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 [ ] giữa kỳ [X] 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

Ôn tập Nhập môn An Toàn Thông Tin
Thời gian 90 phút. Không sử dụng tài liệu.

1. Hãy dùng thuật toán Euclid mở rộng để tính $18^{-1} \mod 799$. Hãy mô tả chi tiết từng bước trong quá trình tính toán.
2. Hãy dùng thuật toán tính luỹ thừa nhanh để tính $976^{3532} \mod 11413$.
3. Xét nhóm $\mathbb{Z}_{23}^*$ với 5 là một phần tử sinh. Hãy tính logarit rời rạc $\mathsf{Dlog}_5(17)$ trong nhóm này; và dùng nó để tính giá trị của hàm Diffie-Hellman $\mathsf{DH}_5(17, 15)$.
4. Tính đa thức
$$(x^6 + x^4 + x + 1)/(x^7 + x^6 + x^3 + x^2 + 1),$$
trong $GF(2^8)$ với đa thức bất khả quy là $P(x) = x^8 + x^4 + x^3 + x + 1$ (đa thức AES).
5. Xét đường cong Elliptic
$$E: \quad y^2 = x^3 + 2x + 2 \mod 17$$
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 $bP = (16, 13)$ từ Bob.

   Hãy tính khoá chia sẻ abP giữa Alice và Bob.
6. 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.
   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 và e, tìm x sao cho $x^e = 8 \bmod N$.
   D) Cho trước N, e, và lấy ngẫu nhiên $x \in \mathbb{Z}_N^*$, tìm y sao cho $x^e = y \bmod N$

7. Xét hệ mã khối BkExam chuyên dùng cho thi cuối kỳ. Nó có kích thước khối là 4 bit và độ dài khoá là 64 bit. Mỗi khối được viết như một số hexa, ví dụ $5 \oplus 9 = c$.

Hàm mã hoá BkExam với khoá cụ thể K được cho bởi bảng sau:

m	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$E_K(m)$	c	8	2	7	d	0	6	1	a	e	f	4	b	9	5	3

Biết rằng thông điệp được mã hoá dùng các mode như dưới đây. Hãy giải mã nó.

(a) ECB mode với bản mã `c994f88`

(b) CBC mode với bản mã `b144f`

8. 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.

9. Xét hàm băm kháng xung đột $H : \{0,1\}^\ell \to \{0,1\}^n$. Với mỗi hàm băm H_i dưới đây, hãy giải thích tại sao H_i là kháng xung đột, hoặc mô tả cách hiệu quả để tìm xung đột cho H_i:

(a) Với $\Delta \neq O^\ell$ cố định, ta định nghĩa $H_1(m) := H(m) \oplus H(m \oplus \Delta)$.

(b) Với $\Delta \neq O^\ell$ cố định, ta định nghĩa $H_2(m) := H(m) \oplus \Delta$.

10. Xét (Gen, S, V) là sơ đồ chữ ký số (chống giả mạo) với không gian thông điệp $\{0,1\}^*$. Sinh cặp khoá ký/kiểm tra chữ ký $(pk_0, sk_0) \leftarrow Gen()$ và $(pk_1, sk_1) \leftarrow Gen()$. Những sơ đồ nào dưới đây là an toàn? Hãy giải thích ngắn gọn.

(a) Ký: $S_1(sk_0, m) := S(sk_0, m \| m)$. Kiểm tra: $V_1(pk_0, m, \sigma) := V_1(pk_0, m \| m, \sigma)$.

(b) Ký với giá trị ngẫu nhiên: với $m \in \{0,1\}^n$ thực hiện:

$$S_2(sk_0, m) := [\text{ chọn ngẫu nhiên } r \leftarrow \{0,1\}^n,\ \text{output } (r,\ S(sk_0, m \oplus r),\ S(sk_0, r))\ ]$$
$$V_2(pk_0, m, (r,\ \sigma_0,\ \sigma_1)) = 1 \quad \Leftrightarrow \quad V(pk_0,\ m \oplus r,\ \sigma_0) = V(pk_0,\ r,\ \sigma_1) = 1$$

11. Máy chủ email BK Mail mã hoá mọi email gửi tới Bob bằng khoá công khai pk_{bob} của Bob. Khi Bob đi nghỉ mát, Bob ra lệnh BK Mail: với tất cả email được gửi tới Bob, hãy chuyển tiếp cho đồng nghiệp Alice xử lý. Khóa công khai của Alice là pk_{alice}. Để làm điều này, BK Mail cần một cách để **dịch** một email được mã hóa theo khoá công khai pk_{bob} thành một email được mã hóa theo khoá công khai pk_{alice} của Alice. Việc này có thể thực hiện dễ dàng nếu BK Mail có sk_{bob}, nhưng vấn đề là, sau đó BK Mailcó thể đọc tất cả email gửi tới Bob, đây là điều Bob không muốn!

