

# ĐỀ 01 - LTMM 2021.2 (75 phút)

## A. TRẮC NGHIỆM (5 điểm)

Câu 1: Sử dụng hệ thống Caesar để giải mã bản tin HQFUBSWHG WHAW cho kết quả bản rõ nào?

A. ABANDONED LOCK  
B. ENCRYPTED TEXT

C. ABANDONED TEXT  
D. ENCRYPTED LOCK

Caesar Cipher (or Additive Cipher / Shift Cipher)

$$\text{Encrypt: } C = (P + K) \bmod 26$$

$$\text{Decrypt: } D = (C - K) \bmod 26.$$

Câu 2: Nghịch đảo nhân của 550 trong tập  $\mathbb{Z}_{1769}$  là:  
A. 434      B. 224      C. 550      D. Không tồn tại.

$$\gcd(550, 1769) = 1$$

	$r_1$	$r_2$	$r$	$t_1$	$t_2$	$t$
9						
3	1769	550	119	0	1	-3
4	550	119	74	1	-3	13
1	119	74	45	-3	13	-16
1	74	45	29	13	-16	29
1	45	29	16	-16	29	-45
1	29	16	13	29	-45	74
1	16	13	3	-45	74	-119
1	13	3	1	74	-119	550
4	3	1	0	-119	550	-1769
3	1	0		550	-1769	
	1	0				

Câu 3: Beispiel tương ứng với đa thức  $x^6 + x^5 + x^2 + x + 1$  trong  $GF(2^8)$ :  
A. 0001 0011      B. 11000110      C. 001 00110      D. 0100011

Câu 4: Bép rõ: "cryptography"  $\xrightarrow{\text{hệ thống Vigenère}}$  Bép mật?

Câu 4: Bép rõ: "cryptography"  $\xrightarrow{\text{từ khóa "LUCKY"}}$  Bép mật?

Plaintext	C	r	y	p	t	o	g	r	a	p	h	y
p's value	2	17	24	15	19	14	6	17	0	15	7	24
Key word	L	U	C	K	Y	L	U	C	K	Y	L	U
Key Stream	11	20	2	10	24	11	20	2	10	24	11	20
c's value	13	11	0	25	17	25	0	19	10	13	18	18
Ciphertext	n	l	a	z	r	t	a	t	k	n	s	s

→ đáp án A

Câu 5: Hệ mật DES bao gồm ... rounds (vòng lặp) với mỗi khóa vòng riêng & nr.  
 A. 12      B. 18      C. 9      D. 16

Câu 6: Đặc tính làm rối (confusion) của hệ mật che giấu mối liên hệ giữa bàn mật và bàn rõ?  
 A. Đúng      B. Sai

Mối quan hệ giữa ciphertext và plaintext  $\rightarrow$  diffusion (P-box)  
 ciphertext và key  $\rightarrow$  confusion. (S-box)

Câu 7: Khối P-boxes etc 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 fracth học moduler:  $(a/b) = a(b^{-1})$   
 A. Đúng      B. Sai.

Câu 10: Trường GF(2) bao gồm hai phần tử  $\{1\}$  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.

$$123_{(10)} = 1111011_{(2)}$$

Chọn falso  $P_1 = 1$ .

$$P_1 = (P_1 \cdot 2022) \bmod 13 \text{ if bit 1}$$

$$P_1 = P_1 \text{ if bit 0}$$

bit	$P_1$	$P_1 = P_1^2 \bmod 13$	
1	1	$1^2 \bmod 13 = 1$	
1	7	$7^2 \bmod 13 = 10$	5
1	5	12	6
1	6	10	5
0	5	12	7
1	12	1	5
1	7	10	

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

A. 48, 32      B. 64, 32      C. 56, 24      D. 32, 32.

Câu 13: Nhập 2 đa thức  $(x^6 + x^4 + x^2 + x + 1)$  và  $(x^7 + x + 1)$  trong GF(2<sup>8</sup>) với đa thức tối giản  $(x^8 + x^4 + x^3 + x + 1)$  cho kết quả?

$$P_1 = x^6 + x^4 + x^2 + x + 1 \quad ; \quad P_2 = x^7 + x + 1.$$

$$\begin{aligned}
 P_1 \times P_2 &= (x^6 + x^4 + x^2 + x + 1) \times (x^7 + x + 1) \\
 &= x^7(x^6 + x^4 + x^2 + x + 1) + x(x^6 + x^4 + x^2 + x + 1) + (x^6 + x^4 + x^2 + x + 1) \\
 &= x^{13} + x^{11} + x^9 + x^8 + x^7 + x^4 + x^5 + x^3 + x^2 + x + x^6 + x^4 + x^2 + x + 1 = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^3 + x^2 + x + 1
 \end{aligned}$$

$$P_1 \times P_2 = (x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) \text{ mod } (x^8 + x^4 + x^3 + x + 1)$$

$$\begin{array}{r} x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\ \hline x^{13} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\ \hline x^{11} + x^7 + x^6 + x^4 + x^3 + 1 \\ \hline x^7 + x^6 + 1 \end{array}$$

→ đáp án C.

