

1 Giới thiệu

(1) **Mật mã khoá đối xứng** MULTIPLE CHOICE Multiple answers allowed

Hệ mật mã khoá đối xứng có

- khoá bí mật để mã hoá và khoá công khai để giải mã.
- khoá công khai để mã hoá và khoá bí mật để giải mã.
- hai khoá khác nhau.
- khoá mã hoá và khoá giải mã giống nhau.

(2) **Mật mã khoá công khai** MULTIPLE CHOICE Multiple answers allowed

Khoá đối xứng có

- khoá bí mật để mã hoá và khoá công khai để giải mã.
- khoá mã hoá và khoá giải mã giống nhau.
- hai khoá khác nhau.
- khoá công khai để mã hoá và khoá bí mật để giải mã.

(3) **Hàm băm mật mã** MULTIPLE CHOICE Multiple answers allowed

Đầu ra của hàm băm mật mã

- có thể dễ dàng tính được bởi kẻ tấn công.
- là dãy bit độ dài thay đổi.
- là dãy bit độ dài cố định.
- không thể tính được bởi kẻ tấn công.

(4) **Chữ ký số** MULTIPLE CHOICE Multiple answers allowed

Trong các sơ đồ chữ ký số, giá trị băm của thông điệp thường được mã hoá dùng

- khoá công khai của người dùng
- mật khẩu của người dùng.
- khoá bí mật của người dùng
- khoá phiên

Total of marks: 4

2 Hệ mã dòng

(1) **One Time Pad** SHORT ANSWER Case-Insensitive

Giả sử bạn biết mã hóa của thông điệp “attack at vn” dùng one time pad encryption là

6c73d5240a948c86981bc294

(bản rõ ở dạng mã ASCII 8-bit và bản mã được viết ở dạng hexa). Bản mã của thông điệp “attack at us” với cùng khóa OTP là _____.

Chú ý: bạn chỉ điền mã ASCII 8-bit của bản mã ở dạng hexa.

Total of marks: 1

3 Chế độ mã khối

(1) **ECB mode** SHORT ANSWER Case-Insensitive

Xét hệ mã khối **BkExam** chuyên dùng cho việc thi học kỳ. **BkExam** sử dụng các chữ cái để mã hoá. Hàm mã hoá **BkExam** với khoá cụ thể K được cho bởi bảng sau:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
m	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$E_K(m)$	P	K	X	C	Y	W	R	S	E	J	U	D	G	O	Z	A	T	N	M	V	F	H	L	I	B	Q

Bản mã của thông điệp: “ANTOAN” dùng **ECB mode** là _____.

(2) **CBC mode** SHORT ANSWER Case-Insensitive

Xét hệ mã khối **BkExam** chuyên dùng cho việc thi học kỳ. **BkExam** sử dụng các chữ cái để mã hoá. Hàm mã hoá **BkExam** với khoá cụ thể K được cho bởi bảng sau:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
m	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$E_K(m)$	P	K	X	C	Y	W	R	S	E	J	U	D	G	O	Z	A	T	N	M	V	F	H	L	I	B	Q

Do phép toán \oplus không định nghĩa trên tập $\{A, \dots, Z\}$, ta thay thế nó với phép cộng theo modun 26 (ví dụ, $C \oplus D = F$ và $Y \oplus C = A$).

Bản mã của thông điệp: “TT” dùng **CBC mode** với $IV=C$ là _____.

Chú ý: Bạn phải viết cả IV vào bản mã.

Total of marks: 2

4 Lý thuyết số

- (1) **Phần tử sinh** MULTIPLE CHOICE Multiple answers allowed

Những phần tử nào dưới đây là phần tử sinh của \mathbb{Z}_{13}^* ?

- a. 2
- b. 9
- c. 3
- d. 7
- e. 5

- (2) **Euclid mở rộng** SHORT ANSWER Case-Insensitive

Hãy dùng thuật toán Euclid mở rộng để tính $15^{-1} \pmod{799}$.

