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: IT4015 .....

Bài thi: giữa kỳ [ ] cuối kỳ [X] ..... Ngày thi: 10/07/2020....

| Số thứ tự |
| --- |
| |

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

Thời gian 90 phút. Không được sử dụng tài liệu. **Đề lẻ**

1. Hãy dùng thuật toán Euclid mở rộng để tính $15^{-1} \mod 799$. Hãy mô tả chi tiết từng bước trong quá trình tính toán.

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

3. Xét nhóm $\mathbb{Z}_{23}^*$ với 5 là một phần tử sinh. Hãy tính logarit rời rạc $\mathsf{Dlog}_5(17)$ trong nhóm này; và dùng nó để tính giá trị của hàm Diffie-Hellman $\mathsf{DH}_5(16, 17)$.

Bảng 1. Các điểm $k \cdot G$ với $G = (5,1)$ trên đường cong $E$.

| $k$ | 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) | $\mathcal{O}$ | |

**4.** 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 4.

Xét điểm $P = (16,13)$. 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 $a = 6$ và gửi điểm $aP$ cho Bob;
- Nhận được điểm $bP = (10,11)$ từ Bob.

Hãy tính khoá chia sẻ $abP$ giữa Alice và Bob.

**5.** Xét sơ đồ chữ ký RSA "đơn giản" với khoá công khai $(N, e)$. Giả sử rằng bạn đã có chữ ký $\sigma$ của thông điệp $m_1 = 17$. Hãy mô tả cách tấn công giả mạo chữ ký cho thông điệp $m_3 = 4913$. (Giả sử $N > 2^{2048}$.)

**6.** 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 $\{A, \ldots, Z\}$, 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: "SECURITY" dùng

(a) ECB mode;

(b) CBC mode với $IV$ là chữ $X$.

**7.** Giả sử $H$ và $H'$ là các ***hàm băm kháng xung đột***. Hàm băm $H''(x) = H(H'(x))$ có kháng xung đột hay không? Hãy giải thích.

**8.** Xét $H$ là một hàm băm kháng xung đột. Hệ MAC định nghĩa bởi:

Để xác thực thông điệp $m$ với khoá bí mật $k$, ta tính tag $t := H(k\|m)$.

có an toàn không? Nếu không an toàn hãy chỉ ra một cách tấn công; còn nếu có thì hãy chứng minh.

**9.** Máy chủ email BK Mail mã hoá mọi email gửi tới Bob bằng khoá công khai $pk_{\text{bob}}$ 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 $pk_{\text{alice}}$. Để làm điều này, BK Mail cần một cách để **dịch** một email được mã hóa theo khoá công khai $pk_{\text{bob}}$ thành một email được mã hóa theo khoá công khai $pk_{\text{alice}}$ của Alice. Việc này có thể thực hiện dễ dàng nếu BK Mail có $sk_{\text{bob}}$, nhưng vấn đề là, sau đó BK Mail có 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 $E_{\text{sym}}$ là hệ mã khoá đối xứng với không gian khoá $\mathcal{K}_{\text{sym}}$, và $H$ là một hàm băm $H : \mathbb{G} \to \mathcal{K}_{\text{sym}}$.

Giả sử rằng $pk_{\text{bob}}$ và $pk_{\text{alice}}$ 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 $pk_{\text{bob}}$ cho $pk_{\text{alice}}$, Alice và Bob cùng nhau tính $\tau := \alpha/\alpha' \in \mathbb{Z}_q$. Họ gửi $\tau$ tới máy chủ BK Mail.

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

(b) Hãy giải thích cách mà BM Mail dùng $\tau$ 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 $pk_{\text{bob}}$ cho cùng thông điệp $m$.

(c) Liệu máy chủ BK Mail có thể giải mã $c$ hoặc $c'$ khi biết $\tau$ hay không? Nếu có hãy chỉ ra cách giải mã; nếu không hãy chứng minh.