

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			ĐỂ THI CƯỚI KỲ 2022.1  Học phần: ET3310 – LÝ THUYẾT MẬT MẬ  Ngày thi: 08/03/2023  Thời gian làm bài: 60 phút  (Được sử dụng tài liệu, bản in bảng tra cứu, máy tính  Trường nhóm chuyển			
Ký	CBGD phụ trách để thi:		cẩm tay. Nộp để thi cùng với bài làm)  Trường nhóm chuyên môn:			
duyệt	Dotro		- Ky			
A. TI	RẮC NGHIỆM (6 điểm, m	ỗi câu chọn 1	ý đúng duy nhất, làm vào giấy thí)			
Câu 1 A. Má	. Tiến trình giải mặt mà hóa y phát dữ liệu sh truyền	chuyen doi t	bản mật thành bản rõ thực hiện ở đầu?  B Máy nhận dữ liệu  D. Cả A.B.C			
Câu 2.	Hê mật AES theo tiểu chu	ần FIPS PUB	3 197 có ba cấu hình khác nhau về số vòng			
A. Kích (C.)Độ c	thước khối dữ liệu State		B. Kiểu dữ liệu đầu vào hệ mật D. Kiểu mật mã hóa từng vòng			
(A) Khóa	cong knai B. Kiloa bi ili	at C. A	l Signature) bên nhận sử dụng? và B D. Khóa vòng			
Câu 4. I A. 1001	Biểu diễn tương ứng với đ 2011 B. 11000110	a thức $x^7 + x^5$ C. 10	$5 + x^2 + x + 1 \text{ trong } GF(2^8)$ 0100110 D. 10100111			
Câu 5. I A. 2	Iệ mật Triple DES hoạt độ	ộng sử dụng l C. 4	bao nhiêu khóa? D. 5			
Câu 6. H (rounds)?	ệ mật AES hoạt động ở c	ấu hình khóa	a có độ dài 192 bit thực hiện bao nhiều vòng			
A. 10	B.12	C. 14	D. 16			
	nao tác "Dịch hàng (Shift	rows)" được	c thực hiện tại bước trong mỗi round của hệ			
mật AES. A. 1	<b>B</b> 2	C. 3	D. 4			
Câu 8. Đa A. $x^4 + x^3 + C$ $x^8 + x^4 + C$	-x+1	B x16 +x5 +x	ng mã AES là đa thức nào dưới đây? x <sup>3</sup> +x+1 x+1			
Câu 9. Khó A. Khóa cô	oa nào được sử dụng để ng khai B. Khóa bí mậ	chuyển bản it C. A	rõ thành <u>bản mật</u> trong hệ mật bất đối xứng? và B D. Khóa vòng			
A. Digital S	ignature	B. En D. Au	tược sử dụng cho những ứng dụng nào?  ncryption  uthentication			
<b>Câu 11.</b> Phầ A. GF(2 <sup>4</sup> )	n phi tuyến của mã AE B. GF(2 <sup>8</sup> )	S là S-box C. GF	được tính toán trong trường hữu hạn nào? $F(2^{16})   D. GF(2^{32})$			
<b>Câu 12.</b> Xác A. x <sup>2</sup> +1	định nghịch đảo nhân B. x <sup>3</sup> +x <sup>2</sup> +x	của (x <sup>2</sup> +x+ C. x <sup>3</sup> -	1) mod $(x^4 + x^3 + 1)$ ? +x+1 D. $x^3 + x^2 + 1$			
Câu 13. Tập A. Đúng	{1, 3, 4, 9, 15, 25} là t B Sai	ập siêu tăng	g (superincreasing).			

V

QC NE

Câu 14. Thuật toán nào thực hiện theo các bước dưới đây: 1. p, q - two prime numbers, (private, chosen) 2. n = p q, (public, calculated) 2. If P(q) and P(q) are P(q) and P(q) are P(q) and P(q) are P(q) and P(q) are P(q) are P(q) are P(q) are P(q) are P(q) and P(q) are P(q4.  $d = e-1 \pmod{\Phi(n)}$ , (private, calculated) 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? R 2128-1 A. 2256-1 C. 2512-1 D. 2192-1 Câu 17. Giá trị hàm Euler - Phi của 787 là? B. 784 C. 785 A. 878 D. 786 Câu 18. Kết quả của phép tính sau: 3^201mod 11 = ? B. 5 (A) 3 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)? B. LDPDZOJT A. LDPDZOJT D. Không có lựa chọn nào đúng C. LDPOZOJT Câu 20. Chế độ ECB (Electronic Code Book) áp dụng cho hệ mật nào? A. Hệ mật Caesar B. Hệ mật dòng D. Hê mật bất đối xứng (C) Hệ mật khối

