4 điểm)

Xét hệ mật AES-128 với khóa là SEEECRYPTOGRAPHY với bản tin rõ (plaintext) là HAPPYFOREVERYONE. Hãy xác định:

- a. Ma trận khóa gốc và khối trạng thái (state) ứng với bản tin rõ với giả thiết các ký tự được mã hóa theo bảng mã ASCII và các phần tử ma trận thể hiện dưới dạng Hexa;
- b. Khối trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1;
- c. Cột đầu tiên (w_{04}) khóa mở rộng cho vòng 1.

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI TRƯỜNG ĐIỆN - ĐIỆN TỬ Đề số: 01 Tổng số trang: 2		ĐỀ THI GIỮA KỲ 2022.2 Học phần: ET3310 - LÝ THUYẾT MẬT MÃ Ngày thi: 09/06/2023 Thời gian làm bài: 75 phút (Chỉ được sử dụng TL viết tay và bảng in tra cứu. Nộp đề thi cùng với bài làm) Trưởng nhóm chuyên môn: 
Ký duyệt	CBGD phụ trách đề thi: 	

A. TRẮC NGHIỆM (4 điểm)

- Câu 1. Biểu diễn tương ứng với đa thức $x^6 + x^5 + x^2 + x + 1$ trong $GF(2^8)$
 A. 00010011 B. 11000110 C. 00100110 ☒ D. 01100111
- Câu 2. Mật mã hóa bản rõ "cryptophy" sử dụng hệ mật Vignere với từ khóa "LUCKY" cho kết quả bản mật?
 A. nlazeiibljii B. nlazeiibljii C. olaaeiibljki D. mlaaeiibljki ☒
- Câu 3. Đặc tính lầm rối (confusion) của hệ mật che giấu mối liên hệ giữa bản mật (ciphertext) và bản rõ (plaintext)?
☐ A. Đúng ☒ B. Sai
- Câu 4. Khối P-Box được sử dụng để tạo đặc tính phân tán (diffusion) của hệ mật.
☒ A. Đúng B. Sai
- Câu 5. Trường $GF(2)$ bao gồm hai phần tử $\{1, 2\}$ và hai phép toán cộng và nhân.
☐ A. Đúng ☒ B. Sai
- Câu 6. Trong hệ mật DES khóa vòng (round key) gồm ____ bits và khối đầu vào mỗi vòng có độ dài ____ bits.
☒ A. 48, 32 B. 64, 32 C. 56, 24 D. 32, 32
- Câu 7. Tìm nghịch đảo nhân của $(x^7+x+1) \bmod (x^8+x^4+x^3+x+1)$.
 A. x^7+x B. x^6+x^3 ☒ C. x^7 D. x^5+1
- Câu 8. Trong hệ mật DES 64 bit khóa đầu vào được rút ngắn thành 56 bits bằng cách loại bỏ các bit cách nhau 4 bit.
☐ A. Đúng ☒ B. Sai
- Câu 9. Hệ mật AES sử dụng khối đầu vào ____ bits với kích thước khóa ____ bits.
 A. 128; 128 or 256 B. 64; 128 or 192
 C. 256; 128, 192, or 256 ☒ D. 128; 128, 192, or 256
- Câu 10. Cấu trúc hệ mật AES-128 bao hàm ____ vòng tương tự và ____ có sự khác biệt.
 A. 2 cặp 5 vòng; vòng luân phiên ☒ B. 9; vòng cuối
 C. 8; vòng đầu và vòng cuối D. 10; không vòng nào

B. TỰ LUẬN (6 điểm)

Câu 1 (3 điểm):

Xét hệ mật AES-128 với khóa là HUSTALUMINIHOUSE với bản tin rõ (plaintext) là HQ_TÊN của sinh viên (viết HOA, không dấu cách) lấy 16 ký tự (chèn ký tự Z nếu chưa đủ độ dài). Hãy trình bày nguyên lý và xác định giá trị:

- Khởi trạng thái (state) từ bản tin rõ đã cho và được mã hóa theo bảng mã ASCII. Giá trị các phần tử của ma trận trạng thái thể hiện dưới dạng Hexa.
- Khởi trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1
- Khóa vòng 1
- Khởi trạng thái tạo ra bởi vòng 1

Câu 2 (2 điểm):

Trong DES, cho khóa 64 bits ban đầu vào $K = 0123\ ABCD\ 4567\ 8910$, tìm khóa vòng đầu tiên $K_1 = ?$

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI TRƯỜNG ĐIỆN - ĐIỆN TỬ		ĐỀ THI CUỐI KỲ 2021.2	
Đề số: 01 Tổng số trang: 2		Học phần: ET3310 - LÝ THUYẾT MẬT MÃ	
		Ngày thi: 08/08/2022	
		Thời gian làm bài: 75 phút	
		(Chỉ được sử dụng tài liệu viết tay, bảng in tra cứu và máy tính cầm tay. Nộp đề thi cùng với bài làm)	
Ký duyệt	CBGD phụ trách đề thi:	Trưởng nhóm chuyên môn:	
	<i>[Signature]</i>	<i>[Signature]</i>	

A. TRẮC NGHIỆM (5 điểm, mỗi câu chọn 1 ý đúng duy nhất, làm vào giấy thi)

Câu 1. Sử dụng hệ mật Caesar để giải bản mật HQFUBSWHG WHAW cho kết quả bản rõ nào?

- ☒ A. ABANDONED LOCK ☒ B. ENCRYPTED TEXT

Chọn K

C. ABANDONED TEXT

D. ENCRYPTED LOCK

Câu 2. Nghịch đảo nhân của 550 trong tập Z_{1769} là

A. 434 B. 224

☒ C. 550

D. Không tồn tại

Nhân mod $1769 = 1$

Câu 3. Biểu diễn tương ứng với đa thức $x^6 + x^5 + x^2 + x + 1$ trong $GF(2^8)$

A. 00010011

B. 11000110

C. 00100110

☒ D. 01100111

Câu 4. Mật mã hóa bản rõ "cryptography" sử dụng hệ mật Vignere với từ khóa "LUCKY" cho kết quả bản mật?

