

**Question 1**

Answer saved

Marked out of 1.00

Flag question

Hãy dùng thuật toán tính lũy thừa nhanh để tính  $779^{279998} \bmod 11413$  biết rằng  $11413 = (101 \times 113)$ .

Giá trị  $779^{279998} \bmod 11413$  bằng

**Question 2**

Not yet answered

Marked out of 1.00

Flag question

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  $m = 18$  và khoá tạm thời  $k_E = 35$ .

Chữ ký  $(r, s)$  là

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

**Question 3**

Not yet answered

Marked out of 1.00

Flag question

Xét sơ đồ mã hoá RSA được cài đặt các tham số  $p = 13$  và  $q = 11$ . Khoá công khai là  $e = 7$ . Ta cần giải mã bản mã  $y = 3$ .  
Ta giải mã được bản rõ  $x$  bằng

**Question 4**

Not yet answered

Marked out of 1.00

Flag question

Xét đường cong Elliptic

$$E: y^2 = x^3 + 2x + 2 \bmod 17$$

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  $P = (13, 10)$ . Hãy tính điểm  $Q = 312 \cdot P$ .

Điểm  $Q$  là

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

**Question 5**

Not yet answered

Marked out of 1.00

Flag question

Xét  $\mathbb{Z}_{19}^*$  là một nhóm cyclic với 3 là một phần tử sinh. Hãy tính giá trị  $DH_3(11, 8)$  trong nhóm này.  
Giá trị  $DH_3(11, 8)$  bằng

Question 3  
Not yet answered  
Marked out of 1.00  
Flag question

Xét sơ đồ mã hoá RSA được cài đặt các tham số  $p = 13$  và  $q = 11$ . Khoá công khai là  $e = 7$ . Ta cần giải mã bản mã  $y = 3$ .  
Ta giải mã được bản rõ  $x$  bằng

Question 4  
Not yet answered  
Marked out of 1.00  
Flag question

Xét đường cong Elliptic

$$E: y^2 = x^3 + 2x + 2 \bmod 17$$

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

### Question 6

Not yet answered

Marked out of 1.00

Flag question

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

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: "xx" dùng CBC mode với IV=S là

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

### Question 7

Not yet answered

Marked out of 1.00

Flag question

Những phần tử nào dưới đây là phần tử sinh của  $\mathbb{Z}_{17}^*$ ?

Select one or more:

- ☐ a. 6,  $\langle 6 \rangle = \{1, 6, 2, 12, 4, 7, 8, 14, 16, 11, 15, 5, 13, 10, 9, 3\}$
- ☐ b. 3,  $\langle 3 \rangle = \{1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6\}$
- ☐ c. 5,  $\langle 5 \rangle = \{1, 5, 8, 6, 13, 14, 2, 10, 16, 12, 9, 11, 4, 3, 15, 7\}$
- ☐ d. 7,  $\langle 7 \rangle = \{1, 7, 15, 3, 4, 11, 9, 12, 16, 10, 2, 14, 13, 6, 8, 5\}$
- ☐ e. 2,  $\langle 2 \rangle = \{1, 2, 4, 8, 16, 15, 13, 9, 1, 2, 4, 8, 16, 15, 13, 9\}$

### Question 8

Not yet answered

Marked out of 1.00

Flag question

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

Bản mã của thông điệp: "DVKDQVXQNG" dùng ECB mode là

### Question 9

Not yet answered

Marked out of 1.00

Flag question

Cho sơ đồ chữ ký RSA (không kết hợp với hàm băm) với khoá công khai  $(n = 9797, e = 3)$ , những chữ ký nào dưới đây là hợp lệ?

Select one or more:

- ☐  $(m = 2015, \sigma = 1695)$
- ☐  $(m = 4706, \sigma = 1683)$
- ☐  $(m = 1894, \sigma = 1629)$
- ☐  $(m = 2600, \sigma = 8502)$

### Question 10

Not yet answered

Marked out of 1.00

Flag question

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  $m = 20$  và khoá tạm thời  $k_E = 35$ .  
Chữ ký  $(r, s)$  là

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

**Question 11**

Not yet  
answered

Marked out of  
1.00

Flag question

Hệ mật mã khoá đối xứng có

Select one or more:

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

**Question 12**

Not yet  
answered

Marked out of  
1.00

Flag question

Xét sơ đồ mã hoá RSA được cài đặt các tham số  $p = 11$  và  $q = 13$ . Khoá công khai là  $e = 7$ . Ta cần giải mã **bản mã**  $y = 2$ .  
Ta giải mã được bản rõ  $x$  bằng

