VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY
UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING

Advance Cryptography and Coding Theory (CO3083)

Problem Set 1
Provable Security Foundations

Advisor:
Phan Thanh Tan - 2213076.

HO CHI MINH CITY, SEPTEMBER 2025

Contents

1 Cryptographic Foundations (20 points)

1.1 Basic Concepts (10 points)

1. **Define the three primary security goals of cryptography and provide a real-world example for each.**

   - **Confidentiality:** Ensures that data is accessible only to authorized parties.
     - *Ví dụ:* **Transparent Memory Encryption (TME)** được sử dụng trong các CPU hiện đại (như AMD SEV). Dữ liệu trong bộ nhớ chính (**RAM**) được mã hóa để bảo vệ **trạng thái bí mật** khỏi các cuộc tấn công vật lý hoặc hypervisor độc hại.
   - **Integrity:** Guarantees that data has not been altered, deleted, or tampered with without detection.
     - *Ví dụ:* Sử dụng **Merkle Trees** trong các hệ thống phân tán/blockchain để xác minh hiệu quả tính toàn vẹn của một tập dữ liệu lớn bằng cách chỉ kiểm tra **Root Hash**.
   - **Authenticity:** Verifies the identity or origin of a user or a piece of data.
     - *Ví dụ:* **Digital Signatures** được sử dụng trong **Certificate Transparency Logs** để xác minh tính hợp pháp của các chứng chỉ SSL/TLS do Cơ quan Cấp chứng chỉ (**CA**) phát hành.

2. **Explain Kerckhoff's principle and why it is fundamental.**

   - **Nguyên lý Kerckhoff:** Tính bảo mật của một lược đồ mật mã phải dựa **chỉ** vào **tính ngẫu nhiên và bí mật của khóa K**, và **không** dựa trên sự bí mật của thuật toán Enc đó. Điều này thường được tóm tắt là "Kẻ tấn công biết hệ thống".
   - **Tầm quan trọng Cốt lõi:** Nguyên lý này cho phép **Đánh giá Đồng cấp Công khai** các thuật toán, điều cần thiết để xác định các lỗi tinh vi mà một nhóm kín có thể bỏ sót. Đây là nền tảng của khuôn khổ **Provable Security** (Bảo mật Có thể Chứng minh).
   - **Ví dụ Vi phạm & Hậu quả:**
     - *Vi phạm:* Thuật toán mã hóa **A5/1** ban đầu được sử dụng trong mạng GSM đã được giữ bí mật (**Security by Obscurity**).
     - *Hậu quả:* Khi bị đảo ngược kỹ thuật và tiết lộ, các nhà mật mã học nhanh chóng tìm thấy **các lỗ hổng nghiêm trọng** (ví dụ: tấn công Known-Plaintext hiệu quả), chứng minh rằng sự bí mật đã ngăn cản việc phát hiện và giảm thiểu lỗi sớm.

3. **Compare and contrast symmetric and asymmetric cryptography:**

   (a) **Fundamental difference in key management:**
   - **Mật mã đối xứng:** Sử dụng **một khóa bí mật duy nhất, được chia sẻ** cho cả mã hóa và giải mã. Thách thức chính là **Phân phối Khóa An toàn** giữa tất cả các bên ($\mathcal{O}(N^2)$ khóa cần thiết trong mạng N người dùng).
   - **Mật mã bất đối xứng (Khóa công khai):** Sử dụng **một cặp khóa** ($\mathbf{K_{public}}, \mathbf{K_{private}}$). Thách thức chính là quản lý **Cơ sở hạ tầng Khóa Công khai (PKI)** và **Thu hồi Khóa**.

   (b) **Mathematical/computational assumptions for security:**
   - **Đối xứng (ví dụ: AES, ChaCha20):** Dựa trên giả định rằng mã khối/mã dòng là **Hoán vị Giả Ngẫu nhiên (PRP)** hoặc **Hàm Giả Ngẫu nhiên (PRF)** an toàn. Bảo mật dựa trên **Tính không phân biệt** với một hàm/hoán vị ngẫu nhiên thực sự.
   - **Bất đối xứng (ví dụ: RSA, ECC):** Dựa trên **Giả định về Độ khó Tính toán** liên quan đến lý thuyết số:
     - **RSA**: Độ khó của **Bài toán Phân tích Số nguyên (IFP)**.
     - **ECC**: Độ khó của **Bài toán Logarit Rời rạc trên Đường cong Elliptic (ECDLP)**.