☒ A. nlazratknss

B. nlazratknii

C. olaaeiibjlsj

D. mlaaeiibljis

Câu 5. Hệ mật DES bao gồm _____ rounds (vòng lặp) với mỗi khóa vòng riêng rẽ.

A. 12

B. 18

C. 9

☒ D. 16

Câu 6. Đặc tính lầm rối (confusion) của hệ mật che giấu mối liên hệ giữa bản mật (ciphertext) và bản rõ (plaintext)?

A. Đúng

☒ B. Sai

Câu 7. Khối P-Box được sử dụng để tạo đặc tính phân tán (diffusion) của hệ mật.

☒ A. Đúng

B. Sai

Câu 8. Tương tự như hệ mật DES, hệ mật AES cũng sử dụng cấu trúc Feistel.

A. Đúng

☒ B. Sai

nhỏ

Câu 9. Trong toán học modun: $(a/b) = a(b^{-1})$

A. Đúng

☒ B. Sai

Câu 10. Trường $GF(2)$ bao gồm hai phần tử $\{1, 2\}$ và hai phép toán cộng và nhân.

A. Đúng

☒ B. Sai

1, 0, 1

Câu 11. Xác định giá trị $2022^{123} \bmod 13 =$

A. 3

B. 7

☒ C. 5

D. 15

Câu 12. Trong hệ mật DES khóa vòng (round key) gồm _____ bits và khối đầu vào mỗi vòng có độ dài _____ bits.

☒ A. 48, 32

B. 64, 32

C. 56, 24

D. 32, 32

Câu 13. Nhân hai đa thức $(x^6 + x^4 + x^2 + x + 1)$ và $(x^7 + x + 1)$ trong $GF(2^8)$ với đa thức tối giản $(x^8 + x^4 + x^3 + x + 1)$ cho kết quả?

A. $x^7 + x^6 + x^3 + x^2 + 1$

B. $x^6 + x^5 + x^2 + x + 1$

☒ C. $x^7 + x^6 + 1$

D. $x^7 + x^6 + x + 1$

Câu 14. Số vòng (rounds) hệ mật AES-256 thực thi?

A. 10

B. 12

☒ C. 14

D. 16

192 - 12

128 - 10

256 - 14

Câu 15. Nghịch đảo nhân của $(x^7 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$?

A. $x^7 + x$

B. $x^6 + x^3$

☒ C. x^7

D. $x^5 + 1$

Câu 16. Thuật toán nào được lựa chọn cho hệ mật AES?

- A. MARS B. Blowfish C. RC6 D. Rijndael

Câu 17. Khối đầu vào mỗi vòng trong hệ mật DES được mở rộng từ 32 bits thành 48 bits thông qua cơ chế

- A. Mở rộng đồng bit hiện có B. Thêm số ngẫu nhiên
C. Thêm các bit 0 D. Thêm các bit 1

Câu 18. Kích thước của mỗi từ (Word) của hệ băm SHA-512 khi sử lý khối dữ liệu 1024- bit?

- A. 64 bits B. 128 bits C. 512 bits D. 256 bits

Câu 19. Trong hệ mật DES 64 bits khóa đầu vào được rút ngắn thành 56 bits bằng cách loại bỏ các bit cách nhau 4 bit.

- A. Đúng B. Sai

Câu 20. Hệ mật AES sử dụng khối đầu vào _____ bits với kích thước khóa _____ bits.

- A. 128; 128 or 256 B. 64; 128 or 192
C. 256; 128, 192, or 256 D. 128; 128, 192, or 256

Câu 21. Tập {1, 2, 3, 9, 14, 34} là tập siêu tăng (superincreasing).

- A. Đúng B. Sai

Câu 22. Cấu trúc hệ mật AES-128 bao gồm _____ vòng tương tự và _____ có sự khác biệt.

- A. 2 cặp 5 vòng ; vòng luân phiên B. 9 ; vòng cuối
C. 8 ; vòng đầu và vòng cuối D. 10 ; không vòng nào

Câu 23. Để tạo ra chữ ký số (digital signatures) giá trị băm của bản tin đầu vào được mật mã hóa với khóa công khai của người tạo chữ ký số.

- A. Đúng B. Sai

Câu 24. Xét hệ mật Knapsack có khóa bí mật {1 6 8 15 24}, hãy xác định giá trị bản mật ứng với bản rõ 10011.

- A. 40 B. 22 C. 31 D. 47

Câu 25. Bản tin đầu vào hệ băm SHA-512 được chèn để có độ dài thỏa mãn tiêu chí nào?

- A. $832 \bmod 1024$ B. $768 \bmod 1024$ C. $960 \bmod 1024$ D. $896 \bmod 1024$

B. TỰ LUẬN (5 điểm)

Câu 1 (2 điểm):

Cho hai số nguyên tố $p=17$ và $q=31$. Hãy sử dụng thuật toán RSA để thực hiện:

- Xác định cặp khóa công khai (n, e) , cặp khóa bí mật (n, d) dựa trên hai số p, q đã cho?
- Cho bản tin rõ là giá trị bảng mã ASCII của chữ cái thứ hai (viết HOA theo hệ Latin) trong tên của sinh viên, hãy thực hiện phép mật mã hóa và kiểm tra kết quả sau khi giải mật mã?

Câu 2 (3 điểm):

Xét hệ mật AES-128 với khóa là HUSTALUMINIHOUSE với bản tin rõ (plaintext) là HQ TÊN của sinh viên (viết HOA, không dấu cách) lấy 16 ký tự (chèn ký tự Z nếu chưa đủ độ dài). Hãy trình bày nguyên lý và xác định giá trị:

- Khối trạng thái (state) từ bản tin rõ đã cho và được mã hóa theo bảng mã ASCII. Giá trị các phần tử của ma trận trạng thái thể hiện dưới dạng Hexa.
- Khối trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1.
- Byte đầu tiên của khối trạng thái tạo ra bởi bước biến đổi Mix Column của vòng 1.