**Question 13**

Not yet  
answered

Marked out of  
1.00

Flag question

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  $m = 21$  và khoá tạm thời  $k_E = 35$ .  
Chữ ký  $(r, s)$  là

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

**Question 14**

Not yet  
answered

Marked out of  
1.00

Flag question

Xét sơ đồ mã hoá RSA được cài đặt các tham số  $p = 13$  và  $q = 11$ . Khoá công khai là  $e = 7$ . Ta cần giải mã **bản mã**  $y = 10$ .  
Ta giải mã được bản rõ  $x$  bằng

**Question 15**

Not yet  
answered

Marked out of  
1.00

Flag question

Hãy tính logarit rời rạc của 10 với cơ sở 2 trong  $\mathbb{Z}_{13}^*$ .  
Giá trị của  $\text{Dlog}_2(10)$  bằng

**Question 16**

Not yet  
answered

Marked out of  
1.00

Flag question

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  $m = 27$  và khoá tạm thời  $k_E = 35$ .  
Chữ ký  $(r, s)$  là

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

**Question 17**Not yet  
answeredMarked out of  
1.00

Flag question

Cho sơ đồ chữ ký RSA (không kết hợp với hàm băm) với khoá công khai  $(n = 9797, e = 3)$ , những chữ ký nào dưới đây là hợp lệ?

Select one or more:

- ☐  $(m = 3310, \sigma = 1874)$
- ☐  $(m = 3964, \sigma = 1871)$
- ☐  $(m = 9067, \sigma = 1870)$
- ☐  $(m = 5078, \sigma = 1873)$

**Question 16**Not yet  
answeredThì xem xét sơ đồ chữ ký ElGamal. Bạn có khoá bí mật cá  
tương ứng là  $(p, g, a) = (97, 2, 15)$ . Hãy tính chữ k  
và khóa tạm thời  $k_0 = 304$ .**Question 18**Not yet  
answeredMarked out of  
1.00

Flag question

Xét  $\mathbb{Z}_{19}^*$  là một nhóm cyclic với 3 là một phần tử sinh. Hãy tính giá trị  $DH_3(2, 4)$  trong nhóm này.  
Giá trị  $DH_3(2, 4)$  bằng

**Question 19**Not yet  
answeredMarked out of  
1.00

Flag question

Hãy tính logarit rời rạc của 9 với cơ sở 2 trong  $\mathbb{Z}_{13}^*$ .  
Giá trị của  $Dlog_2(9)$  bằng

**Question 20**Not yet  
answeredMarked out of  
1.00

Flag question

Select one or more:

- ☐  $(m = 6006, \sigma = 1869)$
- ☐  $(m = 8987, \sigma = 1872)$
- ☐  $(m = 6022, \sigma = 1868)$
- ☐  $(m = 6549, \sigma = 1867)$

**Những** thành phần mật mã nào dưới đây nhằm bảo mật thông điệp?

Select one or more:

- ☐ Sơ đồ chữ ký số
- ☐ Mã xác thực thông điệp
- ☐ Hệ mật mã khoá đối xứng
- ☐ Hàm băm
- ☐ Hệ mật mã khoá công khai

**Question 22**

Not yet  
answered

Marked out of  
1.00

Flag question

Giả sử bạn biết mã hóa của thông điệp "gui duc 100d" dùng one time pad encryption là

$$\langle CODE \rangle > 6c73d5240a948c86981bc294 \langle /CODE \rangle$$

(bản rõ ở dạng mã ASCII 8-bit và bản mã được viết ở dạng hexa). Bản mã của thông điệp "gui duc 010d" với cùng khóa OTP là

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

**Question 23**

Not yet  
answered

Marked out of  
1.00

Flag question

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

Giá trị  $770^{279999} \bmod 11413$  bằng

**Question 24**

Not yet  
answered

Marked out of  
1.00

Flag question

Xét sơ đồ mã hoá RSA được cài đặt các tham số  $p = 11$  và  $q = 13$ . Khoá công khai là  $e = 7$ . Ta cần giải mã bản mã  $y = 5$ .

Ta giải mã được bản rõ  $x$  bằng

**Question 25**

Not yet  
answered

Marked out of  
1.00

Flag question

Hãy tính logarit rời rạc của 11 với cơ sở 2 trong  $\mathbb{Z}_{13}^*$ .