Xét $\mathbb{G}$ là một nhóm cấp nguyên tố q và $g \in \mathbb{G}$ là một phần tử sinh. Ta xét một biến thể của hệ mật ElGamal trong đó khoá công khai là $pk := u = g^\alpha \in \mathbb{G}$ và hàm mã hoá định nghĩa như sau:

$$E(pk, m) = \left\{\beta \leftarrow \mathbb{Z}_q,\ v = g^\beta,\ k = H(u^\beta),\ c = E_{\text{sym}}(k, m),\ \text{output } (v, c)\right\}$$

với E_{sym} là hệ mã khoá đối xứng với không gian khoá $\mathscr{K}_{\text{sym}}$, và H là một hàm băm $H : \mathbb{G} \to \mathscr{K}_{\text{sym}}$.

Giả sử rằng pk_{bob} và pk_{alice} là khoá công khai trong sơ đồ mã hoá trên với khoá bí mật tương ứng là $sk_{\text{bob}} = \alpha \in \mathbb{Z}_q$ và $sk_{\text{alice}} = \alpha' \in \mathbb{Z}_q$. Để cho phép dịch bản mã từ pk_{bob} cho pk_{alice}, Alice và Bob cùng nhau tính $\tau := \alpha/\alpha' \in \mathbb{Z}_q$. Họ gửi τ tới máy chủ BK Mail.

(a) Hãy giải thích cách mà máy chủ BK Mail dùng τ để dịch bản mã $c \leftarrow E(pk_{\text{bob}}, m)$ thành bản mã c' cho pk_{alice} cho cùng thông điệp m.

(b) Hãy giải thích cách mà BM Mail dùng τ để dịch bản mã theo hướng ngược lại. Tức là, nếu $c \leftarrow E(pk_{\text{alice}}, m)$ thì BK Mail có thể xây dựng bản mã c' cho pk_{bob} cho cùng thông điệp m.

(c) Khi Bob quay về sau kỳ nghỉ mát, anh ta phải làm gì để từ nay Alice không còn đọc được email của anh ta nữa?

12. Giả sử Alice và Bob mỗi người sống ở một trong 63 tỉnh thành. Alice hiện sống ở tỉnh $a \in \{1, \ldots, 63\}$ và Bob đang sống ở tỉnh $b \in \{1, \ldots, 64\}$. Họ có thể giao tiếp với nhau và Alice muốn kiểm tra liệu cô ấy có sống cùng tỉnh với Bob không. Nếu họ ở cùng tỉnh, Alice có thể biết điều này; nhưng nếu không thì cô ấy không biết liệu Bob đang ở tỉnh nào. Bob không được biết gì về tỉnh mà Alice đang sống.

Họ thống nhất với nhau sơ đồ sau:

- Họ cố định một nhóm $\mathbb{G}$ (có thể là nhóm $\mathbb{Z}_p^*$ hoặc nhóm điểm trên đường cong Elliptic) có cấp q và một phần tử sinh g.
- Alice chọn ngẫu nhiên x và y thuộc $\mathbb{Z}_q$ và gửi cho Bob $(A_0, A_1, A_2) = (g^x, g^y, g^{xy+a})$
- Bob chọn ngẫu nhiên r và s thuộc $\mathbb{Z}_q$ và gửi lại cho Alice $(B_1, B_2) = (A_1^r g^s,\ (A_2/g^b)^r A_0^s)$

Bây giờ, Alice nên làm gì để kiểm tra liệu Bob có cùng tỉnh với mình (tức là kiểm tra $a = b$)?

Để ý rằng Bob không lấy được thông tin gì từ giao thức này bởi vì anh ấy đơn giản nhận được bản mã Elgammal "đơn giản" của g^a với khoá công khai g^x. Ta có thể chỉ ra rằng nếu $a \neq b$ thì Alice không có thông tin gì từ giao thức này vì cô ấy nhận được bản mã của một giá trị ngẫu nhiên.

A) Alice kiểm tra $a = b$ bằng cách kiểm tra nếu $B_2^x / B_1 = 1$.

B) Alice kiểm tra $a = b$ bằng cách kiểm tra nếu $B_2^x B_1 = 1$.

C) Alice kiểm tra $a = b$ bằng cách kiểm tra nếu $B_2 B_1^x = 1$.

D) Alice kiểm tra $a = b$ bằng cách kiểm tra nếu $B_2 / B_1^x = 1$.

E) Alice kiểm tra $a = b$ bằng cách kiểm tra nếu $B_2 / B_1 = 1$.