Câu 14: Số vòng (rounds) để mật AES-256 thực thi?

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

AES-128 : 10

AES-192 : 12 rounds

AES-256 : 14

\* Câu 15: Nghiên cứu nhân của  $(x^7 + x + 1) \text{ mod } (x^8 + x^4 + x^3 + x + 1)$  ?

A.  $x^7 + x$

B.  $x^6 + x^3$

C.  $x^7$

D.  $x^5 + 1$ .

(?)

$q$	$r_1$	$r_2$	$r$	$t_1$	$t_2$	$t$
$x^2$	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x + 1$	$x^4 + x^3 + x^2 + 1$	0	1	$x$
$x^3 + x^2 + 1$	$x^7 + x + 1$	$x^4 + x^3 + x^2 + 1$	$x$	1	$x$	$x^4 + x^3 + x + 1$
$x^3 + x^2 + 1$	$x^4 + x^3 + x + 1$	$x$	1	$x$	$x^4 + x^3 + x + 1$	$x^7 + x^5 + x^2 + 1$
$x$	$x$	1	0	$x^4 + x^3 + x + 1$	$x^7 + x^5 + x^2 + 1$	
$\rightarrow$	1	0	—			

Câu 16: Thuật toán nào được lựa chọn cho hệ thống AES?

A. MARS

B. Blowfish

C. RCG

D. Rijndael

Câu 17: Khoác đầu vào mỗi vòng trong hệ thống DES được mở rộng từ 32 bits thành 48 bits

thông qua cách.....

A. Nhập rộng dung lượng hiện có

B. Thêm số nguyên 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 xử lý khôi dử liệu  
1024 bit? A. 64 bits B. 128 bits C. 512 bits D. 256 bits.
- Câu 19: Trong hệ mật DES 64 bits khôi dửi vào để nén 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 khôi dửi vào ... bits và kích thước khôi ... 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. Day siêu tăng: nếu mỗi phần tử cuối dài đều lớn hơn tổng các  
phần tử phía trước nó. B. Sai.
- Câu 22: Các khía hệ mật AES-128 bao gồm ... vòng luồng từ và ... có sự khác biệt.  
A. 2 cấp 5 vòng ; vòng biến phiên. B. 9 ; vòng cuối (còn Nix Column) C. 8 ; vòng đầu và vòng cuối D. 10 ; không vòng nào.
- Câu 23: Để tạo ra chữ ký số (digital signatures) gửi trại băm của bản tin đầu vào  
được mã hóa với khóa công khai của người tạo chữ ký số.
- Câu 24: Xét hệ mật knapsack có khóa bí mật  $\{1, 6, 8, 15, 24\}$  hãy xác định  
giá trị ban nhất riêng với bán rõ 10011.  
A. 40 B. 22 C. 31 D. 47

- Câu 25: Ban tin đầu vào hệ băm SHA-512 phải chèn để có độ dài thỏa mãn  
tùy chí nào?  
A.  $832 \bmod 1024$  B.  $768 \bmod 1024$  C.  $960 \bmod 1024$  D.  $896 \bmod 1024$

### B.TỰ LUYÂN (5 điểm)

Câu 1: (2 điểm) Cho hai số nguyên tố  $p=17$  và  $q=31$ . Hãy sử dụng thuật toán RSA:

- Xác định cặp khóa công khai  $(n, e)$ , cặp khóa bí mật  $(n, d)$  dựa trên 2 số  $p, q$  đã cho.
- Cho biết tìn rõ là gtn' bằng mã ASCII của chữ cái thứ 2 (viết hoa theo hệ latin) trong tên của sinh viên, hãy thực hiện phép mã hóa và kiểm tra kết quả sau khi giải mật mã?

Giải:

a) Ta có:  $n = p \cdot q = 17 \cdot 31 = 527$   
 $\varphi(n) = (p-1)(q-1) = (17-1) \cdot (31-1) = 480$

Chọn  $e = 233$  ( $\gcd(233, 480) = 1$ )

Tìm  $d \equiv e^{-1} \pmod{480}$ .

	$r_1$	$r_2$	$r$	$t_1$	$t_2$	$t$
9				0	1	-2
2	480	233	14	1	-2	33
16	233	14	9	-2	33	-35
1	14	9	5	33	-35	68
1	9	5	4	-35	68	-103
1	5	4	1	68	-103	480
4	4	1	0	-103	480	/
/	1	0	/			

$\Rightarrow d \equiv -103 \pmod{480} = 377$ .