   (c) **Scenario where one is clearly preferable:**
   - **Ưu tiên Đối xứng: Mã hóa một tệp lớn** (ví dụ: video 10 GB). Các thuật toán đối xứng (như AES) nhanh hơn nhiều lần (thường $\sim 1,000\times$) so với các lược đồ bất đối xứng cho mã hóa dữ liệu hàng loạt.

- **Ưu tiên Bất đối xứng: Thiết lập kênh liên lạc an toàn ban đầu** giữa hai bên chưa có bí mật chung từ trước. Các lược đồ bất đối xứng (ví dụ: Diffie-Hellman) cho phép trao đổi khóa an toàn qua một kênh không an toàn.

1.2 Perfect Secrecy (10 points)

1. **One-Time Pad with bitwise AND($\wedge$) operation.**

   (a) **Is this scheme correct?**

   - **Kết luận: KHÔNG đúng**.
   - **Giải thích:** Tính đúng đắn yêu cầu $\text{Dec}(K, \text{Enc}(K, M)) = M$. Thao tác AND, $\text{Enc}(K, M) = K \wedge M$, là **không thể đảo ngược** vì nó gây ra **mất mát thông tin**. Nếu $K_i = 0$ và $M_i = 1$, bản mã C_i sẽ là 0. Khi có $C_i = 0$ và $K_i = 0$, không thể phục hồi duy nhất $M_i = 1$.

   (b) **Does this scheme provide perfect secrecy?**

   - **Kết luận: KHÔNG**.
   - **Chứng minh:** Bảo mật hoàn hảo yêu cầu $\Pr[M|C] = \Pr[M]$. Nếu kẻ thù quan sát $C = 1$ (giả sử $n = 1$ bit), chúng biết $K = 1$ và $M = 1$.

   $$\Pr[M = 0|C = 1] = 0 \neq \Pr[M = 0] = 1/2$$

   Vì bản mã $C = 1$ đã rò rỉ thông tin (nó loại bỏ $M = 0$), bảo mật hoàn hảo bị phá vỡ.

2. **OTP on decimal digits (mod 10).**

   (a) **Prove that this scheme is correct.** Chúng ta phải chứng minh $\text{Dec}(K, \text{Enc}(K, M)) \equiv M \pmod{10}$.

   $$\text{Dec}(K, \text{Enc}(K, M)) \equiv \text{Dec}(K, (K + M) \pmod{10})$$
   $$\text{Dec}(K, \text{Enc}(K, M)) \equiv ((K + M) - K) \pmod{10}$$
   $$\text{Dec}(K, \text{Enc}(K, M)) \equiv M \pmod{10}$$

   Lược đồ là đúng.

   (b) **Prove that this scheme provides perfect secrecy.** Chúng ta phải chứng minh $\Pr[C = c|M = m] = \Pr[C = c]$ với mọi $c, m \in \{0, \ldots, 9\}$.

   $$\Pr[C = c|M = m] = \Pr[K + m \equiv c \pmod{10}] = \Pr[K \equiv c - m \pmod{10}]$$

   Vì K được chọn ngẫu nhiên đồng nhất từ $\{0, \ldots, 9\}$, đối với bất kỳ giá trị cố định nào của $c - m \pmod{10}$, chỉ có chính xác một giá trị của K thỏa mãn phương trình.

   $$\Pr[K \equiv k_0 \pmod{10}] = 1/10$$

   Vì $\Pr[C = c|M = m] = 1/10$, xác suất này độc lập với m. Do đó, lược đồ cung cấp bảo mật hoàn hảo.

3. **OTP with key length half the message length.**

   - **Lược đồ:** $M = (M_1, M_2)$ và $C = (C_1, C_2) = (K \oplus M_1, K \oplus M_2)$.
   - **Tấn công Cụ thể:** **Tấn công Tái sử dụng Khóa (Key Reuse Attack)**.
   - **Thông tin Trích xuất:** Kẻ tấn công quan sát $C = (C_1, C_2)$.