## 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.

	Z minim
	TRUÖN
	V
WA NOI	ĐỂ THỊ GIỮA KÝ 2022.2
TRUỐNG ĐẠI HỌC BÁCH KHOA HÀ NỘI TRƯỚNG ĐIỆN – ĐIỆN TỬ	Học phần: ET3310 – LÝ THUYẾT MẬT MÃ Ngày thi: 09/06/2023
Để số: 01 Tổng số trang: 2	Thời gian làm bài: 75 phút (Chi được sử dụng TL viết tay và bằng in tra cứu. Nộp đề thi cùng với bài làm)
Ký duyệt CBGD phụ trách để thi:	Trướng nhóm chuyên môn:
A. TRÁC NGHIỆM (4 điểm)	
Câu 1. Biểu diễn tương ting với da thiết A. 00010011 B. 11000110 Câu 2. Mật mã hóa bản rỗ "cryptography	x <sup>6</sup> + x <sup>5</sup> + x <sup>2</sup> + x +1 trong GF(2 <sup>8</sup> ) C. 00100110 D 01100111 " sử dụng hệ mật Vignere với từ khóa "LUCKY" cho
kết quả bản mật?  A. nlazeiibljii  B. nlazeiibljii  Cân 3. Đặc tính làm rối (confusion) của h	C. olaaciibljki D. mlaaciibljki nệ mật che giấu mối liên hệ giữa bán mật (ciphertext) và
bản rỗ (plaintext)?	
Câu 4. Khối P-Box được sử dụng để tạo c	
A Dung GE(2) bao gồm hai phần t	ừ {1, 2} và hai phép toán cộng và nhân.
	nd key) gồm bits và khối đầu vào mỗi vòng có độ
dàibits.	0.56.04
A 48, 32 B. 64,32 Câu 7. Tim nghịch đảo nhân của (x <sup>7</sup> +x+1)	) mod $(x^8 + x^4 + x^3 + x + 1)$ .
, 7. R x + x -	(C) X
Câu 8. Trong hệ mặt DES 04 bit khoa dad bit cách nhau 4 bit.	vào được rút ngắn thành 56 bits bằng cách loại bỏ các
A Dúng 8 B Sai	hito wai lafata at a ta a ta
Câu 9. Hệ mật AES sử dụng khối đầu vào A. 128; 128 or 256	B. 64; 128 or 192
C 256: 128 192 or 256	(D) 128; 128, 192, or 256
Câu 10. Cầu trúc hệ mật AES-128 bao hàn	vòng tương tự vàcó sự khác biệt.
A. 2 cặp 5 vòng ; vòng luân phiên 6. 8 ; vòng đầu và vòng cuối	B 9 ; vòng cuối D. 10 ; không vòng nào
B. TỰ LUẬN (6 điểm)	, mong rong nao
Câu 1 (3 điểm):	
Xét hệ mật AES-128 với khóa là HUSTAL	LUMINIHOUSE với bản tin rõ (plaintext) là HO_TÊN
của sinh viên (việt HOA, không dấu cách) trình bày nguyên lý và xác định giá trị:	lấy 16 ký tự (chèn ký tự Z nếu chưa đủ độ dài). Hãy
	đã cho và được mã hóa theo bảng mã ASCII. Giá trị
các phần tử của ma trận trạng thái th	
	chóa vòng (Add Round Key) trước vòng 1
c. Khóa vòng I	
d. Khối trạng thái tạo ra bởi vòng 1	The second second
<u>u 2</u> (2 điểm):	
ong DES, cho khóa 64 bits ban đầu vào =?	K = 0123 ABCD 4567 8910, tìm khóa vòng đầu ti
The state of the s	
The second second second	The state of the s



# husteduvn-...repoint.com Xong

☐ Thông tin

IRU	ÔNG ĐẠI HỌC BÁCH KHOA HÀ NỘI TRƯỚNG ĐIỆN – ĐIỆN TỬ	Học phần: ET3316 - LÝ THUYẾT MẬT MÀ		
	Để vô: 01 Tổng số trang: 2	Ngày thi: 08/08/2022 Thời gian làm bài: 75 phút (Chi được sử dụng tài liệu viết tay, báng in tra cứu và máy tính cẩm tay. Nộp để thi cùng với bài làm)		
Ky duyệt	CBGD phụ trách để thị:	Trường nhóm chuyển môn:		