Vậy khóa công khai  $(n, e) = (527, 233)$   
 khóa bí mật  $(n, d) = (527, 377)$ .

\* b) plaintext: "N"  $\rightarrow 78$  (ASCII)  $\rightarrow 01001110$

$\Rightarrow C = 78^{233} \pmod{527}$ .

Ta có:  $233 = 11101001_{(2)}$

Khởi tạo  $p_1 = 1$ .

bit	$p_1$	$p_1 = p_1^2 \pmod{527}$	$p_1 = (p_1 \cdot 78) \pmod{527}$ if bit 1 if bit 0
1	1	$1^2 \pmod{527} = 1$	78
1	78	$78^2 \pmod{527} = 287$	252
1	252	$252^2 \pmod{527} = 264$	39
0	39	$39^2 \pmod{527} = 467$	467
1	467	$467^2 \pmod{527} = 438$	436
0	436	$436^2 \pmod{527} = 376$	376
0	376	$376^2 \pmod{527} = 140$	140
1	140	$140^2 \pmod{527} = 101$	500

→ Ciphertext  $C = 500$ .

\* Giải mã & kiểm tra:  $P_{377} = 500^{377} \pmod{527}$ .

Tà có:  $377_{(10)} = 101111001_{(2)}$ . Tính sao  $P_1 = 1$ .

bit	$P_i$	$P_i = P_i^2 \pmod{527}$	$P_i = P_1 \quad \text{if bit 0}$ $P_i = (P_1 \cdot 500) \pmod{527} \quad \text{if bit 1}$
1	1	1	500
0	500	202	202
1	202	225	249
1	249	342	252
1	252	264	250
1	250	314	481
0	481	8	8
0	8	64	64
1	64	407	78

$\Rightarrow P = 78$ . Kiểm tra đúng!

Câu 2: (3 điểm)

Xét hệ thống AES-128 với khóa là HALSTALUMINIHOUSE và bản tin rõ (plain text) là TÊN của nhà nến (viết hoa, không dấu cách) bao gồm 16 ký tự (chứa kí tự Z nếu chưa đủ độ dài). Hãy trình bày nguyên lý và xác định quá trình:

- Khởi động thái (state) từ bản tin rõ đã cho và được mã hóa theo bảng mã ASCII.
- Giai tri các phần tử của ma trận trạng thái hiện diện dưới dạng hexa.
- Khởi động thái khi thực hiện công thức vòng (Add Round Key) trước vòng 1.
- Byte đầu tiên của khởi động thái tạo ra bao nhiêu biến đổi? Max Column của vòng 1.

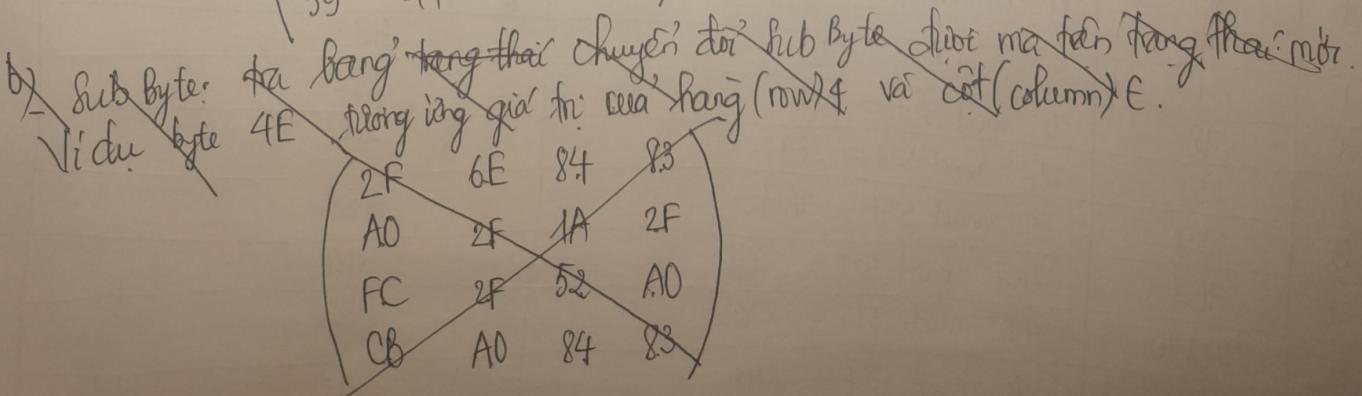
Giai:

Plain text: NGUYEN NGOC HOANGA.