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI TRƯỜNG ĐIỆN - ĐIỆN TỬ Đề số: 02 Tổng số trang: 2		ĐỀ THI CUỐI KỲ 2022.1 Học phần: ET3310 – LÝ THUYẾT MẬT MÃ Ngày thi: 08/03/2023 Thời gian làm bài: 60 phút (Được sử dụng tài liệu, bản in bảng tra cứu, máy tính cầm tay. Nộp đề thi cùng với bài làm) Trưởng nhóm chuyên môn:
Ký duyệt	CBGD phụ trách đề thi:	

A. TRẮC NGHIỆM (6 điểm, mỗi câu chọn 1 ý đúng duy nhất, làm vào giấy thi)

Câu 1. Tiến trình mật mã hóa chuyển đổi bản rõ thành bản mật thực hiện ở đâu?

- ☒ A. Máy phát dữ liệu B. Máy nhận dữ liệu
☐ C. Kênh truyền D. Cả A,B,C

Câu 2. Hệ mật AES theo tiêu chuẩn FIPS PUB 197 có ba cấu hình khác nhau về độ dài khóa và?

- ☒ A. Kích thước khối dữ liệu State B. Kiểu dữ liệu đầu vào hệ mật
☐ C. Số vòng (rounds) D. Kiểu mật mã hóa từng vòng

Câu 3. Tiến trình tạo chữ ký số (Digital Signature) bên gửi sử dụng ...?

- ☐ A. Khóa công khai ☒ B. Khóa bí mật C. A và B D. Khóa vòng

Câu 4. Chế độ CBC (Cipher Block Chaining) áp dụng cho hệ mật nào?

- ☒ A. Hệ mật Caesar B. Hệ mật dòng
☐ C. Hệ mật khối D. Hệ mật bất đối xứng

Câu 5. Hệ mật Triple DES hoạt động sử dụng bao nhiêu khóa?

- ☐ A. 5 B. 4 ☒ C. 3 D. 2

Câu 6. Hệ mật AES hoạt động ở cấu hình khóa có độ dài 256 bit thực hiện bao nhiêu vòng (rounds)?

- ☐ A. 10 B. 12 ☒ C. 14 D. 16

Câu 7. Thao tác "Tráo Byte (SubBytes)" được thực hiện tại bước ... trong mỗi round của hệ mật AES.

- ☒ A. 1 B. 2 C. 3 D. 4

Câu 8. Đa thức tối giản nào được sử dụng trong mã AES là đa thức nào dưới đây?

- ☐ A. $x^4 + x^3 + x + 1$ B. $x^{16} + x^5 + x^3 + x + 1$
☒ C. $x^6 + x^3 + x + 1$ ☒ D. $x^8 + x^4 + x^3 + x + 1$

Câu 9. Khóa nào được sử dụng để chuyển bản mật thành bản rõ trong hệ mật RSA?

- ☐ A. Khóa công khai ☒ B. Khóa bí mật C. A và B D. Khóa vòng

Câu 10. Thuật toán Diffie-Helman algorithm được sử dụng cho những ứng dụng nào?

- ☐ A. Digital Signature ☒ B. Key Exchange
☐ C. Decryption D. Authentication

Câu 11. Phần phi tuyến của mã AES là S-box được tính toán trong trường hữu hạn nào?

- ☐ A. GF(2) B. GF(2⁴) ☒ C. GF(2⁸) D. GF(2¹⁶)

Câu 12. Xác định nghịch đảo nhân của $(x^2 + x + 1) \bmod (x^4 + x + 1)$?

- ☐ A. $x^2 + 1$ ☒ B. $x^2 + x$ C. $x^3 + x + 1$ D. $x^3 + x^2 + 1$



Câu 14. Thuật toán nào thực hiện theo các bước dưới đây:

1. p, q – two prime numbers, (private, chosen)
2. $n = p \cdot q$, (public, calculated)
3. e , with $\gcd(\Phi(n), e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
4. $d = e^{-1} \pmod{\Phi(n)}$, (private, calculated)

A. DHKE

B. AES

☒ C. RSA

D. ECC

Câu 15. Các bit dùng để làm bit Parity trong hệ mật DES là?

A. 2, 4, 6, 8, 12, 14, 16, 18

B. 2, 4, 8, 16, 24, 32, 48, 64

☒ C. 8, 16, 24, 32, 40, 48, 56, 64

D. 4, 8, 16, 24, 32, 40, 48, 64

Câu 16. Hệ mật SHA-512 có thể sử dụng để tính giá trị băm của bản tin có độ dài tối đa bao nhiêu bit?

A. $2^{56}-1$

☒ B. $2^{128}-1$

C. $2^{512}-1$

D. $2^{192}-1$

Câu 17. Giá trị hàm Euler - Phi của 787 là?

A. 878

B. 784

C. 785

☒ D. 786

Câu 18. Kết quả của phép tính sau: $3^{201} \pmod{11} = ?$

☒ A. 3

B. 5

C. 6

D. 10

Câu 19. Lựa chọn nào ứng với bản mật khi mật mã hóa bản rõ "dtvtbkhn" sử dụng hệ mật mã Affine với khóa mật mã là (18,6)?

A. LDPDZQJT

B. LDPDZOJT

C. LDPOZOJT

☒ D. Không có lựa chọn nào đúng

Câu 20. Chế độ ECB (Electronic Code Book) áp dụng cho hệ mật nào?

A. Hệ mật Caesar

B. Hệ mật dòng

☒ C. Hệ mật khối

D. Hệ mật bất đối xứng

B. TỰ LUẬN (4 điểm)

Xét hệ mật AES-128 với khóa là SEEECRYPTOGRAPHY với bản tin rõ (plaintext) là HAPPYFOREVERYONE. Hãy xác định:

- a. Ma trận khóa gốc và khối trạng thái (state) ứng với bản tin rõ với giả thiết các ký tự được mã hóa theo bảng mã ASCII và các phần tử ma trận thể hiện dưới dạng Hexa;
- b. Khối trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1;
- c. Cột đầu tiên (w_{04}) khóa mở rộng cho vòng 1.