Giá trị 15^{-1} là _____.

- (3) **Tính lũy thừa nhanh** SHORT ANSWER Case-Insensitive

Hãy dùng thuật toán tính lũy thừa nhanh để tính $779^{280001} \pmod{11413}$ biết rằng $11413 = (101 \times 113)$.

Giá trị $779^{280001} \pmod{11413}$ bằng _____.

- (4) **Logarit rời rạc** SHORT ANSWER Case-Insensitive

Hãy tính logarit rời rạc của 5 cơ sở 2 trong \mathbb{Z}_{13}^* .

Giá trị của $\text{Dlog}_2(5)$ bằng _____.

- (5) **Logarit rời rạc** MULTIPLE CHOICE Multiple answers allowed

Xét G là một nhóm cyclic cấp q và g là một phần tử sinh. Giả sử rằng bài toán logarit rời rạc là khó trong G . Những bài toán nào dưới đây cũng là khó trong G ?

- a. Lấy ngẫu nhiên $x \in \mathbb{Z}_q$, tìm y sao cho $g^x = y$
- b. Lấy ngẫu nhiên $y \in G$, tìm x sao cho $g^x = y$
- c. Tìm x và y sao cho $g^x = y$.
- d. Lấy ngẫu nhiên hai giá trị $x \in \mathbb{Z}_q$ và $y \in G$, tính $y^x \cdot g$

Total of marks: 5

5 Hệ mật mã RSA

(1) **Giải mã RSA** SHORT ANSWER Case-Insensitive

Xét sơ đồ mã hoá RSA được cài đặt các tham số $p = 31$ và $q = 37$. Khoá công khai là $e = 17$. Ta cần giải mã **bản mã** $y = 2$.

Ta giải mã được bản rõ x bằng _____.

(2) **Bài toán RSA** MULTIPLE CHOICE Multiple answers allowed

Trong các bài toán dưới đây, ta giả sử N là tích của hai số nguyên tố lớn p và q , và e nguyên tố cùng nhau với $\phi(N)$.

Nếu bài toán RSA là khó, vậy những bài toán nào dưới đây cũng khó?

- a. Cho trước N , e , và lấy ngẫu nhiên $y \in \mathbb{Z}_N^*$, tìm x sao cho $x^e = y \bmod N$.
- b. Cho trước N và e , tìm x, y sao cho $x^e = y \bmod N$.
- c. Cho trước N, e , và lấy ngẫu nhiên $x \in \mathbb{Z}_N^*$, tìm y sao cho $x^e = y \bmod N$.
- d. Cho trước N và e , tìm x sao cho $x^e = 8 \bmod N$.

(3) **Sửa đổi bài toán RSA** MULTIPLE CHOICE Multiple answers allowed

Nhắc lại rằng hoán vị của sập RSA được định nghĩa trong nhóm \mathbb{Z}_N^* với N là tích của hai số nguyên tố lớn. Khóa công khai là (N, e) và khóa bí mật là (N, d) trong đó d là nghịch đảo của e trong $\mathbb{Z}_{\phi(N)}^*$.

Giả sử trong thuật toán RSA, thay vì dùng hợp số N bạn lại dùng số nguyên tố p . Trong trường hợp này, bằng những cách nào dưới đây người ta có thể tính được khóa bí mật (N, d) từ khóa công khai (N, e) .

- a. $d \leftarrow e^{-1} \pmod{p-1}$.
- b. $d \leftarrow e^2 \pmod{p}$.
- c. $d \leftarrow -e \pmod{p}$.
- d. $d \leftarrow e^{-1} \pmod{p}$.

Total of marks: 3

6 Giao thức Diffie-Hellman

(1) **Tính hàm Diffie-Hellman** SHORT ANSWER Case-Insensitive

Xét \mathbb{Z}_{19}^* là một nhóm cyclic với 3 là một phần tử sinh. Hãy tính giá trị $\text{DH}_3(7, 15)$ trong nhóm này.