     (a) Kẻ tấn công tính toán:

     $$C_1 \oplus C_2 = (K \oplus M_1) \oplus (K \oplus M_2)$$

     (b) Vì $K \oplus K = \mathbf{0}$, các khóa triệt tiêu lẫn nhau:

     $$C_1 \oplus C_2 = M_1 \oplus M_2$$

   - **Bảo mật bị phá vỡ:** Kẻ tấn công trích xuất được **tổng XOR của hai khối bản rõ** $(M_1 \oplus M_2)$. Đây là một phần thông tin phi tầm thường phá vỡ tính bảo mật, đặc biệt nếu M_1 và M_2 là các văn bản ngôn ngữ tự nhiên.

2 Provable Security (20 points)

2.1 Libraries and Indistinguishability (10 points)

(a) **Are libraries $\mathcal{L}_1$ and $\mathcal{L}_2$ indistinguishable?**

- **Kết luận:** **Có thể phân biệt** (Distinguishable) với xác suất không đáng kể.
- **Chương trình Phân biệt $\mathcal{D}$:**
  i. $\mathcal{D}$ truy vấn oracle với $M_A = \mathbf{0}^n$. Kết quả $C_1 = \text{QUERY}(\mathbf{0}^n)$.
  ii. $\mathcal{D}$ truy vấn oracle với $M_B = C_1$. Kết quả $C_2 = \text{QUERY}(C_1)$.
  iii. $\mathcal{D}$ xuất **1** nếu $C_2 = \mathbf{0}^n$. Ngược lại, xuất **0.
- **Phân tích (Advantage is non-negligible):**
  - **Trong $\mathcal{L}_1$ (OTP):** $C_1 = K \oplus \mathbf{0}^n = K$. Đối với truy vấn thứ hai, $C_2 = K \oplus C_1 = K \oplus K = \mathbf{0}^n$. $\mathcal{D}$ thắng với $\Pr[\mathcal{D} \text{ outputs } 1] = \mathbf{1}$.
  - **Trong $\mathcal{L}_2$ (Modified Random):** R_1, R_2 được chọn ngẫu nhiên. C_1 là giá trị ngẫu nhiên. C_2 cũng sẽ là giá trị ngẫu nhiên, và $\Pr[C_2 = \mathbf{0}^n]$ là **không đáng kể**, $\text{negl}(n) \approx 1/2^n$.
- **Lợi thế (Advantage):** $\text{Adv}(\mathcal{D}) \approx |1 - \text{negl}(n)| \approx \mathbf{1}$, là **không đáng kể**.

(b) **Analyze the indistinguishability of the following pairs of libraries.**

i. **$\mathcal{L}_A$ and $\mathcal{L}_B$:**
- **Kết luận:** **Không thể phân biệt** ($\mathcal{L}_A \equiv \mathcal{L}_B$).
- **Chứng minh:** Trong cả hai thư viện, đầu ra y được chọn **ngẫu nhiên đồng nhất** và được trả về. Biến ngẫu nhiên phụ z trong $\mathcal{L}_B$ được tạo ra nhưng **không được sử dụng** trong đầu ra. Các phân phối đầu ra là giống hệt nhau.

ii. **$\mathcal{L}_C$ and $\mathcal{L}_D$:**
- **Kết luận:** **Có thể phân biệt**.
- **Chiến lược Phân biệt:** Gọi $\text{ENC}(\mathbf{0}^n) \to C$ và sau đó $\text{DEC}(C) \to M'$.
- **Phân tích:** Trong $\mathcal{L}_C$, M' **luôn luôn** bằng $\mathbf{0}^n$. Trong $\mathcal{L}_D$, $\text{DEC}(C)$ trả về một thông điệp ngẫu nhiên độc lập M', vì vậy $\Pr[M' = \mathbf{0}^n] \approx 1/2^n$. $\mathcal{D}$ có thể phân biệt dễ dàng.