Được quét bằng CamScanner

Câu 13. Hệ mật SHA-512 có thể sử dụng để tính giá trị băm của bản tin có độ dài tối đa bao nhiêu bit?

- A. $2^{192}-1$ B. $2^{256}-1$ ☒ C. $2^{128}-1$ D. $2^{512}-1$

Câu 14. A mật mã hóa bản rõ "dvtbkhn" sử dụng hệ mật mã Affine với khóa mật mã là (14,4) rồi gửi cho B. Đây là bản mật mã A đã gửi đi?

- A. LDPDZQJT B. LDPOZOJT *fu*
C. LDPDZOJT D. Không có lựa chọn nào đúng

Câu 15. Các bit dùng để làm bit Parity trong hệ mật DES là?

- A. 2, 4, 6, 8, 12, 14, 16, 18 ☒ B. 8, 16, 24, 32, 40, 48, 56, 64
C. 2, 4, 8, 16, 24, 32, 48, 64 D. 4, 8, 16, 24, 32, 40, 48, 64

Câu 16. Thuật toán nào thực hiện theo các bước dưới đây:

1. p, q – two prime numbers, (private, chosen)
2. $n = p \cdot q$, (public, calculated)
3. e , with $\gcd(\Phi(n), e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
4. $d = e^{-1} \pmod{\Phi(n)}$, (private, calculated)

- A. RC4 ☒ B. RSA C. Knapsack D. ECC

Câu 17. Tập $\{1, 3, 6, 13, 27, 52\}$ là tập siêu tăng (superincreasing).

- ☒ A. Đúng B. Sai

Câu 18. Kết quả của phép tính sau: $3^{201} \bmod 11 = ?$

- A. 10 B. 6 C. 5 D. 3

Câu 19. Biểu diễn tương ứng của đa thức $x^6 + x^4 + x^3 + x^2 + x$ trong $GF(2^8)$ là:

- A. 01010111 B. 01001110 C. 01011110 D. 11011010

Câu 20. Giá trị hàm Euler - Phi của 773 là?

- A. 377 B. 770 C. 771 ☒ D. 772

B. TỰ LUẬN (6 điểm)

Xét hệ mật AES-128 với khóa là HUSTCRYPTOGRAPHY và bản tin rõ (plaintext) là SUNSHINEINSUMMER. Hãy xác định:

- a. Ma trận khóa gốc và khối trạng thái (state) ứng với bản tin rõ với giả thiết các ký tự được mã hóa theo bảng mã ASCII và các phần tử ma trận thể hiện dưới dạng Hexa;
- b. Khối trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1;
- c. Cột đầu tiên (w_{04}) của khóa mở rộng cho vòng 1.

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
TRƯỜNG ĐIỆN - ĐIỆN TỬ

Đề số: 02 Tổng số trang: 2

ĐỀ THI CUỐI KỲ 2022.1

Học phần: ET3310 - LÝ THUYẾT MẬT MÃ

Ngày thi: 08/03/2023

Thời gian làm bài: 60 phút

(Được sử dụng tài liệu, bản in bảng tra cứu, máy tính cầm tay. Nộp đề thi cùng với bài làm)

Trưởng nhóm chuyên môn:

Ký
duyet

CBGD phụ trách đề thi:

A. TRẮC NGHIỆM (6 điểm, mỗi câu chọn 1 ý đúng duy nhất, làm vào giấy thi)

Câu 1. Tiến trình mật mã hóa chuyển đổi bản rõ thành bản mật thực hiện ở đâu ?

- A. Máy phát dữ liệu
B. Máy nhận dữ liệu
C. Kênh truyền
D. Cả A,B,C

Câu 2. Hệ mật AES theo tiêu chuẩn FIPS PUB 197 có ba cấu hình khác nhau về độ dài khóa và ?

- A. Kích thước khối dữ liệu State
B. Kiểu dữ liệu đầu vào hệ mật
C. Số vòng (rounds)
D. Kiểu mật mã hóa từng vòng

Câu 3. Tiến trình tạo chữ ký số (Digital Signature) bên gửi sử dụng _____ ?

- A. Khóa công khai
B. Khóa bí mật
C. A và B
D. Khóa vòng

Câu 4. Chế độ CBC (Cipher Block Chaining) áp dụng cho hệ mật nào?

- A. Hệ mật Caesar
B. Hệ mật dòng
C. Hệ mật khối
D. Hệ mật bất đối xứng

Câu 5. Hệ mật Triple DES hoạt động sử dụng bao nhiêu khóa?

- A. 5
B. 4
C. 3
D. 2

Câu 6. Hệ mật AES hoạt động ở cấu hình khóa có độ dài 256 bit thực hiện bao nhiêu vòng (rounds)?

- A. 10
B. 12
C. 14
D. 16

Câu 7. Thao tác "Tráo Byte (SubBytes)" được thực hiện tại bước ____ trong mỗi round của hệ mật AES.

- A. 1
B. 2
C. 3
D. 4

Câu 8. Đa thức tối giản nào được sử dụng trong mã AES là đa thức nào dưới đây?

- A. $x^4 + x^3 + x + 1$
B. $x^{16} + x^5 + x^3 + x + 1$
C. $x^6 + x^3 + x + 1$
D. $x^8 + x^4 + x^3 + x + 1$

Câu 9. Khóa nào được sử dụng để chuyển bản mật thành bản rõ trong hệ mật RSA?

- A. Khóa công khai
B. Khóa bí mật
C. A và B
D. Khóa vòng

Câu 10. Thuật toán Diffie-Helman algorithm được sử dụng cho những ứng dụng nào?

- A. Digital Signature
B. Key Exchange
C. Decryption
D. Authentication

Câu 11. Phần phi tuyến của mã AES là S-box được tính toán trong trường hữu hạn nào?

- A. $GF(2)$
B. $GF(2^4)$
C. $GF(2^8)$
D. $GF(2^{16})$

Câu 12. Xác định nghịch đảo nhân của $(x^2 + x + 1) \bmod (x^4 + x + 1)$?