Plain text in hexa: 4E 47 55 59 45 4E 4E 47 4F 43 48 4F 41 4E 47 41

a) Khởi động thái (state) từ bản rõ đã cho:

$$\begin{pmatrix} 4E & 45 & 4F & 41 \\ 47 & 4E & 43 & 4F \\ 55 & 4E & 48 & 47 \\ 59 & 47 & 4F & 41 \end{pmatrix}$$



b) Key: FIRST ALUMINI HOUSE

key in Hexa: 48 55 53 54 41 4C 55 4D 49 4E 49 48 4F 55 53 45  
 ⇒ Roundkey No.0 Matrix:

$$\begin{pmatrix} 48 & 41 & 49 & 4F \\ 55 & 4C & 4E & 55 \\ 53 & 55 & 49 & 53 \\ 54 & 4D & 48 & 45 \end{pmatrix}$$

Thực hiện Add Round key - cộng khóa vòng trước  
 phần tử 8bit trong vòng của state matrix  
 ví dụ:  $4E \oplus 48 = 06$

$$\begin{array}{r} 0100\ 1110 \\ 0100\ 1000 \\ \hline 0000\ 0110 \end{array}$$

$$4F \oplus 49 = 06$$

$$\begin{array}{r} 0100\ 1111 \\ 0100\ 1001 \\ \hline 0000\ 0110 \end{array}$$

$$43 \oplus 4B = 0D$$

$$\begin{array}{r} 0100\ 0011 \\ 0100\ 1110 \\ \hline 0000\ 1101 \end{array}$$

$$48 \oplus 49 = 01$$

$$\begin{array}{r} 0100\ 1000 \\ 0100\ 1001 \\ \hline 0000\ 0001 \end{array}$$

$$41 \oplus 4F = 0E$$

$$\begin{array}{r} 0100\ 0001 \\ 0100\ 1111 \\ \hline 0000\ 1110 \end{array}$$

$$4E \oplus 55 = 1B$$

$$\begin{array}{r} 0100\ 1110 \\ 0101\ 0101 \\ \hline 0001\ 1011 \end{array}$$

$$47 \oplus 53 = 14$$

$$\begin{array}{r} 0100\ 0111 \\ 0101\ 0011 \\ \hline 0001\ 0100 \end{array}$$

vòng 1 bằng cách XOR từng  
 vế Roundkey No.0 matrix.

$$45 \oplus 41 = 04$$

$$\begin{array}{r} 0100\ 0101 \\ 0100\ 0001 \\ \hline 0000\ 0100 \end{array}$$

$$47 \oplus 55 = 12$$

$$\begin{array}{r} 0100\ 0111 \\ 0101\ 0101 \\ \hline 0001\ 0010 \end{array}$$

$$55 \oplus 53 = 06$$

$$\begin{array}{r} 0101\ 0101 \\ 0101\ 0011 \\ \hline 0000\ 0110 \end{array}$$

$$59 \oplus 54 = 0D$$

$$\begin{array}{r} 0100\ 0111 \\ 0101\ 0011 \\ \hline 0001\ 0100 \end{array}$$

$$47 \oplus 4D = 08$$

$$4F \oplus 48 = 07$$

$$41 \oplus 45 = 04$$

$$4E \oplus 4C = 02$$

$$\begin{array}{r} 0100\ 1110 \\ 0100\ 1100 \\ \hline 0000\ 0010 \end{array}$$

$$4E \oplus 55 = 1B$$

$$\begin{pmatrix} 06 & 04 & 06 & 0E \\ 12 & 02 & 0D & 1B \\ 06 & 1B & 01 & 14 \\ 0D & 08 & 07 & 04 \end{pmatrix}$$

Vòng 1: Thực hiện công thức vòng trước:

c) Vòng 1: Thực hiện như sau là:

$$\begin{pmatrix} 06 & 04 & 06 & 0E \\ 12 & 02 & 0D & 1B \\ 06 & 1B & 01 & 14 \\ 0D & 08 & 07 & 04 \end{pmatrix}$$

Thực hiện Substitution Bytes: thay thế mỗi phần tử (bytes) của block matran trạng thái hiện tại bằng giá trị tương ứng ở ABS S-box.

Điều byte AB được thay thế bởi giá trị tạo bởi row 1 và column (col) B là AF.  
 (hang)

S-box	6F	F2	6F	AB
Sub Bytes	82	FF	D7	4F
	6F	4F	7C	FA
	D7	30	C5	F2

- Thực hiện步子 Shift Row:

Shift Row	6F	F2	6F	AB
	FF	D7	4F	82
	7C	FA	6F	4F
	F2	D7	30	C5

hang 1 - gửi nguyên.  
 hang 2 dịch rộng tac 1  
 hang 3 \_\_\_\_\_ 2  
 hang 4 \_\_\_\_\_ 3.