Giá trị của  $\text{Dlog}_2(11)$  bằng

**Question 26**

Not yet  
answered

Marked out of  
1.00

Flag question

Giả sử bạn biết mã hóa của thông điệp "gui duc 100d" dùng one time pad encryption là

$$\langle CODE \rangle > 6c73d5240a948c86981bc294 \langle /CODE \rangle$$

(bản rõ ở dạng mã ASCII 8-bit và bản mã được viết ở dạng hexa). Bản mã của thông điệp "gui duc 010d" với cùng khóa OTP là

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

**Question 27**

Not yet  
answered

Marked out of  
1.00

Flag question

Cho sơ đồ chữ ký RSA (không kết hợp với hàm băm) với khoá công khai  $(n = 9797, e = 3)$ , những chữ ký nào dưới đây là hợp lệ?

Select one or more:

- ☐  $(m = 8481, \sigma = 1866)$
- ☐  $(m = 8966, \sigma = 1672)$
- ☐  $(m = 6022, \sigma = 1898)$
- ☐  $(m = 6549, \sigma = 1967)$

**Question 28**

Not yet  
answered

Marked out of  
1.00

Flag question

Cho sơ đồ chữ ký RSA (không kết hợp với hàm băm) với khoá công khai  $(n = 9797, e = 3)$ , những chữ ký nào dưới đây là hợp lệ?

Select one or more:

- ☐  $(m = 3310, \sigma = 1274)$
- ☐  $(m = 5078, \sigma = 1973)$
- ☐  $(m = 3134, \sigma = 1871)$
- ☐  $(m = 9207, \sigma = 1870)$

**Question 29**

Not yet  
answered

Marked out of  
1.00

Flag question

Giả sử có  $n + 1$  bên, gọi là  $B, A_1, \dots, A_n$ , muốn có một khóa chung cho cả nhóm. Họ muốn có một giao thức sao cho mọi người đều có chung một khóa bí mật, nhưng kẻ nghe lén dù thấy được toàn bộ quá trình trao đổi vẫn không xác định được  $k$ . Các bên thống nhất một nhóm  $G$  có cấp nguyên tố  $q$  với phần tử sinh  $g$  và dùng giao thức sau đây :

- Mỗi bên  $A_i$  chọn một số ngẫu nhiên  $a_i$  thuộc  $\{1, \dots, q\}$  và gửi cho Bên  $B$  giá trị  $X_i \leftarrow g^{a_i}$ .
- Bên  $B$  sinh một số ngẫu nhiên  $b$  thuộc  $\{1, \dots, q\}$  và trả lại bên  $A_i$  thông điệp  $Y_i \leftarrow X_i^b$ .

Khóa cuối cùng của nhóm là  $g^b$ . Rõ ràng Bên  $B$  có thể tính được khóa này. Các bên  $A_i$  tính khóa này như thế nào?

Select one:

- ☐ Bên  $A_i$  tính  $g^b$  bằng  $Y_i^{a_i}$
- ☐ Bên  $A_i$  tính  $g^b$  bằng  $Y_i^{-a_i}$
- ☐ Bên  $A_i$  tính  $g^b$  bằng  $Y_i^{1/a_i}$
- ☐ Bên  $A_i$  tính  $g^b$  bằng  $Y_i^{-1/a_i}$

**Question 30**Not yet  
answeredMarked out of  
1.00

Flag question

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  $a$  và tính điểm  $aP = (3, 16)$  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.

**Question 31**Not yet  
answeredMarked out of  
1.00

Flag question

Cho sơ đồ chữ ký RSA (không kết hợp với hàm băm) với khoá công khai  $(n = 9797, e = 3)$ , những chữ ký nào dưới đây là hợp lệ?

Select one or more:

- ☐  $(m = 4706, \sigma = 1673)$
- ☐  $(m = 1829, \sigma = 1629)$
- ☐  $(m = 2630, \sigma = 8502)$
- ☐  $(m = 2015, \sigma = 1865)$

**Question 32**Not yet  
answeredMarked out of  
1.00

Flag question

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  $a$  và tính điểm  $aP = (7, 6)$  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.