duyệt De	my Tuens	10879	Duga Tv		<b>3</b> 5	
A. TRÁC NGHI	EM (5 điểm, mỗi c	âu chọn I ý ở	tíng duy nhất	, làm vào ,	giấy thí)	
	nật <u>Caesar</u> để giải bả LOCK B		BSWHG WHA		quá bản rõ nào?	
Câu 2. Nghịch đảo r A. 434	nhân của 550 trong tậ B. 224	ip Z <sub>1769</sub> là		Mod . Không tổ	1 769 = { n tại	
Câu 3. Biểu diễn tư A. 00010011	ong ímg với đã thức x B. 11000110	C. 001001	and the second second second	(2 <sup>8</sup> ) 01100111		
Câu 4, Mật mã hóa bản mật?	bán rő "cryptography		nật Vignere vớ	ri từ khóa "	LUCKY" cho kết	quá
A nlazrzatknss	B. nlazrzati	knii C.	olaaciibljsi	D. ml	aaeiibljis	
Câu 5. Hệ mật DES A. 12	bao gồm round B. 18	ds (vòng lặp) v C. 9	với mỗi khóa v D		ē.	
Câu 6. Đặc tính làm (plaintext)? A. Đúng	rối (confusion) của h B.Sai	ệ mật che giất	ı mối liên hệ g	iữa bản mậ	t (ciphertext) và bi	in rõ
Câu 7. Khối P-Box ( A) Đúng	được sử dụng để tạo đ B. Sai	ặc tính phân t	án (diffusion) o	của hệ mật.		
Câu 8. Tương tự như A. Đủng	r hệ mật DES, hệ mật B. Sai	AES cũng sử	dụng cấu trúc			
Câu 9. Trong toán h A. Đúng	oc mođun: (a/b) = a(b B)Sai	r¹)				
Câu 10. Trường GF A. Đúng	2) bao gồm hai phần B Sai	từ {1, 2} và h	ai phép toán cộ	ng và nhân		
Câu 11. Xác định gi A. 3	á trí 2022 <sup>123</sup> mod 13 =	- (E)	D.	16		
Câu 12. Trong hệ m	ật DES khóa vòng (ro	ound key) gồm			mỗi vòng có độ d	ài
bits. A 48, 32	B. 64,32	C. 56, 24	D.	32, 32		924
cho kết quả?	thức (x <sup>6</sup> +x <sup>4</sup> +x <sup>2</sup> +x+1)		trong GF(2 <sup>8</sup> ) v	ối đa thức t	ối giản (x <sup>8</sup> +x <sup>4</sup> +x <sup>3</sup> +	x+1)
A. $x^7 + x^6 + x^3 + x^2 + 1$	B. x6+x5+ x2+x+1	$C.x^7 + x^6 + 1$	D.s	x3+x6+x+1		
Câu 14. Số vòng (ro A. 10	unds) hệ mật AES-25 B. 12	6 thực thi? C.14	D.		92 - 12	
Câu 15. Nghịch đảo A. x²+x	nhân của (x <sup>7</sup> +x+1) m B. x <sup>6</sup> +x <sup>3</sup>	od (x <sup>8</sup> + x <sup>4</sup> + x		x <sup>5</sup> +1	128-10 256-14	

Trang 1/2

Được quét bằng CamScanner





## husteduvn-...repoint.com

Xong

		5334
(←	Thông	tir
	THOITY	CII

υυός quer pang Camscanner

A. MARS	in não được lực chọn ch B. Blowfish	C. RC6	D. Rijindael	
Câu 17. Khối đầu chế	vào mỗi vòng trong hệ	mật DES được mới	ộng từ 32 bits thành 48	blis thông qua cơ
A Mở rộng dùng C. Thêm các bit 0	bit hiện có	B. Thêm D. Thêm	số ngẫu nhiên các bit I	
A. 64 bits	B. 128 bits	C. 512 bits	khi sử lý khối đữ liệu D. 256 bits	
Câu 19. Trong hệ t cách nhau 4 bit. A. Đủng	mật DES 64 bits khóa đ B.Sai	lầu vào được rút ngi	in thành 56 bits bằng c	ách loại bỏ các bit
Câu 20. Hệ mật AI A. 128; 128 or 256 C. 256; 128, 192, o		B. 64; 12	kích thước khóa 28 or 192 28, 192, or 256	bits.
Cấu 21. Tập (1, 2,) A. Đúng	3, 9, <u>14,</u> 34} là tập siêu B. Sai	tăng (superincreas	ing).	
Câu 22. Cấu trúc hệ A. 2 cập 5 vòng ; vò C. 8 ; vòng đầu và v		D. 10; k	g tương tự vàcó : ng cuối hông vòng nào	sự khác biệt.
	nữ ký số (digital signat người tạo chữ ký số. B. Sai	ures) giá trị băm củ	a bản tin đầu vào đượ	rc mật mã hóa với
Câu 24. Xét hệ mật 10011.	Knapsack có khóa bí n	nật {1 6 8 15 24}, l	nãy xác định giá trị bá	in mật ứng với bản rõ
<b>A</b> 2.40	B. 22	C. 31	D. 47	
Câu 25. Bản tin đầu	vào hệ băm SHA-512	được chèn để có đ	ộ dài thỏa mãn tiêu c	ní nào?

### 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:

a. Xác định cặp khóa công khai (n, e), cặp khóa bí mật (n, d) dựa trên hai số p, q đã cho?

b. Cho bắn 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:

- a. 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.
- c. Byte đầu tiên của khối trạng thái tạo ra bởi bước biến đổi Mix Column của vòng 1.