- Mix Column: Nhận ma trận hàng thứ i hiện tại và ma trận cơ định:

02	03	01	01	6F	F2	6F	AB
01	02	03	01	FF	D7	4F	82
01	01	02	03	7C	FA	6F	4F
03	01	01	02	F2	D7	30	C5

Taco:  
 $(02 \cdot 6F) \oplus (03 \cdot FF) \oplus (01 \cdot 7C) \oplus (01 \cdot F2)$

$$\begin{aligned} \text{+) } 02 \cdot 6F &= \cancel{02} \underbrace{0000\ 0010}_{x^6}, \underbrace{0110\ 1111}_{(x^6+x^5+x^3+x^2+x+1)} \\ &= x^7 + x^6 + x^4 + x^3 + x^2 + x \\ &= 1101\ 1110. \end{aligned}$$

$$\begin{aligned} \text{+) } 03 \cdot FF &= 0000\ 0011, \underbrace{0111\ 0111}_{(x+1)(x^6+x^5+x^4+x^2+x+1)} \\ &= x^7 + x^6 + x^5 + x^3 + x^2 + x + x^6 + x^5 + x^4 + x^2 + x + 1 \\ &= x^7 + x^4 + x^3 + 1 \\ &= 1001\ 1001 \end{aligned}$$

$$\text{+) } 01 \cdot 7C = 7C = 0111\ 1100$$

$$\text{+) } 01 \cdot F2 = F2 = 1111\ 0010.$$

Vậy byte đầu tiên của khối hàng thứ i tạo ra bởi bước biến đổi Mix Column của vòng 1 là C9.

$$\left. \begin{array}{r} 1101\ 1110 \\ 1001\ 1001 \\ 0111\ 1100 \\ 11\ 11\ 0010 \\ \hline 1100\ 1001 \end{array} \right\} \text{||} \text{ C9}$$

ĐỀ 01 - LTNM 2022.1. (60 phút)

A. TRẮC NGHIỆM (6 điểm)

Câu 1: Quá trình giải mã hóa chuyển đổi bản mật thành bản rõ thuộc luồng đầu  
A. Máy phát dữ liệu B. Máy nhận dữ liệu C. Kênh truyền D. Các A, B, C.

Câu 2: Hệ mật AES theo tiêu chuẩn FIPS PUB 197 có 3 vòng

(round) và ... ?

A. Kích thước khối dữ liệu State

C. Độ dài khóa

B. Kiểu dữ liệu đầu vào hệ mật

D. Độ dài vòng

Câu 3: Quá trình thêm định chữ ký số (Digital Signature) bên nhận sử dụng ... ?

A. Khoa công khai

B. Khoa bí mật

C. A và B

D. Khoa vòng

Câu 4: Bước đến không king đa thức  $x^7 + x^5 + x^2 + x + 1$  trong  $GF(2^8)$

A. 10010011

B. 11000110

C. 10100110

D. 10100111

$$x^7 + x^5 + x^2 + x + 1 = 1 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0$$

$$= 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1$$

Câu 5: Hệ mật Triple DES hoạt động sử dụng bao nhiêu khóa?  $\sum = 192$  bit.

A. 2

B. 3

C. 4

D. 5

Câu 6: Hệ mật AES hoạt động với các khóa có độ dài 192 bit thực hiện bao nhiêu vòng?

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

Sub Bytes

B. 2

Shift Rows

C. 3

Mix Column

D. 4

Add Round Key

Câu 8: Các bước tối giản nào được sử dụng trong mã AES?

A.  $x^4 + x^3 + x + 1$

C.  $x^8 + x^4 + x^3 + x + 1$

B.  $x^{16} + x^5 + x^3 + x + 1$

D.  $x^6 + x^3 + x + 1$

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

A. Khoa công khai

B. Khoa bí mật

C. A & B

D. Khoa vòng

Câu 10: Thuật toán Diffie - Hellman có sử dụng trong những ứng dụng nào?

A. Digital Signature

C. Key Exchange

B. Encryption

D. Authentication

Câu 11: Phản phi tuyến của AES là S-box được tính toán thông thường như sau?

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.  $x^5 + 1$

B.  $x^3 + x^2 + x$

C.  $x^3 + x + 1$

D.  $x^3 + x^2 + 1$

$q$	$r_1$	$r_2$	$r$	$t_1$	$t_2$	$t$
$x^2 + 1$	$x^4 + x^3 + x$	$x^5 + x + 1$	$x$	0	1	$x^2 + 1$
$x + 1$	$x^2 + x + 1$	$x$	1	1	$x^2 + 1$	$x^3 + x^2 + x$
$x$	$x$	1	0	$x^2 + 1$	$x^3 + x^2 + x$	$x^4 + x^3 + 1$
	1	0		$x^3 + x^2 + x$	$x^4 + x^3 + 1$	

Câu 13: Tập  $\{1, 3, 4, 9, 15, 25\}$  là tập siêu tang.