- A. $x^2 + 1$
B. $x^2 + x$
C. $x^3 + x + 1$
D. $x^3 + x^2 + 1$

- Câu 16. Nghịch đảo nhân của $(x^7+x+1) \bmod (x^8 + x^4 + x^3 + x + 1)$?
 A. x^7 B. x^7+x^3 C. x^7+1 D. x^5+1
- Câu 17. Khối đầu vào vòng 2 trong hệ mật DES mở rộng từ 32 bits thành 48 bits thông qua cơ chế?
☒ A. Mở rộng dùng bit hiện có B. Thêm số ngẫu nhiên
 C. Thêm các bit 0 D. Thêm các bit 1
- Câu 18. Số bit biểu diễn giá trị đầu ra của hệ băm SHA512 khi xử lý khối dữ liệu 10^6 bit?
 A. 64 bits B. 128 bits C. 512 bits D. 256 bits
- Câu 19. Trong hệ mật DES 64 bits khóa đầu vào được rút ngắn thành 56 bits bằng cách loại bỏ các bit cách nhau 8 bit.
☒ A. Đúng B. Sai
- Câu 20. Hệ mật AES sử dụng khối đầu vào _____ bits với kích thước khóa _____ bits.
 A. 128; 128 or 256 B. 64; 128 or 192
 C. 256; 128, 192, or 256 ☒ D. 128; 128, 192, or 256
- Câu 21. Tập $\{1, 3, 12, 9, 24, 54\}$ là tập siêu tăng (superincreasing).
☒ A. Đúng ☒ B. Sai
- Câu 22. Cấu trúc hệ mật AES-192 sử dụng khóa có độ dài _____ bits và lặp _____ vòng.
 A. 128; 10 B. 128; 12 C. 192, 12 D. 256; 14
- Câu 23. Để tạo ra chữ ký số (digital signatures) giá trị băm của bản tin đầu vào được mật mã hóa với khóa bí mật của người tạo chữ ký số.
☒ A. Đúng B. Sai
- Câu 24. Số phần tử đồng dư với 49 trong tập Z_{49} là
 A. 40 B. 36 C. 31 D. 7
- Câu 25. Bản tin đầu vào hệ băm SHA-512 được chèn để có độ dài thỏa mãn tiêu chí nào?
 A. $698 \bmod 1024$ B. $896 \bmod 1024$ C. $512 \bmod 1024$ D. $968 \bmod 1024$

B. TỰ LUẬN (5 điểm)

Giải thiết Bình muốn trao đổi dữ liệu với An sử dụng hệ mật Elgamal, lựa chọn số nguyên tố $p = 17$, (primitive root). An và Bình lựa chọn và giữ kín $a = 15$ và Bình giữ kín $b = 13$ để thực thi thuật toán Γ nhằm trao đổi khóa bí mật. An mật mã hóa bản tin có giá trị $M = 6$ (chữ "G" trong bảng mã ký tự tiếp ứng với tập Z_{26}) và gửi cho Bình.

Hãy thực hiện các nội dung sau:

- Xác định giá trị khóa công khai của An và Bình sử dụng để trao đổi khóa bí mật
- Xác định giá trị khóa bí mật sử dụng để mật mã hóa dữ liệu trao đổi giữa An và Bình
- Vẽ hình minh họa mô tả nguyên lý trao đổi khóa sử dụng thuật toán DHKE và mật mã hóa sử dụng thuật toán Elgamal.
- Xác định bản tin mật An gửi cho Bình
- Bản tin Bình khôi phục ứng với bản tin mật An gửi.

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI TRƯỜNG ĐIỆN – ĐIỆN TỬ		ĐỀ THI CUỐI KỲ 2021.2	
Đề số: 01	Tổng số trang: 2	Học phần: ET3310 – LÝ THUYẾT MẬT MÃ	Ngày thi: 05/08/2023
Ký duyệt		Thời gian làm bài: 75 phút (Chỉ được sử dụng tài liệu in và máy tính cầm tay. Nộp đề thi cùng với bài làm)	
CBGD phụ trách đề thi: PGS.TS. Đỗ Trọng Tuấn		Trưởng nhóm chuyên môn: PGS.TS. Hà Duyên Trung	