2.2 Security Proofs (10 points)

i. **Determine whether Σ' is a secure encryption scheme.**
- **Lược đồ:** $C = (C_1, C_2)$ với $C_1 = K \oplus M$ và $C_2 = K \oplus (M \oplus 1^n)$.
- **Kết luận: KHÔNG an toàn**.
- **Tấn công Cụ thể (Phá vỡ Tính bảo mật):** Kẻ tấn công tính toán **XOR của hai khối bản mã**:
$$C_1 \oplus C_2 = (K \oplus M) \oplus (K \oplus M \oplus 1^n) = \mathbf{1}^n$$
- **Giải thích:** Mối quan hệ $C_1 \oplus C_2 = \mathbf{1}^n$ luôn đúng, tiết lộ một mối quan hệ tuyến tính **độc lập với M và K**. Điều này phá vỡ tính bảo mật (IND-CPA).

ii. **Prove that for the OTP game, $\Pr[b' = b]$ is exactly $1/2$.**

Áp dụng Định lý Bayes để tìm xác suất thông điệp là M_0 (tức là $b = 0$) khi quan sát bản mã $C = c$:
$$\Pr[b = 0 | C = c] = \frac{\Pr[C = c | b = 0] \cdot \Pr[b = 0]}{\Pr[C = c]}$$
- $\Pr[b = 0] = 1/2$ (Sự lựa chọn của Challenger).
- $\Pr[C = c | b = 0] = \Pr[K \oplus M_0 = c] = \Pr[K = c \oplus M_0] = 1/2^n$.
- $\Pr[C = c]$ (Tổng xác suất): $\Pr[C = c] = (1/2^n) \cdot (1/2) + (1/2^n) \cdot (1/2) = 1/2^n$.

Thay thế ngược lại:
$$\Pr[b = 0 | C = c] = \frac{(1/2^n) \cdot (1/2)}{1/2^n} = 1/2$$
Vì $\Pr[b = 0 | C = c] = 1/2$, xác suất kẻ tấn công đoán đúng b là $1/2$. Do đó, $\Pr[b' = b] = 1/2$.

3 Computational Cryptography (30 points)

3.1 Computational Security Concepts (15 points)

A. **Explain why computational security is important, and discuss the limitations of both approaches.**

- **Tầm quan trọng của Bảo mật Tính toán:** Là **cách tiếp cận thực tế duy nhất** cho truyền thông hiện đại, cho phép **khóa ngắn, có thể tái sử dụng** (ví dụ: 128 bit) để mã hóa an toàn các thông điệp dài tùy ý. Nó cũng thiết yếu cho các lược đồ khóa công khai.
- **Hạn chế:**
  - **Lý thuyết Thông tin (Information-Theoretic):** Khóa phải được sử dụng một lần và phải bằng chiều dài thông điệp, điều này là **không khả thi** với dữ liệu lớn.
  - **Tính toán (Computational):** Bảo mật chỉ là **tạm thời**. Nó dựa trên việc kẻ tấn công không có đủ thời gian và tài nguyên. Bảo mật có thể bị phá vỡ nếu sức mạnh tính toán tăng lên (ví dụ: máy tính lượng tử) hoặc một thuật toán hiệu quả hơn được phát hiện.

B. **Brute-force attack on AES-128.**

A. **Estimate the cost to try all possible keys.**

- Số lượng khóa: 2^{128}. Chi phí để tấn công vét cạn 2^{128} khóa là **cực kỳ đắt đỏ** (vượt quá GDP toàn cầu và tài nguyên năng lượng sẵn có) bằng công nghệ tính toán cổ điển.

B. **Discuss whether the computational approach to security makes sense.**

- **Kết luận: CÓ, điều này hoàn toàn hợp lý.**
- **Chứng minh:** Bảo mật tính toán đảm bảo độ phức tạp tấn công (2^{127} phép toán) là **đủ khó** (tức là mất nhiều thời gian hơn tuổi thọ của vũ trụ để thực thi). Nó cung cấp một sự đảm bảo an toàn thực tế và có thể định lượng.