Giá trị $\text{DH}_3(7, 15)$ bằng _____.

(2) **Diffie-Hellman sửa đổi** MULTIPLE CHOICE One answer only

Giả sử ta sửa đổi giao thức Diffie-Hellman như sau. Alice vẫn tương tác như thông thường, tức là chọn số ngẫu nhiên a trong $\{1, \dots, p-1\}$ và gửi cho Bob $A \leftarrow g^a$. Bob, tuy vậy, chọn số ngẫu nhiên b trong $\{1, \dots, p-1\}$ và gửi cho Alice $B \leftarrow g^{1/b}$. Giá trị chia sẻ bí mật secret nào dưới đây họ có thể sinh và làm thế nào họ sinh được?

- a. $\text{secret} = g^{ab}$. Alice tính giá trị secret bằng $B^{1/a}$ và Bob tính bằng A^b .
- b. $\text{secret} = g^{ab}$. Alice tính giá trị secret bằng B^a và Bob tính bằng A^b .
- c. $\text{secret} = g^{a/b}$. Alice tính giá trị secret bằng $B^{1/b}$ và Bob tính bằng A^a .
- d. $\text{secret} = g^{a/b}$. Alice tính giá trị secret bằng B^a và Bob tính bằng $A^{1/b}$.

Total of marks: 2

7 Đường cong Elliptic

(1) Cộng điểm trên EC SHORT ANSWER Case-Insensitive

Xét đường cong Elliptic

$$E : y^2 = x^3 + 2x + 2 \pmod{17}$$

Để tiện cho việc tính toán, các điểm là bội của phần tử sinh $(5, 1)$ được liệt kê trong Bảng dưới đây.

k	1	2	3	4	5	6	7	8	9	10
$k \cdot G$	(5,1)	(6,3)	(10,6)	(3,1)	(9,16)	(16,13)	(0,6)	(13,7)	(7,6)	(7,11)
k	11	12	13	14	15	16	17	18	19	
$k \cdot G$	(13,10)	(0,11)	(16,4)	(9,1)	(3,16)	(10,11)	(6,14)	(5,16)	\mathcal{O}	

Xét điểm $P_1 = (13, 10)$ và $P_2 = (6, 14)$. Hãy tính điểm $Q = P_1 + P_2$.

Điểm Q là _____.

Chú ý: Hãy viết đáp án dưới dạng (p, q) , không có dấu cách ở giữa.

(2) Chia sẻ khoá trên EC SHORT ANSWER Case-Insensitive

Xét đường cong Elliptic

$$E : y^2 = x^3 + 2x + 2 \pmod{17}$$

Để tiện cho việc tính toán, các điểm là bội của phần tử sinh $(5, 1)$ được liệt kê trong Bảng dưới đây.

k	1	2	3	4	5	6	7	8	9	10
$k \cdot G$	(5,1)	(6,3)	(10,6)	(3,1)	(9,16)	(16,13)	(0,6)	(13,7)	(7,6)	(7,11)
k	11	12	13	14	15	16	17	18	19	
$k \cdot G$	(13,10)	(0,11)	(16,4)	(9,1)	(3,16)	(10,11)	(6,14)	(5,16)	\mathcal{O}	

Xét điểm $P = (13, 10)$. Alice và Bob sẽ thiết lập khoá chia sẻ dùng giao thức Diffie-Hellman trên đường cong E . Cụ thể, Alice sẽ thực hiện:

- Chọn giá trị $a = 4$ và gửi điểm aP cho Bob;
- Nhận được điểm $bP = (16, 13)$ từ Bob.

Khoá chia sẻ abP giữa Alice và Bob là _____.

Chú ý: Hãy viết đáp án dưới dạng (p, q) , không có dấu cách ở giữa.