# husteduvn-...repoint.com Xong

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 MẬ  Ngày thi: 08/03/2023  Thời gian làm bài: 60 phút  (Được sử dụng tài liệu, bản in báng tra cứu, máy tính  Trường nhất thi cùng với bài làm)
Ký CBGD phụ trách đề thi:	Trường nhóm chuyển môn:

	Để số: 02	Tổng số trang: 2	(Được sử dụn cầm tay. Nộp	g tài liệu, bản in bảng tra cứu, máy tính để thi cùng với bài làm)
Ký duyệt	CBGD phụ	trách để thi:	Trưởng nhóm	chuyên môn:
Câu 1 A Má C. Kê Câu 2 ? A. Kíc Câu 3 A. Kho	RÁC NGHI  I. Tiến trình ấy phát dữ liệ nh truyền  I. Hệ mật AE ch thước khố vòng (round  I. Tiến trình to ốa công khai	EM (6 điểm, mỗi câu c mật mã hóa chuyển đồ ệu ES theo tiêu chuẩn FIP sĩ dữ liệu State	B. Máy nhật D. Cả A,B,( S PUB 197 có ba cấ  B. Kiểu dữ  D. Kiểu mật  Signature) bên gửi  C. A và B  ining) áp dụng cho l  B. Hệ mật dòng	nất thực hiện ở đầu ? n đữ liệu  lu hình khác nhau về độ dài khóa và liệu đầu vào hệ mật t mã hóa từng vòng sử dụng ? D. Khóa vòng hệ mật nào?
C.Hê	mật khối		<ul> <li>D. Hệ mật bất đối</li> </ul>	CONTROL OF CO.
A. 5		ple DES hoạt động sử B. 4	CL 3	D. 2
(rounds A. 10	;)?	B.12	© 14	56 bit thực hiện bao nhiều vòng  D. 16
AES.		B. 2	C. 3	i bước trong mỗi round của hệ mật  D. 4
Câu 8. ł A. x <sup>4</sup> +x	$x^3 + x + 1$ $x^3 + x + 1$		D. $x^8 + x^4 + x^3 + x$	+1
A Vháo	aâna lehai	D Khóa hi mất	C. A Va D	bản rỗ trong hệ mật RSA? D. Khóa vòng
Câu 10.	Thuật toán	Diffie-Helman algo	orithm được sử dụn	ng cho những ứng dụng nào?
A. Digita	l Signature	е	B. Key Exchange	
Câu 11.	Phần phi tư	yến của mã AES là B. GF(24)	S-box được tính t GF(28)	oán trong trường hữu hạn nào?  D. GF(2 <sup>16</sup> )
Câu 12. 2 A. x <sup>2</sup> +1	Xác định n	ghịch đảo nhân của B. x <sup>2</sup> +x	(x <sup>2</sup> +x+1) mod (x <sup>4</sup> C. x <sup>3</sup> +x+1	D. $x^{3}+x^{2}+1$





## husteduvn-...repoint.com

Xong

← Thông tin

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

- p, q two prime numbers, (private, chosen)
- n = p q, (public, calculated)
- 3. e, with  $gcd(\Phi(n), e) = 1$ ,  $1 \le e \le \Phi(n)$ , (public, chosen)
- 4. d = e-1(mod Φ(n)), (private, calculated)

A. DHKE

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

© 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 bằm của bản tin có độ dài tối đa bao

nhiêu bit?

A. 2256-1

B 2128-1

C. 2512-1

D. 2192-1

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

B. 784

D. 786

Câu 18. Kết quả của phép tính sau: 3^201mod 11 = ?

A. 3

B. 5

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. Hê mật dòng

C. Hệ mật khối

D. Hệ mật bất đối xứng

### B. TU LUAN (4 điểm)

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

- Ma trân khóa gốc và khối trạng thái (state) ứng với bản tín rõ với giả thiết các ký tụ được mã hóa theo bảng mã ASCII và các phần từ ma trận thể hiện dưới dạng Hexa;
- Khôi trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1;
- Cột đầu tiên (w<sub>04</sub>) khóa mở rộng cho vòng 1.



Xét hệ mật AES-128 với khóa là HUSTCRYPTOGRAPHY và bản tin rõ (plaintext) là

mã hóa theo bảng mã ASCII và các phần từ ma trận thể hiện dưới dạng Hexa;
 b. Khối trạng thái khi thực hiện cộng khóa vòng (Add Round Key) trước vòng 1;

Ma trận khóa gốc và khối trạng thái (state) ứng với bản tin rõ với giả thiết các ký tự được