A. đúng B sai.

Câu 14: Đáp án C.

Câu 15: Các bit dùng để làm bit Parity trong hệ thống DBS 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 thống SHA-512 có thể sử dụng để tính giá trị băm của 1 file 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 băm Euler - phi của 787 là?

A. 878

B. 784

C. 785

D 786.

Chú ý:  $\phi(1) = 0$ .

$\phi(p) = p-1$  nếu  $p$  là số nguyên tố.

$\phi(m \times n) = \phi(m) \times \phi(n)$  nếu  $(m, n)$ 互质 (cùng nhau).

$\phi(p^e) = p^e - p^{e-1}$  nếu  $p$  nguyên tố.

$\rightarrow 787$  là số nguyên tố  $\Rightarrow \phi(787) = 787 - 1 = 786$ .

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

$201_{(10)} = 11001001_{(2)}$ . Chọn  $\alpha = 1$

A Đáp án

bit	$P_1$	$P_1 = P_1^2 \bmod 11$	$-P_1 = P_1 \bmod 11$ / $P_1 = (P_1 \cdot 3) \bmod 11$ if bit 1
1	1	1	3
1	3	9	5
0	5	3	3
0	3	9	9
1	9	4	1
0	1	1	1
0	1	1	1
1	1	1	<span style="border: 1px solid red; border-radius: 50%; padding: 2px;">3</span>

Câu 19: Ban rõ: "đvtbkhin"  $\xrightarrow[\text{Khoá mật } (18,6)]{\text{Affine}}$ , Ban mật?  
 A. LDPDZQJT      B. LDPPDZOJT      C. LDPOZOJST      D. K. có kí tự chẵn đều

$$\left\{ \begin{array}{l} C = (P \times K_1 + K_2) \bmod 26 \\ P = ((C - K_2) \times K_1^{-1}) \bmod 26 \end{array} \right.$$

$$d : 3 \rightarrow (3 \times 18 + 6) \bmod 26 = 8 \rightarrow i$$

t : 19

v : 21

t : 19

b : 1

K : 10

h : 7

n : 13

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

A. Hệ mật Caesar

B. Hệ mật đồng (CBC)

C. Hệ mật khóa

D. Hệ mật bát đối xứng.

### B. TƯ LUẬN (Adiem)

Xét hệ mật AES-128 với khóa: SEE CRYPTOGRAPHY

Plaintext: HAPPY FOREVERONE. Hãy xác định:

..... (ASCII, dạng hexa)

a) Ma trận khóa gốc và khai trạng thái (state) ..... (Add Round Key) vòng 1.

b) Khai trạng thái (khu vực hiện công khao vòng) (Add Round Key) vòng 1.

c) Cột đầu tiên ( $w_0$ ) khóa mở rộng cho vòng 1.

Giai:

a)  
+) Chuyển khóa gốc sang dạng hexa:

S	E	E	E	C	R	Y	P	T	O	G	R	A	P	H	Y
53	45	45	45	43	52	59	50	54	4F	47	52	41	50	48	59

Ma trận khóa gốc:

53	43	54	41
45	52	4F	50
45	59	47	48
45	50	52	59

phai trạng thái (State):

48	59	45	59
41	46	56	4F
50	4F	45	4E
50	52	52	45

+) Chuyển plaintext sang dạng hexa:

H	A	P	P	Y	F	O	R	E	V	E	R	Y	O	N	E
48	41	50	50	59	46	4F	52	45	56	45	52	59	4F	4E	45

b) Thực hiện cộng khóa vòng (Add Round Key) trước vòng 1

Round key No. 0 Matrix:  $\begin{pmatrix} 48 & 59 & 45 & 59 \\ 41 & 46 & 56 & 4F \\ 50 & 4F & 45 & 4E \\ 5D & 52 & 52 & 45 \end{pmatrix}$

State:  $\begin{pmatrix} 53 & 43 & 54 & 41 \\ 45 & 52 & 4F & 50 \\ 45 & 59 & 47 & 48 \\ 45 & 5D & 52 & 59 \end{pmatrix}$