A. TRẮC NGHIỆM (5 điểm, mỗi câu chọn 1 ý đúng duy nhất, làm vào giấy thi)

- Câu 1. Hệ thống truyền thông áp dụng mật mã khóa công khai sử dụng để mật mã dữ liệu.
A. 1 khóa ☒ B. 2 khóa C. 3 khóa D. 4 khóa
- Câu 2. Thuật ngữ..... thể hiện tính chất của tiến trình truyền đạt thông tin giữa những người dùng hợp pháp một cách bí mật ở định dạng không thể hoặc rất khó đọc được.
☒ A. Cryptography B. Symmetricity C. Asymmetricity D. Cả A, B, C
- Câu 3: Tiến trình mật mã hóa đầu cuối diễn ra ở thành phần nào trong hệ thống truyền thông?
A. Bên gửi B. Bên nhận C. Kênh truyền ☒ D. Cả A và B
- Câu 4: Hệ mật Caesar là một ví dụ của
A. Hệ mật nhân ☒ B. Hệ mật dịch C. Hệ mật lặp D. Không có ý đúng
- Câu 5: Bản tin 1000 bits được mật mã hóa bởi hệ mật dòng sẽ cho đầu ra là bits.
A. 500 ☒ B. 1000 C. 1100 D. 1200
- Câu 6. Loại hệ mật nào dưới đây sử dụng chung khóa để mật mã hóa và giải mật mã hóa:
☒ A. Symmetric key ~~B. Asymmetric key~~ C. Public key D. Cả A và B
- Câu 7. Biểu diễn tương ứng với đa thức $x^6 + x^5 + x^3 + x + 1$ trong $GF(2^8)$
A. 00101010 B. 11000110 C. 00010011 ☒ D. 01101011
- Câu 8. Mật mã hóa bản rõ "kryptosgraphein" sử dụng hệ mật Vignere với từ khóa "HUST" cho kết quả bản mật?
A. lrzrzatknss ☒ B. rlqiaikzyuhalf C. olaeiiblsicf D. lrqiaikzyuhalf
- Câu 9. Thuật toán mật mã nào dưới đây được chuẩn hóa năm 2001 nhằm thay thế hệ mật DES.
☒ A. Rijndael B. Knapsack C. RC4 D. RSA
- Câu 10. Trong mật mã khối, kỹ thuật nào tạo ra yếu tố khuếch tán (diffusion)?
☒ A. Hoán vị sử dụng bảng tra cứu B. Thay thế bit bằng cách sử dụng S-Box
C. Sử dụng nhiều khóa D. Sử dụng bộ sinh khóa tự động
- Câu 11. Một hệ mật sử dụng kỹ thuật nào khi thực hiện mật mã hóa bằng cách mã xáo trộn các chữ cái vào các vị trí khác nhau.
A. Substitution B. Stream C. Running key ☒ D. Transposition
- Câu 12. Trường $GF(2^8)$ bao gồm 8 phần tử và hai phép toán cộng và nhân.
A. Đúng ☒ B. Sai ~~256 phần tử~~
- Câu 13. Xác định giá trị $45^{17} \bmod 101 =$
A. 31 B. 17 C. 47 D. 45
- Câu 14. AES sử dụng S-box để làm gì trong quá trình mật mã hóa?
☒ A. Thay thế các phần tử B. Sinh khóa C. Trao đổi khóa D. Hoán vị các phần tử
- Câu 15. Nhân hai đa thức (x^2+x+1) và (x^2+1) trong trường GF với đa thức tối giản (x^3+x+1) cho kết quả
A. x^2+1 ☒ B. x^2+x C. x^3+1 D. $x+1$

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI TRƯỜNG ĐIỆN - ĐIỆN TỬ		ĐỀ THI CUỐI KỲ 2021.2	
Đề số: 01		Học phần: ET3310 - LÝ THUYẾT MẬT MÃ	
Tổng số trang: 2		Ngày thi: 08/08/2022	
		Thời gian làm bài: 75 phút	
		(Chỉ được sử dụng tài liệu viết tay, bảng in tra cứu và máy tính cầm tay. Nộp đề thi cùng với bài làm)	
Ký duyệt	CBGD phụ trách đề thi:	Trưởng nhóm chuyên môn:	
	<i>Đinh Thị Thuần</i>	<i>Hồ Đuỳnh Truong</i>	

A. TRẮC NGHIỆM (5 điểm, mỗi câu chọn 1 ý đúng duy nhất, làm vào giấy thi)

- Câu 1. Sử dụng hệ mật Caesar để giải bản mật HQFUBSWHG WHAW cho kết quả bản rõ nào?
A. ABANDONED LOCK B. ENCRYPTED TEXT
C. ABANDONED TEXT D. ENCRYPTED LOCK
- Câu 2. Nghịch đảo nhân của 550 trong tập Z_{1769} là
A. 434 B. 224 C. 550 D. Không tồn tại
- Câu 3. Biểu diễn tương ứng với đa thức $x^6 + x^5 + x^2 + x + 1$ trong $GF(2^8)$
A. 00010011 B. 11000110 C. 00100110 D. 01100111
- Câu 4. Mật mã hóa bản rõ "cryptography" sử dụng hệ mật Vignere với từ khóa "LUCKY" cho kết quả bản mật?
A. nlazrzatknss B. nlazrzatknii C. olaaeiiblsj D. mlaaeiiblsj
- Câu 5. Hệ mật DES bao gồm _____ rounds (vòng lặp) với mỗi khóa vòng riêng rẽ.
A. 12 B. 18 C. 9 D. 16
- Câu 6. Đặc tính làm rối (confusion) của hệ mật che giấu mối liên hệ giữa bản mật (ciphertext) và bản rõ (plaintext)?
A. Đúng B. Sai
- Câu 7. Khối P-Box được sử dụng để tạo đặc tính phân tán (diffusion) của hệ mật.
A. Đúng B. Sai
- Câu 8. Tương tự như hệ mật DES, hệ mật AES cũng sử dụng cấu trúc Feistel.
A. Đúng B. Sai
- Câu 9. Trong toán học modun: $(a/b) = a(b^{-1})$
A. Đúng B. Sai
- Câu 10. Trường $GF(2)$ bao gồm hai phần tử $\{1, 2\}$ và hai phép toán cộng và nhân.
A. Đúng B. Sai
- Câu 11. Xác định giá trị $2022^{123} \bmod 13 =$
A. 3 B. 7 C. 5 D. 15
- Câu 12. Trong hệ mật DES khóa vòng (round key) gồm _____ bits và khối đầu vào mỗi vòng có độ dài _____ bits.
A. 48, 32 B. 64, 32 C. 56, 24 D. 32, 32
- Câu 13. Nhân hai đa thức $(x^6 + x^4 + x^2 + x + 1)$ và $(x^7 + x + 1)$ trong $GF(2^8)$ với đa thức tối giản $(x^8 + x^4 + x^3 + x + 1)$ cho kết quả?
A. $x^7 + x^6 + x^3 + x^2 + 1$ B. $x^6 + x^5 + x^2 + x + 1$ C. $x^7 + x^6 + 1$ D. $x^7 + x^6 + x + 1$
- Câu 14. Số vòng (rounds) hệ mật AES-256 thực thi?
A. 10 B. 12 C. 14 D. 16
- Câu 15. Nghịch đảo nhân của $(x^7 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$?
A. $x^7 + x$ B. $x^6 + x^3$ C. x^7 D. $x^5 + 1$

Câu 13. Hệ mật SHA-512 có thể sử dụng để tính giá trị băm của bản tin có độ dài tối đa bao nhiêu bit?