B. TỰ LUẬN (6 điểm)

SUNSHINEINSUMMER. Hãy xác định:

c. Cột đầu tiên (w04) 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  Ký CBGD phụ trách đề thi:	ĐỂ 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  Trường nhóm chuyển môn:
duyệt Ostu	
A. TRẮC NGHIỆM (6 điểm, mỗi câu ch	ọn 1 ý đúng duy nhất, làm vào giấy thĩ)
Câu 1. Tiến trình mật mã hóa chuyển đôi t A. Máy phát dữ liệu	B. Máy nhận dữ liệu  D. Cả A,B,C
Câu 2. Hê mật AES theo tiểu chuẩn FIPS	PUB 197 có ba cấu hình khác nhau về độ dài khóa và
A. Kích thước khối dữ liệu State	<ul> <li>B. Kiểu dữ liệu đầu vào hệ mật</li> <li>D. Kiểu mật mã hóa từng vòng</li> </ul>
Câu 3. Tiến trình tạo chữ ký số (Digital Si	D. Kiloa vong
Câu 4. Chế độ CBC (Cipher Block Chaini A. Hệ mật Caesar C. Hê mất khối	ing) áp dụng cho hệ mật nào? B. Hệ mật dòng D. Hệ mật bất đối xứng
Câu 5. Hệ mật Triple DES hoạt động sử d	C. 3
Câu 6. Hệ mật AES hoạt động ở cấu hình	khóa có độ dài 256 bit thực hiện bao nhiều vòng
	C. 14 D. 16
Câu 7. Thao tác "Tráo Byte (SubBytes)" AES.	được thực hiện tại bước trong mỗi round của hệ mật
A 1 B. 2	C. 3 D. 4
A. $X^{7} + X^{7} + X + 1$ C. $x^{6} + x^{3} + x + 1$	D. $x^8 + x^4 + x^3 + x + 1$
Câu 9. Khóa nào được sử dụng để chuyể A. Khóa công khai B. Khóa bí mật	L. A Va D
Câu 10. Thuật toán Diffie-Helman algori	ithm được sử dụng cho những ứng dụng nào?
A. Digital Signature	B. Key Exchange
Câu 11. Phần phi tuyến của mã AES là S A. GF(2) B. GF(2 <sup>4</sup> )	B-box được tính toán trong trường hữu hạn nào?  C. GF(2 <sup>8</sup> )  D. GF(2 <sup>16</sup> )
00 10 Tr. 1: 1 1: 1 1:	$(x^{2}+x+1) \mod (x^{4}+x+1)$ ? $(x^{3}+x+1) \mod (x^{4}+x+1)$ ? $(x^{3}+x+1) \mod (x^{4}+x+1)$ ?

OC B

d

Câu 16. Nghịch đảo nhân của  $(x^7+x+1) \mod (x^8+x^4+x^3+x+1)$ ? C. x7+1 B.  $x^{7}+x^{3}$ A. x7 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 D. Thêm các bit 1 C. Thêm các bit 0 Câu 18. Sô bít biểu diễn giá trị đầu ra của hệ băm SHA512 khi xử lý khối dữ liệu 106 bit? D, 256 bits C. 512 bits B. 128 bits A. 64 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 bits với kích thước khóa Câu 20. Hệ mật AES sử dụng khối đầu vào bits. B, 64; 128 or 192 A. 128; 128 or 256 D) 128; 128, 192, or 256 C. 256; 128, 192, or 256 Câu 21. Tập {1, 3, 12, 9, 24, 54} là tập siêu tăng (superincreasing). (B) Sai A. Đúng Câu 22. Cấu trúc hệ mật AES-192 sử dụng khóa có độ dài bits và lặp vòng. D. 256; 14 C. 192, 12 B. 128; 12 A. 128; 10 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. B. Sai A. Đúng Câu 24. Số phần tử đồng dư với 49 trong tập Z<sub>49</sub> là .... B. 36 D. 7 A. 40 Câu 25. Bản tin đầu vào hệ băm SHA-512 được chèn để có độ dài thỏa mãn tiêu chí nào? D. 968 mod 1024 C. 512 mod 1024 B. 896 mod 1024 A. 698 mod 1024

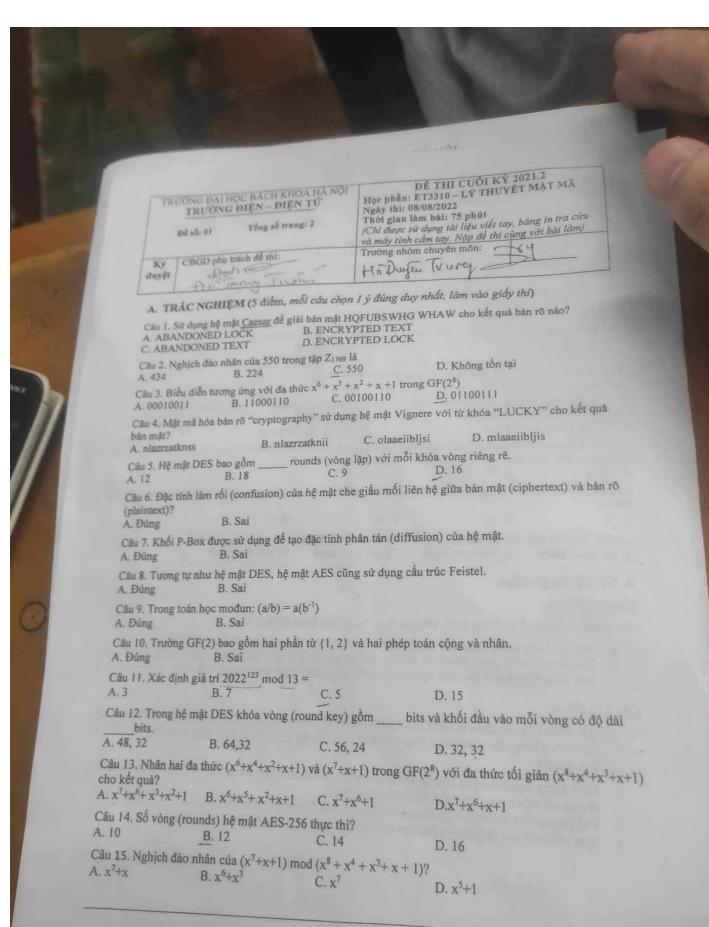
### B. TU LUÂN (5 điểm)