**Question 33**

Not yet answered

Marked out of 1.00

Flag question

Xét sơ đồ mã hoá RSA được cài đặt các tham số  $p = 13$  và  $q = 11$ . Khoá công khai là  $e = 7$ . Ta cần giải mã **bản mã**  $y = 3$ . Ta giải mã được bản rõ  $x$  bằng

Next

**Question 34**

Not yet answered

Marked out of 1.00

Flag question

Hãy dùng thuật toán Euclid mở rộng để tính  $17^{-1} \bmod 113$ . Giá trị  $17^{-1}$  là

**Question 35**

Not yet answered

Marked out of 1.00

Flag question

Xét  $\mathbb{Z}_{19}^*$  là một nhóm cyclic với 3 là một phần tử sinh. Hãy tính giá trị  $\text{DH}_3(7, 17)$  trong nhóm này. Giá trị  $\text{DH}_3(7, 17)$  bằng

Next

**Question 36**

Not yet answered

Marked out of 1.00

Flag question

Hệ mật mã khoá công khai có

Select one or more:

- ☐ hai khoá khác nhau.
- ☐ 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.
- ☐ khoá mã hoá và khoá giải mã giống nhau.

**Question 37**

Not yet answered

Marked out of 1.00

Flag question

Hãy dùng thuật toán Euclid mở rộng để tính  $15^{-1} \bmod 113$ . Giá trị  $15^{-1}$  là

**Question 32**

Not yet answered

Marked out of 1.00

Flag question

Xét đường cong Elliptic

$$E: y^2 = x^3 + 2x$$

Để tiện cho việc tính toán, các điểm là bội của phần tử

$k$	1	2	3	4	5
$k \cdot G$	(5, 1)	(6, 3)	(10, 6)	(3, 1)	(9, 16)
$k \cdot H$	11	12	13	14	15
$k \cdot G + H$	(13, 10)	(0, 1)	(16, 3)	(9, 1)	(3, 19)

**Question 34**

Not yet answered

Marked out of 1.00

Flag question

Hãy dùng thuật toán Euclid mở rộng để tính  $17^{-1}$

Giá trị  $17^{-1}$  là

**Question 35**

Not yet answered

Marked out of 1.00

Flag question

Xét  $\mathbb{Z}_{19}^*$  là một nhóm cyclic với 3 là một phần tử sinh. Hãy tính

giá trị  $\text{DH}_3(7, 17)$  bằng



**Question 38**

Not yet answered

Marked out of 1.00

Flag question

Cho sơ đồ chữ ký RSA (không kết hợp với hàm băm) với khoá công khai  $(n = 9797, e = 3)$ , những chữ ký nào dưới đây là hợp lệ?

Select one or more:

- ☐  $(m = 8287, \sigma = 1872)$
- ☐  $(m = 6906, \sigma = 1869)$
- ☐  $(m = 3934, \sigma = 1871)$
- ☐  $(m = 9007, \sigma = 1870)$

**Question 39**

Not yet answered

Marked out of 1.00

Flag question

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  $m = 19$  và khoá tạm thời  $k_E = 35$ .

Chữ ký  $(r, s)$  là

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

**Question 40**

Not yet answered

Marked out of 1.00

Flag question

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  $a$  và tính điểm  $aP = (6, 14)$  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.

**Question 41**

Not yet answered

Marked out of 1.00

Flag question

Giả sử bạn biết mã hóa của thông điệp "gui duc 100d" dùng one time pad encryption là

<CODE> 6c73d5240a948c86981bc294 </CODE>

(bản rõ ở dạng mã ASCII 8-bit và bản mã được viết ở dạng hexa). Bản mã của thông điệp "gui duc 111d" với cùng khóa OTP là

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

**Question 42**

Not yet answered

Marked out of 1.00

Flag question

Hãy dùng thuật toán Euclid mở rộng để tính  $16^{-1} \bmod 113$ .  
 Giá trị  $16^{-1}$  là

**Question 41**

Not yet answered

Giá trị bí mật mã hóa của thông điệp "a" là bao nhiêu?

&lt; CODE &gt; 6c73d5240a94866981b

**Question 43**

Not yet answered

Marked out of 1.00

Flag question

Xét  $G$  là một nhóm cyclic (còn gọi là nhóm vòng) cấp  $n$  và xét một biến thể sau đây của hệ mật mã ElGamal trong  $G$ :

- **Hàm sinh khoá:** chọn một phần tử sinh ngẫu nhiên  $g$  trong  $G$  và một số ngẫu nhiên  $x$  trong  $\mathbb{Z}_n$ . Output  $pk = (g, h = g^x)$  và  $sk = (g, x)$ .
- **Hàm mã hoá**  $E(pk, m \in G)$ : chọn một số ngẫu nhiên  $r$  trong  $\mathbb{Z}_n$  và output  $(g^r, m \cdot h^r)$ .
- **Hàm giải mã**  $D(sk, (c_0, c_1))$ : output  $c_1/c_0^x$ .