XOR từng 4x4

Ví dụ:  $w[0] \oplus w[0]$

$$\text{Tính: } 53 \oplus 48 = 1B$$

$$\begin{array}{r} 0101 \ 0011 \\ 0100 \ 1000 \\ \hline 0001 \ 1011 \end{array}$$

$$45 \oplus 41 = 08$$

$$\begin{array}{r} 0101 \ 0101 \\ 0100 \ 0001 \\ \hline 0000 \ 0100 \end{array}$$

$$54 \oplus 45 = 11$$

$$\begin{array}{r} 0101 \ 0100 \\ 0100 \ 0101 \\ \hline 0001 \ 0001 \end{array}$$

$$45 \oplus 50 = 15$$

$$\begin{array}{r} 0100 \ 0101 \\ 0101 \ 0000 \\ \hline 0001 \ 0101 \end{array}$$

$$43 \oplus 59 = 1A$$

$$41 \oplus 59 = 18$$

$$52 \oplus 46 = 14$$

$$4F \oplus 56 = 19$$

→ Khởi động thái: mìn chỉ ra sau quá trình cộng khóa vòng thuật vòng 1 là:

$$\begin{pmatrix} 1B & 1A & 11 & 18 \\ 08 & 14 & 19 & 1F \\ 15 & 16 & 02 & 06 \\ 15 & 02 & 00 & 14 \end{pmatrix}$$

c) Khai mạc vòng cho vòng 1: (cột đầu với 1 ðể tạo kíp cột cuối với 0)

w[3]

$$\begin{array}{|c|} \hline 41 \\ \hline 50 \\ \hline 48 \\ \hline 59 \\ \hline \end{array}$$

B1: Rot word  
(diễn đạt 1 byte)

$$\begin{array}{|c|} \hline 50 \\ \hline 48 \\ \hline 59 \\ \hline 41 \\ \hline \end{array}$$

B2: Sub word  
(tại S-box)

g(w[3])

$$\begin{array}{|c|} \hline 53 \\ \hline 52 \\ \hline C8 \\ \hline 83 \\ \hline \end{array}$$

w[0]

$$\begin{array}{|c|} \hline 53 \\ \hline 45 \\ \hline 45 \\ \hline 45 \\ \hline \end{array}$$

XOR

$\oplus$

$$\begin{array}{|c|} \hline 01 \\ \hline 00 \\ \hline 00 \\ \hline 00 \\ \hline \end{array}$$

=

$$\begin{array}{|c|} \hline 01 \\ \hline 13 \\ \hline 8E \\ \hline C6 \\ \hline \end{array}$$

ĐỀ 01 - LTMM 2022.2 (75 phút)

A. TRẮC NGHIÊM (4 điểm)

Câu 1: Đa thức:  $x^6 + x^5 + x^4 + x^3 + 1 \rightarrow GF(2^8)$ : 0110 0111  $\rightarrow$  đáp án ①

Câu 2: P: "cryptography" K: "Lucky", C = ?

Câu 3: B

Câu 4: A

Câu 5: B

Câu 6: A

Câu 7:

Câu 8: B

Câu 9: D

Câu 10: B

B. TỰ LUẬN (6 điểm)

Câu 1: (3 điểm) AES-128, khóa: HUST ALUMINUM HOUSE

Plaintext: NGUYỄN NGỌC HOANGA.

a) Giống đề 2021.2  
state:

4E	45	4F	41
47	4E	43	4E
55	4E	48	47
59	47	4F	41

b) Giống 2021.2

06	04	06	0E
12	02	0D	1B
06	1B	01	14
0D	08	07	04

c) Khảo sát 1.  
- (chỗ ghi):

w[0]	w[1]	w[2]	w[3]
48	41	49	4F
55	4C	4E	55
53	55	49	53
54	4D	48	45

$$w[0] = (48, 55, 53, 54)$$

$$w[1] = (41, 4C, 55, 4D)$$

$$w[2] = (49, 4E, 49, 48)$$

$$w[3] = (4F, 55, 53, 45)$$

+) g(w[3]):

- quay trại w[3] 1 byte: (55, 53, 54, 48)

- Byte Substitution (S-box): (F0, E1, D0, 52)

- Adding round constant (01, 00, 00, 00) đilver: (FD, ED, D0, 52)

$$\rightarrow w[4] = w[0] \oplus g(w[3]).$$

0100 1111 1011	1000 1101 0101	0101 1101 1011	0101 0010 0111	0101 0100 0101 0010 0000 0110
B5	B8	B8	73	06

$$\rightarrow w[5] = w[4] \oplus w[2]$$

w[4]	w[3]	w[2]	w[5]	w[6]	w[4]	w[5]
$\begin{pmatrix} B5 \\ B8 \\ 73 \\ 06 \end{pmatrix}$	$\begin{pmatrix} A1 \\ 4C \\ 55 \\ 4D \end{pmatrix}$	$\begin{pmatrix} F4 \\ F4 \\ 26 \\ 4B \end{pmatrix}$	$\begin{pmatrix} 49 \\ 4E \\ 49 \\ 48 \end{pmatrix}$	$\begin{pmatrix} BD \\ BA \\ 6F \\ 03 \end{pmatrix}$	$\begin{pmatrix} 4F \\ 55 \\ 53 \\ 45 \end{pmatrix}$	$\begin{pmatrix} F2 \\ EF \\ 3C \\ 46 \end{pmatrix}$

Vậy khóa vòng 1 là:

B5	F4	BD	F2
B8	F4	BA	EF
73	26	6F	3C
06	4B	03	46

hay khóa vòng 1 là: B5 B8 73 06 F4 F4 26 4B BD BA 6F 03 F2 EF 3C 46.

d) Khởi tạo thai tạo ra bài vòng 1.

