TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Họ tên SV: ..... MSSV: .....

Học phần: **Nhập môn An toàn Thông tin** ..... Mã HP: .....

Bài thi [X] giữa kỳ [ ] cuối kỳ ..... Ngày thi:.....

Số thứ tự

Điểm của bài thi	Chữ ký của (các) cán bộ chấm thi	Chữ ký của cán bộ coi thi

Đề thi giữa kỳ Nhập môn An toàn Thông tin
Thời gian 90 phút. Được sử dụng tài liệu trong khi làm bài.

1. Hãy dùng thuật toán Euclid mở rộng để tính $19^{-1} \mod 799$.

2. Hãy dùng thuật toán tính luỹ thừa nhanh để tính $977^{280001} \mod 11413$ biết rằng $11413 = (101 \times 113)$.

3. Xét nhóm $\mathbb{Z}_{23}^*$ với 5 là một phần tử sinh. Hãy tính logarit rời rạc $\mathrm{Dlog}_5(16)$ trong nhóm này; và dùng nó để tính giá trị của hàm Diffie-Hellman $\mathrm{DH}_5(16, 15)$.

Nhắc lại: Hàm Diffie-Hellman định nghĩa bởi $\mathrm{DH}_g(g^a,\ g^b) = g^{ab}$.

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

(a) 2, $\langle 2\rangle = \{1,2,4,8,16,15,13,9,1,2,4,8,16,15,13,9\}$

(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) 6, $\langle 6\rangle = \{1,6,2,12,4,7,8,14,16,11,15,5,13,10,9,3\}$

5. Nhóm $\mathbb{Z}_{170}^*$ có bao nhiêu phần tử? Hãy giải thích ngắn gọn cách tính.

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

7. 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 $y \in G$, tìm x sao cho $g^x = y$

(b) Lấy ngẫu nhiên hai giá trị $x \in \mathbb{Z}_q$ và $y \in G$, tính $y^x \cdot g$

(c) Lấy ngẫu nhiên $x \in \mathbb{Z}_q$, tìm y sao cho $g^x = y$

(d) Tìm x và y sao cho $g^x = y$.

8. Tính đa thức

$$(x^7 + x^4 + x + 1)/(x^7 + x^6 + x^3 + x^2 + 1),$$

trong $GF(2^8)$ với đa thức bất khả quy là $P(x) = x^8 + x^4 + x^3 + x + 1$ (đa thức AES).

9. Xét đường cong Elliptic

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

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 $Q = 78 \cdot P$.

10. Xét đường cong Elliptic

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

và 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 $bP = (10, 11)$ từ Bob.

Hãy tính khoá chia sẻ abP giữa Alice và Bob.

11. 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? Hãy giải thích.

1. Cho trước N, e, và lấy ngẫu nhiên $y \in \mathbb{Z}_N^*$, tìm x sao cho $x^e = y \mod N$.

2. Cho trước N và e, tìm x, y sao cho $x^e = y \mod N$.

3. Cho trước N và e, tìm x sao cho $x^e = 8 \mod N$.

4. Cho trước N, e, và lấy ngẫu nhiên $x \in \mathbb{Z}_N^*$, tìm y sao cho $x^e = y \mod N$

12. Giả sử bạn biết mã hóa của thông điệp "`gui duc 100d`" 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 "`gui duc 321d`" với cùng khóa OTP là gì?

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

13. Xét hệ mã khối **BkExam** chuyên dùng cho thi giữa 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 `XOR` không định nghĩa trên tập $\{A, \ldots, Z\}$, ta thay thế nó với phép cộng theo modun 26 (ví dụ, $C \oplus D = F$ và $Y \oplus C = A$).

Hãy mã hoá thông điệp: "`NMATTT`" dùng

(a) ECB mode;

(b) CBC mode với IV là chữ X.

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

Bản rõ x tương ứng với bản mã $y = 2$ là gì?

15. Xét F là một hệ mã khối an toàn với kích thước khối n. Những hệ MAC nào dưới đây là an toàn? Nếu không an toàn hãy chỉ ra một cách tấn công; còn nếu có thì hãy chứng minh.

(a) Để xác thực thông điệp $m = m_1 \dots m_\ell$ với $m_i \in \{0,1\}^n$, ta tính tag

$$t := F_k(m_1) \oplus \cdots \oplus F_k(m_\ell).$$

(b) Để xác thực thông điệp $m = m_1 \dots m_\ell$ với $m_i \in \{0,1\}^{n/2}$, ta tính tag

$$t := F_k(\langle 1 \rangle \| m_1) \oplus \cdots \oplus F_k(\langle \ell \rangle) \| m_\ell)$$

với $\langle i \rangle$ là biểu diễn dạng $n/2$-bit của số nguyên i.

16. Người ta muốn xây dựng hệ MAC $\mathscr{I}$ dùng hai hệ MAC $\mathscr{I}_1 = (S_1, V_1)$ và $\mathscr{I}_2 = (S_2, V_2)$, sao cho tại một thời điểm nào đó một trong hai hệ $\mathscr{I}_1$ hoặc $\mathscr{I}_2$ bị phá (nhưng không phải cả hai cùng bị phá) thì $\mathscr{I}$ vẫn an toàn.

Định nghĩa $\mathscr{I} = (S, V)$ trong đó

$$S((k_1, k_2), m) := (S_1(k_1, m), S_2(k_2, m)),$$

và V định nghĩa bởi: trên input $((k_1, k_2), m, (t_1, t_2))$, V chấp nhận nếu và chỉ nếu cả $V_1(k_1, m, t_1)$ và $V_2(k_2, m, t_2)$ đều chấp nhận. Hãy chứng minh rằng $\mathscr{I}$ an toàn nếu $\mathscr{I}_1$ an toàn **hoặc** $\mathscr{I}_2$ an toàn.

17. 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 $\|$ ký hiệu phép ghép xâu.

(a) $H''(x) = H(x) \,\|\, 0 \ldots 0$

(b) $H''(x) = H(H'(x))$

(c) $H''(x) = H(x) \,\|\, H'(x)$

(d) $H''(x) = H(x) \oplus H'(x)$.

18. 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?

(a) $(m = 123, \sigma = 6292)$

(b) $(m = 4333, \sigma = 4768)$

(c) $(m = 4333, \sigma = 1424)$

19. 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 $k_E = 31$.

20. Hãy chỉ ra sự khác biệt giữa sơ đồ chữ ký ElGamal và sơ đồ chữ ký DSA.