- A. $2^{192}-1$ B. $2^{256}-1$ C. $2^{128}-1$ D. $2^{512}-1$

Câu 14. A mật mã hóa bản rõ "dvtbkhk" sử dụng hệ mật mã Affine với khóa mật mã là (14,4) rồi gửi cho B. Đây là bản mật mã A đã gửi đi?

- A. LDPDZQJT B. LDPOZOJT
C. LDPDZOJT D. Không có lựa chọn nào đúng

Câu 15. Các bit dùng để làm bit Parity trong hệ mật DES là?

- A. 2, 4, 6, 8, 12, 14, 16, 18 B. 8, 16, 24, 32, 40, 48, 56, 64
C. 2, 4, 8, 16, 24, 32, 48, 64 D. 4, 8, 16, 24, 32, 40, 48, 64

Câu 16. Thuật toán nào thực hiện theo các bước dưới đây:

1. p, q – two prime numbers, (private, chosen)
2. $n = p \cdot q$, (public, calculated)
3. e , with $\gcd(\Phi(n), e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
4. $d = e^{-1} \pmod{\Phi(n)}$, (private, calculated)

- A. RC4 B. RSA C. Knapsack D. ECC

Câu 17. Tập $\{1, 3, 6, 13, 27, 52\}$ là tập siêu tăng (superincreasing).

- A. Đúng B. Sai

Câu 18. Kết quả của phép tính sau: $3^{201} \pmod{11} = ?$

- A. 10 B. 6 C. 5 D. 3

Câu 19. Biểu diễn tương ứng của đa thức $x^6 + x^4 + x^3 + x^2 + x$ trong $GF(2^8)$ là:

- A. 01010111 B. 01001110 C. 01011110 D. 11011010

Câu 20. Giá trị hàm Euler - Phi của 773 là?

- A. 377 B. 770 C. 771 D. 772

B. TỰ LUẬN (6 điểm)

Xét hệ mật AES-128 với khóa là **HUSTCRYPTOGRAPHY** và bản tin rõ (plaintext) là **SUNSHINEINSUMMER**. Hãy xác định:

- a. Ma trận khóa gốc và khối trạng thái (state) ứng với bản tin rõ với giả thiết các ký tự được mã hóa theo bảng mã ASCII và các phần tử ma trận thể hiện dưới dạng Hexa;
- b. Khối trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1;
- c. Cột đầu tiên (w_{04}) của khóa mở rộng cho vòng 1.

Câu 16. Thuật toán nào được lựa chọn cho hệ mật AES?

- A. MARS B. Blowfish C. RC6 D. Rijndael

Câu 17. Khối đầu vào mỗi vòng trong hệ mật DES được mở rộng từ 32 bits thành 48 bits thông qua cơ chế

- ☒ A. Mở rộng đồng bit hiện có B. Thêm số ngẫu nhiên
☐ C. Thêm các bit 0 D. Thêm các bit 1

Câu 18. Kích thước của mỗi từ (Word) của hệ băm SHA-512 khi sử lý khối dữ liệu 1024- bit?

- A. 64 bits B. 128 bits C. 512 bits D. 256 bits

Câu 19. Trong hệ mật DES 64 bits khóa đầu vào được rút ngắn thành 56 bits bằng cách loại bỏ các bit cách nhau 4 bit.

- A. Đúng B. Sai

Câu 20. Hệ mật AES sử dụng khối đầu vào _____ bits với kích thước khóa _____ bits.

- A. 128; 128 or 256 B. 64; 128 or 192
C. 256; 128, 192, or 256 D. 128; 128, 192, or 256

Câu 21. Tập $\{1, 2, 3, 9, 14, 34\}$ là tập siêu tăng (superincreasing).

- A. Đúng B. Sai

Câu 22. Cấu trúc hệ mật AES-128 bao gồm _____ vòng tương tự và _____ có sự khác biệt.

- A. 2 cặp 5 vòng; vòng luân phiên B. 9; vòng cuối
C. 8; vòng đầu và vòng cuối D. 10; không vòng nào

Câu 23. Để tạo ra chữ ký số (digital signatures) giá trị băm của bản tin đầu vào được mật mã hóa với khóa công khai của người tạo chữ ký số.

- A. Đúng B. Sai

Câu 24. Xét hệ mật Knapsack có khóa bí mật $\{1, 6, 8, 15, 24\}$, hãy xác định giá trị bản mật ứng với bản rõ 10011.

- A. 40 B. 22 C. 31 D. 47

Câu 25. Bản tin đầu vào hệ băm SHA-512 được chèn để có độ dài thỏa mãn tiêu chí nào?

- A. $832 \bmod 1024$ B. $768 \bmod 1024$ C. $960 \bmod 1024$ ☒ D. $896 \bmod 1024$

B. TỰ LUẬN (5 điểm)

Câu 1 (2 điểm):

Cho hai số nguyên tố $p=17$ và $q=31$. Hãy sử dụng thuật toán RSA để thực hiện:

- Xác định cặp khóa công khai (n, e) , cặp khóa bí mật (n, d) dựa trên hai số p, q đã cho?
- Cho bản tin rõ là giá trị bảng mã ASCII của chữ cái thứ hai (viết HOA theo hệ Latin) trong tên của sinh viên, hãy thực hiện phép mật mã hóa và kiểm tra kết quả sau khi giải mật mã?

Câu 2 (3 điểm):

Xét hệ mật AES-128 với khóa là HUSTALUMINIHOUSE với bản tin rõ (plaintext) là HỌ TÊN của sinh viên (viết HOA, không dấu cách) lấy 16 ký tự (chèn ký tự Z nếu chưa đủ độ dài). Hãy trình bày nguyên lý và xác định giá trị:

- Khối trạng thái (state) từ bản tin rõ đã cho và được mã hóa theo bảng mã ASCII. Giá trị các phần tử của ma trận trạng thái thể hiện dưới dạng Hexa.
- Khối trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1.
- Byte đầu tiên của khối trạng thái tạo ra bởi bước biến đổi Mix Column của vòng 1.