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 E nhằm trao đổi khóa bí mật. An mật mã hóa bản tin có giá trị M=6 (chữ "G" trong bảng mã ký tự tiến ứng với tập  $Z_{26}$ ) và gửi cho Bình.

Hãy thực hiện các nội dung sau:

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

Trover	1			
TRU	ONG ĐẠI HO	OC BÁCH KHOA HÀ NỘI ĐIỆN – ĐIỆN TỐ		
1	Để số: 01	Tổng số trang: 2	ĐỂ THI CUỐ Học phần: ET3310 – LÝ T Ngày thi: 05/08/2023 Thời gian làm bài: 75 phú (Chi được sử dụng tài liệu i	THUYÉT MẬT MÃ t
Ký duyệt	CBGD phụ	trách đề thi:	Nộp để thi cùng với bài làm	1)
duyçı	PGS.TS. Độ	ỗ Trọng Tuấn	Trường nhóm chuyên môn:	
			PGS.TS. Hà Duyên Trung	as when you are a second second
A. TI	RĂC NGHI	LÊM (5 điểm, mỗi câu chọi		
Câu 1.	Hệ thống trư	yền thông áp du	1 I ý đúng duy nhất, làm vớ	ào giấy thi)
A. I k	hóa	B) 2 khóa	hóa công khai sử dụng đ	ễ mật mã dữ liệu.
pháp n A. Cry	Thuật ngữ nột cách bí n ptography	thể hiện tính chất của tiế nật ở định dạng không thể ho B. Symmentricity	n trình truyền đạt thông tin g ặc rất khó đọc được.	iữa những người dùng hợp
A Do	i ien trinh n	nật mã hóa đầu cuối diễn ra ở	thành phần nào trong hệ thố	ing truyền thông ?
	8	B. Ben nhân	Kênh truyền	Cà A và B
Cau 4:	Hệ mật Cae	sar là một ví dụ của		52/10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
A. Hệ i	mật nhân	B.Hệ mật dịch C.	Hệ mật lặp I	O. Không có ý đúng
Câu 5:	Bån tin 1000	bits được mật mã hóa bởi h	ệ mật dòng sẽ cho đầu ra là	bits.
A. 500				D. 1200
Câu 6.	Loại hệ mật	nào dưới đây sử dụng chung	khóa để mật mã hóa và giả	i mật mã hóa:
	metric key	7~LI X		D. Cà A và B
Câu 7. A. 0010		ong ứng với đa thức $x^6 + x^5$ B. 11000110 C.	$+ x^3 + x + 1 \text{ trong GE}(2^8)$	01011
Câu 8. 1	Mật mã hóa	bản rõ "kryptosgraphein" sử	r dụng hệ mật Vignere với t	ừ khóa "HUST" cho kết quả
bản mật			C -l::hii-i-f	D. Ingiailtermhalaf
A. lrazr			Transition (Environmental son) S	D. Irqiaikzyuhalcf
A) Rijno	iael	nật mã nào dưới đây được cl B. Knapsack	C. RC4	D. RSA
A) Hoán C. Sử dụ	vị sử dụng ng nhiều kh	óa	Thay thể bit băng cách sử D. Sử dụng bộ sinh kl	dụng S-Box hóa tự động
Câu 11.	Một hệ mật	sử dụng kỹ thuật nào khi th	ược hiện mật mã hóa bằng	cách mã xáo trộn các chữ ca
A. Subst		B. Stream C.	Running key	(D.)Transposition
Câu 12. ' A. Đúng	Trường GF(	28) bao gồm 8 phần tử và h B Sai	ai phép toán cộng và nhân	Section and read way
. 31		trí 45 <sup>17</sup> mod 101 = B. 17 C.	47 D. 45	etale de Diago (delle page de
.) Thay t	hế các phần	g S-box để làm gì trong qu từ B. Sinh khóa	C. Trao đôi khóa	D. Hoán vị các phần tử
âu 15. N . x <sup>2</sup> +1	Nhân hai đa B x <sup>2</sup> +	thức $(x^2+x+1)$ và $(x^2+1)$ tr x C. $x^3+1$	ong trường GF với đa thủ D. x+1	rc tối giản (x3+x+1) cho kế