- Sub Bytes:

06	04	06	0B
12	02	0D	1B
06	1B	01	14
0D	08	07	04

S-box

6F	F2	6F	AB
82	77	04	4F
6F	4F	7C	PA
D7	30	C5	F2

- Shift Row:

hang 1 gửi nguyên

hang 2 dịch trai 1 byte

hang 3 dịch trai 2 byte

hang 4 dịch trai 3 byte

6F	F2	6F	AB
77	D7	4F	82
FC	FA	6F	4F
F2	D7	30	C5

- Mix Column:

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

6F	F2	6F	AB
77	D7	4F	82
FC	FA	6F	4F
F2	D7	30	C5

$$+ (02 \cdot 6F) \oplus (03 \cdot 7F) \oplus (01 \cdot 7C) \oplus (01 \cdot F2) = C9.$$

$$+ (02 \cdot F2) \oplus (03 \cdot D7) \oplus (01 \cdot PA) \oplus (01 \cdot D7)$$

$$\begin{aligned} \cdot 02 \cdot F2 &= 00000010 \cdot 11110010 = x(x^7 + x^6 + x^5 + x^4 + x) \\ &= x^8 + x^7 + x^6 + x^5 + x^2 \\ &\quad \boxed{x^8 + x^7 + x^6 + x^5 + x^2 + x + 1} \end{aligned}$$

$$\begin{array}{r} 11111111 \\ \hline 11111111 \end{array}$$

**F F.**

$$\cdot 03 \cdot DF = 00000011 \cdot 10010011$$

$$= (x+1)(x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

$$= x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$= x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

$$\boxed{x^6 + x^5 + x}$$

$$01100010 = 62$$

$$\cdot 01 \cdot PA = PA = 10011010$$

$$\cdot 01 \cdot DT = DT = 10010011$$

$$\begin{array}{r} 11111111 \\ 01100010 \\ 11111010 \\ 10010111 \\ \hline 10010000 \end{array}$$

**90**

Làm giống thế → mafen sau Mix Column

xor Randaey No.1

Output vòng 1 cần đếm.

Có thể: (2 điểm) Trong DES, cho khóa 64 bits ban đầu vào K = 0123ABCD 456F 8910

tìm khóa vòng đầu tiên K1 = ?

Ghi:

+ Vết bài K dưới dạng nhị phân:

$$K = 00000001001000111010101101010001010010011000100000$$

K =

0	0	0	0	0	0	0	0	1
0	0	1	0	0	0	1	1	
1	0	1	0	1	0	1	1	
1	1	0	0	1	1	0	1	
0	1	0	0	0	1	0	1	
0	1	1	0	0	1	1	1	
1	0	0	0	1	0	0	1	
0	0	0	1	0	0	0	0	

$\Rightarrow PC_1 K =$

0	1	0	0	1	1	0	0
0	0	1	1	1	0	0	0
0	0	1	0	0	1	1	0
1	0	0	0	0	0	1	0
0	1	1	0	0	0	1	1
1	0	0	0	0	1	0	0
1	1	0	0	0	0	0	0

$$\begin{aligned}
 PG_1K &= 0100 1100 0011 1000 0010 0110 1000 0010 0110 0011 1000 0100 1100 0000 \\
 &= 4 \quad C \quad 3 \quad 8 \quad 2 \quad 6 \quad 8 \quad 2 \quad 6 \quad 3 \quad 8 \quad 4 \quad C \quad 0 \\
 C_0 &= 4C38268 = 0100 1100 0011 1000 0010 0110 1000 \\
 D_0 &= 26384C0 = 0010 0110 0011 1000 0100 1100 0000
 \end{aligned}$$

$\Rightarrow$  Dịch vong trai:  $C_1 = 1001 1000 0111 0000 0100 1101 0000$   
 1 bit  $D_1 = 0100 1100 0111 0000 1001 1000 0000$

1	0	0	1	1	0	0
0	0	1	1	1	0	0
0	0	0	1	0	0	1
1	0	1	0	0	0	0
0	1	0	0	1	1	0
0	0	1	1	1	0	0
0	0	1	0	0	1	1
0	0	0	0	0	0	0

0	0	1	1	1	1
0	0	0	0	1	1
0	0	1	1	0	0
0	0	0	0	0	0
0	0	0	0	0	0
1	1	0	1	1	1
0	1	1	0	1	0
0	0	0	0	0	0

$$\Rightarrow$$
 Khoa  $I_1 = 3C3300037680$