Biến thể ElGamal này không an toàn trước tấn công chọn bản mã vì ta có thể dễ dàng tính toán trên bản mã. Có nghĩa rằng, xét  $(c_0, c_1)$  là output của  $E(pk, m_0)$  và xét  $(c_2, c_3)$  là output của  $E(pk, m_1)$ . Khi đó, cho hai bản mã này, ta có thể dễ dàng xây dựng được bản mã của của  $m_0 \cdot m_1$  như sau:

Select one:

- ☐  $(c_0/c_3, c_1/c_2)$  là mã hoá của  $m_0 \cdot m_1$ .
- ☐  $(c_0 \cdot c_2, c_1 \cdot c_3)$  là mã hoá của  $m_0 \cdot m_1$ .
- ☐  $(c_0 + c_2, c_1 + c_3)$  là mã hoá của  $m_0 \cdot m_1$ .
- ☐  $(c_0 \cdot c_3, c_1 \cdot c_2)$  là mã hoá của  $m_0 \cdot m_1$ .

**Question 44**

Not yet answered

Marked out of 1.00

Flag question

Trong hệ mật RSA chuẩn, modun  $N$  là tích của hai số nguyên tố phân biệt. Giả sử ta chọn modun sao cho nó là tích của ba số nguyên tố, tức là  $N = pqr$ . Cho số mũ  $e$  nguyên tố cùng nhau với  $\varphi(N)$  ta có thể tính khoá bí mật  $d = e^{-1} \bmod \varphi(N)$ . Khoá công khai  $(N, e)$  và khoá bí mật  $(N, d)$  vẫn giống như trước đây. Giá trị  $\varphi(N)$  là gì khi  $N$  là tích của ba số nguyên tố?

Select one:

- ☐  $\varphi(N) = (p-1)(q-1)(r-1)$
- ☐  $\varphi(N) = (p-1)(q-1)$
- ☐  $\varphi(N) = (p-1)(q-1)(r+1)$
- ☐  $\varphi(N) = (p-1)(q-1)r$

**Question 43**

Not yet answered

Marked out of 1.00

Flag question

Xét  $G$  là một nhóm cyclic (còn gọi là nhóm vòng) mã ElGamal trong  $G$ .

- **Hàm sinh khoá:** chọn một phần tử sinh ngẫu nhiên  $g$  trong  $G$ . Output  $pk = (g, h = g^x)$  và  $sk = (g, x)$ .
- **Hàm mã hoá**  $E(pk, m \in G)$ : chọn một số ngẫu nhiên  $r$  trong  $\mathbb{Z}_n$  và output  $(g^r, m \cdot h^r)$ .
- **Hàm giải mã**  $D(sk, (c_0, c_1))$ : output  $c_1/c_0^x$ .

Biến thể ElGamal này không an toàn trước tấn công chọn bản mã. Có nghĩa rằng, xét  $(c_0, c_1)$  là output của  $E(pk, m_0)$  và  $(c_2, c_3)$  là output của  $E(pk, m_1)$ . Khi đó, cho hai bản mã này, ta có thể xây dựng được bản mã của  $m_0 \cdot m_1$  như sau:

Select one:

- ☐  $(c_0/c_3, c_1/c_2)$  là mã hoá của  $m_0 \cdot m_1$ .
- ☐  $(c_0 \cdot c_2, c_1 \cdot c_3)$  là mã hoá của  $m_0 \cdot m_1$ .

**Question 45**

Not yet answered

Marked out of 1.00

Flag question

Hãy dùng thuật toán tính lũy thừa nhanh để tính  $779^{279997} \bmod 11413$  biết rằng  $11413 = (101 \times 113)$ .  
 Giá trị  $779^{279997} \bmod 11413$  bằng

**Question 44**

Not yet answered

Trong hệ mật RSA chuẩn, modun  $N$  là tích của hai số nguyên tố phân biệt. Giả sử ta chọn modun sao cho nó là tích của ba số nguyên tố, tức là  $N = pqr$ . Cho số mũ  $e$  nguyên tố cùng nhau với  $\varphi(N)$  ta có thể tính khoá bí mật  $d = e^{-1} \bmod \varphi(N)$ .