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? C. 2128-1 D. 2512-1 B. 2256\_1 A. 2<sup>192</sup>-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. Đầu là bản mật mà A đã gửi đi? B. LDPOZOJT A. LDPDZQJT D. Không có lựa chọn nào đúng C. LDPDZOJT 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 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) C. Knapsack B. RSA A. RC4 Câu 17. Tập { 1, 3, 6, 13, 27, 52 } là tập siêu tăng (superincreasing). B. Sai A. Đúng Câu 18. Kết quả của phép tính sau: 3^201mod 11 = ? D. 3 Câu 19. Biểu diễn tương ứng của đa thức  $x^6 + x^4 + x^3 + x^2 + x$  trong GF(28) là: D. 11011010 B. 01001110 C. 010111110 A. 01010111 Câu 20. Giá trị hàm Euler - Phi của 773 là? D. 772 B. 770 C. 771 A. 377 B. TU LUAN (6 điểm) SUNSHINEINSUMMER. Hãy xác định:

Xét hệ mật AES-128 với khóa là HUSTCRYPTOGRAPHY và bản tin rõ (plaintext) là

- 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.

					Market Market		
	Security 9						
						1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
200 Vin 100 Vi	a the drawn low to	non cho hệ mặt AES?		estent.			
A. MARS	B. Blowfish	C. RC6	D. Rij	its thành 48 blts thông	qua co	A	
Câu 17. Khối chế	đầu vào mỗi vòng tro	ng në mat Disa ditiçe	hêm số ngẫu nhi	ên			
A Mở rộng đủ	ng bit hiện có t 0	D. T	hêm các bit 1			7 11 71 12 20 72	
Cau 18 Kich th	ước của mỗi từ (Wo	rd) của hệ bảm SHA- C. 512 bits	512 khi sử lý kh D. 25	iối dữ liệu 1024- bit? 6 bits		The state of the s	A
A. 64 bits	8, 128 bits 8 måt DES 64 bits k	hóa đầu vào được rút	ngắn thành 56	bits bằng cách loại bô	oác bit		
cách nhau 4 bit.	B. Sal						
A. Đủng	AES sử dụng khối đ	lu vão bits	với kích thước l	chóa bit	S.		
A 128: 128 or 25	56	D. 12	; 128 or 192 8; 128, 192, or	256			
C. 256; 128, 192,	3 9 14, 34} là tập	siêu tăng (superince	easing).				
A. Đúng	D. Gai		ong tương tự v	à có sự khác bi	ôt.		
Cầu 22. Cấu trúc h A. 2 cặp 5 vòng ; v	nệ mật AES-128 bac	B 9:	vòng cuối				
C. 8; vòng đầu và	vòng cuối	D. 10	; không vòng t	nao lu vào duos mit mii	hóa với		
Câu 23. Để tạo ra c khóa công khai của	hữ ký số (digital si người tạo chữ ký s	0.		lu vào được mật mã			
Câu 24. Xét hê mật	Knapsack có khóa	bí mật {1 6 8 15 24	}, hãy xác định	n giá trị bản mật ứng	g với bản rõ		
10011.	B. 22	C. 31	D. 47				
A. 40 Câu 25. Bản tin đầu	D. ZZ		ố độ dài thỏa n	năn tiêu chí nào?			
A. 832 mod 1024	B. 768 mod 1024	C. 960 mod 1	024 D.89	96 mod 1024			
B. TỰ LUẬN (5 đ	iểm)	MARKETTA POLICE					
<u>Câu 1</u> (2 điểm):							
Cho hai số nguyên tố	p=17 và q=31. Hã	iy sử dụng thuật to	án RSA để thụ	rc hiện:			
<ul> <li>b. Cho bản tin rô</li> </ul>	là giá trị bảng mã	ASCII của chữ cá	i thứ hai (việt	ên hai số p, q đã ch HOA theo hệ Latir 1 khi giải mật mã?	no? n) trong tên của		
<u>Câu 2</u> (3 điểm):						N. A. W.	
Két hệ mật AES-128 viên (viết HOA, không à xác định giá trị:							
<ul> <li>a. Khối trạng thái từ của ma trận t</li> <li>b. Khối trang thái</li> </ul>	trạng thái thê hiện khi thực hiên côn	dưới dạng Hexa.	Round Key)	bảng mã ASCII.		n	
c. Byte đầu tiên ci	ủa khối trạng thái	tạo ra bởi bước bi	ến đổi Mix C	olumn của vòng 1	1 62 H		