Total of marks: 2

8 Hàm băm

- (1) **Hàm băm** MULTIPLE CHOICE Multiple answers allowed

Giả sử H và H' là các hàm băm kháng xung đột. Những hàm băm H'' nào dưới đây là kháng xung đột.

Chú ý: Phép toán \parallel ký hiệu phép ghép xâu.

- $H''(x) = H(H'(x))$
- $H''(x) = H(x) \parallel H'(x)$
- $H''(x) = H(x) \oplus H'(x)$.
- $H''(x) = H(x) \parallel 0 \dots 0$

Total of marks: 1

9 Mac

(1) **MAC an toàn** MULTIPLE CHOICE Multiple answers allowed

Xét một hệ MAC an toàn (S, V) trên (K, M, T) với $M = \{0, 1\}^n$ và $T = \{0, 1\}^{128}$ (cụ thể, không gian khóa là K , không gian thông điệp là $\{0, 1\}^n$, và không gian tag là $\{0, 1\}^{128}$). Những MAC nào dưới đây là MAC an toàn: (ở đây, ta dùng ký hiệu \parallel là ghép xâu).

- $S'(k, m) = S(k, m)[0, \dots, 126]$ và $V'(k, m, t) = [V(k, m, t \parallel 0) \text{ hoặc } V(k, m, t \parallel 1)]$
(cụ thể, $V'(k, m, t)$ outputs “1” nếu hoặc $t \parallel 0$ hoặc $t \parallel 1$ là tag hợp lệ cho m).
- $S'(k, m) = S(k, m \parallel m)$ và $V'(k, m, t) = V(k, m \parallel m, t)$.
- $S'((k_1, k_2), m) = (S(k_1, m), S(k_2, m))$ và
 $V'((k_1, k_2), m, (t_1, t_2)) = [V(k_1, m, t_1) \text{ và } V(k_2, m, t_2)]$
(cụ thể, $V'((k_1, k_2), m, (t_1, t_2))$ outputs “1” nếu cả t_1 và t_2 đều là tag hợp lệ).
- $S'(k, m) = S(k, m[0, \dots, n-2] \parallel 0)$ và $V'(k, m, t) = V(k, m[0, \dots, n-2] \parallel 0, t)$
- $S'(k, m) = S(k, m)$ và
 $V'(k, m, t) = [V(k, m, t) \text{ hoặc } V(k, m \oplus 1^n, t)]$
(cụ thể, $V'(k, m, t)$ outputs “1” nếu t là một tag hợp lệ cho hoặc m hoặc $m \oplus 1^n$).
- $S'(k, m) = S(k, m)$ và
 $V'(k, m, t) = [\text{if } m \neq 0^n \text{ return } V(k, m, t) \text{ else return “1”}]$

Total of marks: 1

10 Chữ ký số

(1) **Chữ ký RSA** MULTIPLE CHOICE Multiple answers allowed

Cho sơ đồ chữ ký RSA (không kết hợp với hàm băm) với khoá công khai ($n = 9797, e = 131$), những chữ ký nào dưới đây là hợp lệ?

- ($m = 4333, \sigma = 1424$)
- ($m = 4333, \sigma = 4768$)
- ($m = 123, \sigma = 6292$)

(2) **Chữ ký ElGamal** SHORT ANSWER Case-Insensitive

Ta xem xét sơ đồ chữ ký ElGamal. Bạn có khoá bí mật của Bob $sk = d = (67)$ và khoá công khai tương ứng $pk = (p, g, g^d) = (97, 23, 15)$. Hãy tính chữ ký Elgamal (r, s) cho thông điệp $m = 17$ và khoá tạm thời $k_E = 31$.

Chữ ký (r, s) là _____.

Chú ý: Hãy viết chữ ký dưới dạng (\mathbf{r}, \mathbf{s}) không có dấu cách ở giữa.

Total of marks: 2