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
TRƯỜNG ĐIỆN - ĐIỆN TỬ

Đề số: 02 Tổng số trang: 2

ĐỀ THI CUỐI KỲ 2022.1

Học phần: ET3310 - LÝ THUYẾT MẬT MÃ

Ngày thi: 08/03/2023

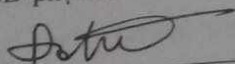
Thời gian làm bài: 60 phút

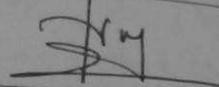
(Được sử dụng tài liệu, bản in bảng tra cứu, máy tính cầm tay. Nộp đề thi cùng với bài làm)

Trưởng nhóm chuyên môn:

Ký
duyet

CBGD phụ trách đề thi:





A. TRẮC NGHIỆM (6 điểm, mỗi câu chọn 1 ý đúng duy nhất, làm vào giấy thi)

Câu 1. Tiến trình mật mã hóa chuyển đổi bản rõ thành bản mật thực hiện ở đâu?

- A. Máy phát dữ liệu
B. Máy nhận dữ liệu
C. Kênh truyền
D. Cả A,B,C

Câu 2. Hệ mật AES theo tiêu chuẩn FIPS PUB 197 có ba cấu hình khác nhau về độ dài khóa và?

- A. Kích thước khối dữ liệu State
B. Kiểu dữ liệu đầu vào hệ mật
C. Số vòng (rounds)
D. Kiểu mật mã hóa từng vòng

Câu 3. Tiến trình tạo chữ ký số (Digital Signature) bên gửi sử dụng _____?

- A. Khóa công khai
B. Khóa bí mật
C. A và B
D. Khóa vòng

Câu 4. Chế độ CBC (Cipher Block Chaining) áp dụng cho hệ mật nào?

- A. Hệ mật Caesar
B. Hệ mật dòng
C. Hệ mật khối
D. Hệ mật bất đối xứng

Câu 5. Hệ mật Triple DES hoạt động sử dụng bao nhiêu khóa?

- A. 5
B. 4
C. 3
D. 2

Câu 6. Hệ mật AES hoạt động ở cấu hình khóa có độ dài 256 bit thực hiện bao nhiêu vòng (rounds)?

- A. 10
B. 12
C. 14
D. 16

Câu 7. Thao tác "Tráo Byte (SubBytes)" được thực hiện tại bước _____ trong mỗi round của hệ mật AES.

- A. 1
B. 2
C. 3
D. 4

Câu 8. Đa thức tối giản nào được sử dụng trong mã AES là đa thức nào dưới đây?

- A. $x^4 + x^3 + x + 1$
B. $x^{16} + x^5 + x^3 + x + 1$
C. $x^6 + x^3 + x + 1$
D. $x^8 + x^4 + x^3 + x + 1$

Câu 9. Khóa nào được sử dụng để chuyển bản mật thành bản rõ trong hệ mật RSA?

- A. Khóa công khai
B. Khóa bí mật
C. A và B
D. Khóa vòng

Câu 10. Thuật toán Diffie-Helman algorithm được sử dụng cho những ứng dụng nào?

- A. Digital Signature
B. Key Exchange
C. Decryption
D. Authentication

Câu 11. Phần phi tuyến của mã AES là S-box được tính toán trong trường hữu hạn nào?

- A. $GF(2)$
B. $GF(2^4)$
C. $GF(2^8)$
D. $GF(2^{16})$

Câu 12. Xác định nghịch đảo nhân của $(x^2 + x + 1) \bmod (x^4 + x + 1)$?

- A. $x^2 + 1$
B. $x^2 + x$
C. $x^3 + x + 1$
D. $x^3 + x^2 + 1$

Câu 14. Thuật toán nào thực hiện theo các bước dưới đây:

1. p, q – two prime numbers, (private, chosen)
2. $n = p \cdot q$, (public, calculated)
3. e , with $\gcd(\Phi(n), e) = 1$, $1 < e < \Phi(n)$, (public, chosen)
4. $d = e^{-1} \pmod{\Phi(n)}$, (private, calculated)

A. DHKE B. AES C. RSA D. ECC

Câu 15. Các bit dùng để làm bit Parity trong hệ mật DES là?

- A. 2, 4, 6, 8, 12, 14, 16, 18 B. 2, 4, 8, 16, 24, 32, 48, 64
C. 8, 16, 24, 32, 40, 48, 56, 64 D. 4, 8, 16, 24, 32, 40, 48, 64

Câu 16. Hệ mật SHA-512 có thể sử dụng để tính giá trị băm của bản tin có độ dài tối đa bao nhiêu bit?

- A. $2^{256}-1$ B. $2^{128}-1$ C. $2^{512}-1$ D. $2^{192}-1$

Câu 17. Giá trị hàm Euler - Phi của 787 là?

- A. 878 B. 784 C. 785 D. 786

Câu 18. Kết quả của phép tính sau: $3^{201} \pmod{11} = ?$

- A. 3 B. 5 C. 6 D. 10

Câu 19. Lựa chọn nào ứng với bản mật khi mật mã hóa bản rõ "dvtbkh" sử dụng hệ mật mã Affine với khóa mật mã là (18,6)?

- A. LDPDZQJT B. LDPDZOJT
C. LDPOZOJT D. Không có lựa chọn nào đúng

Câu 20. Chế độ ECB (Electronic Code Book) áp dụng cho hệ mật nào?

- A. Hệ mật Caesar B. Hệ mật dòng
C. Hệ mật khối D. Hệ mật bất đối xứng

B. TỰ LUẬN (4 điểm)

Xét hệ mật AES-128 với khóa là **SEEECRYPTOGRAPHY** với bản tin rõ (plaintext) là **HAPPYFOREVERYONE**. Hãy xác định:

- a. Ma trận khóa gốc và khối trạng thái (state) ứng với bản tin rõ với giả thiết các ký tự được mã hóa theo bảng mã ASCII và các phần tử ma trận thể hiện dưới dạng Hexa;
- b. Khối trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1;
- c. Cột đầu tiên (w_{04}) khóa mở rộng cho vòng 1.