TRƯỜNG ĐẠI HỌC BÁCH KH TRƯỜNG ĐIỆN – ĐIỆ	Ngay ti	ii: 08/03/2023	OI KÝ 2022.1 THUYẾT MẠT MÃ
Đề số: 02 Tổng số tra	cầm ta)	từ dụng tài liệu, bá Nộp để thi cùng nhóm chuyên mô	in in báng tra cứu, máy tinh
Ký CBGD phụ trách đề thi:			TIM
A. TRẮC NGHIỆM (6 điểm,	mỗi câu chọn 1 ý đúng	duy nhất, làm và	to giấy thí)
Câu 1. Tiến trình mật mã hóa c A. Máy phát dữ liệu	huyên đội bàn rõ thành B. Má D. Cả	ban mặt thực hiệ ly nhận dữ liệu A,B,C	ện ở đâu ?
C. Kênh truyền  Câu 2. Hệ mật AES theo tiêu c	huẩn FIPS PUB 197 có	ba cấu hình khá	c nhau về độ dài khóa và
A. Kích thước khối dữ liệu Stat	B. Ki D. Ki	ều dữ liệu đầu và ều mật mã hóa ti	io hê mât
Câu 3. Tiến trình tạo chữ ký số	I IIIai C. A va D	D. KHO	
Câu 4. Chế độ CBC (Cipher B)  A. Hệ mật Caesar  C Hê mất khối	lock Chaining) áp dụn B. Hệ mật d D. Hệ mật b	át đối xứng	?
Câu 5. Hệ mật Triple DES hoạ 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	c hiện bao nhiêu vòng
(rounds)? A. 10 B.12	C. 14	D. 16	
Câu 7. Thao tác "Tráo Byte (Si	ubBytes)" được thực l	niện tại bước	trong mỗi round của hệ mật
AES. A. 1 B. 2	C. 3	D. 4	
Câu 8. Đa thức tối giản nào đu A. $x^4 + x^3 + x + 1$	D. $x^8 + x^4 + x$	$-x^3 + x + 1$	
Câu 9. Khóa nào được sử dụng A. Khóa công khai B. Khóa b	1 mai		
Câu 10. Thuật toán Diffie-Heli	man algorithm được	sử dụng cho nhi	mg ung dung nao
A. Digital Signature	B. Key Ex	change	
C. Decryption  Câu 11. Phần phi tuyến của mã A. GF(2)  B. GF(2 <sup>4</sup> )	$\tilde{a}$ AES là S-box được $\tilde{O}$ . GF( $2^8$ )	D. G	F(2 <sup>16</sup> )
A. $GF(2)$ B. $GF(2^n)$ Câu 12. Xác định nghịch đảo t  A. $x^2+1$ B. $x^2+x$	nhân của (x²+x+1) m C. x³+x+1	od $(x^4 + x + 1)$	$3+x^2+1$

OC B

d

Câu 14. Thuật toán nào thực hiện theo các bước dưới đây: 1. p, q - two prime numbers, (private, chosen) 2. n = p q, (public, calculated) 3. e, with  $gcd(\Phi(n), e) = 1$ ,  $1 \le e \le \Phi(n)$ , (public, chosen) 4.  $d = e-1 \pmod{\Phi(n)}$ , (private, calculated) 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? B. 2128-1 A. 2256-1 C. 2512-1 D. 2192-1 Câu 17. Giá trị hàm Euler - Phi của 787 là? B. 784 C. 785 A. 878 D. 786 Câu 18. Kết quả của phép tính sau: 3^201mod 11 = ? B. 5 A. 3 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)? B. LDPDZOJT A. 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 D. Hệ mật bất đối xứng S. Hệ mật khối

## 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.

Hệ đơn ký tự on ke. Affine là một ví dụ của ..... ou bảng cách Câu 18. DES sử dụng P-box để làm gi trong quá trình mật mã hóa?

C. Trao đổi khóa C. Running key A. Thay thế các phần từ B. Sinh khóa D. Substitution Cấu 19. Hệ mật DES khóa mật mã đầu vào 64 bits được rút ngắn thành 56 bits bằng cách loại bỏ các bi cách nhau bit. Câu 20: Bản tin 1500 bits được mật mã hóa bởi hệ mật đồng sẽ cho đầu ra là ..... bits.

D. 2000 Câu 21. Số phần từ đồng dư với 49 trong tập Zao là .... Câu 22. Mật mã hóa bản rõ "kryptosgraphein" sử dụng hệ mật Vignere với từ khóa "SEEE" cho kết quả bản A. cvazrzatknss Câu 23. Loại hệ mật nào dưới đây không sử dụng chúng khóa để mật mã hóa và giải mật mã hóa:

C Stream Cinher

D. Cá A và B A. Symmetric key Câu 24. Trong các lựa chọn sau, cái nào KHÔNG phải là độ dài khóa hợp lệ cho AES? Cấu 25. Hệ mật RSA dựa trên cơ sở toán học nào? A Phân tích thừa số của số nguyên tố lớn B. TU LUAN D. 256 bit B. Giải các phương trình đa thức 1. Xét hệ mật AES-128 Với khá. D. Tính định thức ma trận