C. **Birthday Paradox and Hash Functions.**

A. **Number of random inputs needed to find a collision.**

- Đối với đầu ra n-bit, số lượng đầu vào k cần thiết để tìm thấy một va chạm với xác suất 50% là xấp xỉ $k \approx \mathbf{2^{n/2}}$.

B. **Bits of output needed for reasonable security.**

- Để đạt mức bảo mật 2^{128} chống lại tấn công Birthday, ta cần $2^{n/2} = 2^{128}$, tức là $n/2 = 128$ hay $n = 256$.
- **Kết luận:** Một hàm băm cần độ dài đầu ra **ít nhất 256 bit** (ví dụ: SHA-256).

3.2 Distinguishability (15 points)

A. **Show that $\mathcal{L}_1$ and $\mathcal{L}_2$ are indistinguishable using the Hybrid Proof technique.**

- **Hybrid $\mathcal{H}_0 = \mathcal{L}_1$:** SAMPLE() : $X \leftarrow \{0,1\}^n, Y := X \oplus 1^n$, return (X, Y).
- **Hybrid $\mathcal{H}_1 = \mathcal{L}_2$:** SAMPLE() : $Y \leftarrow \{0,1\}^n, X := Y \oplus 1^n$, return (X, Y).
- **Kết luận:** $\mathcal{L}_1$ và $\mathcal{L}_2$ là **Hoàn toàn Không Thể Phân biệt** ($\mathcal{L}_1 \equiv \mathcal{L}_2$).
- **Chứng minh Hybrid (Đồng nhất Phân phối):** Chúng ta chứng minh phân phối xác suất của $\mathcal{L}_1$ và $\mathcal{L}_2$ là giống hệt nhau với bất kỳ cặp đầu ra (x, y) nào.
  - **Phân phối của $\mathcal{L}_1$:**

$$\Pr[\mathcal{L}_1 = (x, y)] = \Pr[X = x \wedge Y = y] = \Pr[X = x \wedge x \oplus y = 1^n]$$

Vì X đồng nhất, ta có:

$$\Pr[\mathcal{L}_1 = (x, y)] = \begin{cases} 1/2^n & \text{nếu } x \oplus y = 1^n \\ 0 & \text{ngược lại} \end{cases}$$

– **Phân phối của $\mathcal{L}_2$:**

$$\Pr[\mathcal{L}_2 = (x, y)] = \Pr[Y = y \wedge X = x] = \Pr[Y = y \wedge y \oplus x = 1^n]$$

Vì Y đồng nhất, ta có:

$$\Pr[\mathcal{L}_2 = (x, y)] = \begin{cases} 1/2^n & \text{nếu } x \oplus y = 1^n \\ 0 & \text{ngược lại} \end{cases}$$

Vì các phân phối là giống hệt nhau, $\mathcal{L}_1 \equiv \mathcal{L}_2$.

B. **Analyze the encryption protocol $\mathcal{L}_{\text{real}}$ and $\mathcal{L}_{\text{ideal}}$.**

A. **Construct a distinguisher $\mathcal{D}$.**

- **Chiến lược:** Khai thác thực tế là khóa tĩnh K được giữ lại trong tổng XOR của các thành phần bản mã trong $\mathcal{L}_{\text{real}}$.
- $\mathcal{D}$ truy vấn ENCRYPT$(\mathbf{0}^n) \to (C_{1,A}, C_{2,A})$.
- $\mathcal{D}$ truy vấn ENCRYPT$(\mathbf{0}^n) \to (C_{1,B}, C_{2,B})$.
- $\mathcal{D}$ xuất **1** nếu $C_{1,A} \oplus C_{2,A} = C_{1,B} \oplus C_{2,B}$.
- **Phân tích:** Trong $\mathcal{L}_{\text{real}}$, $C_1 \oplus C_2 = K$. Vì K là tĩnh, điều kiện $K = K$ **luôn đúng** (Pr $= 1$). Trong $\mathcal{L}_{\text{ideal}}$, các thành phần bản mã là ngẫu nhiên độc lập, vì vậy điều kiện chỉ đúng với xác suất không đáng kể ($\approx 1/2^n$). Các thư viện có thể phân biệt được.

B. **Propose a minimal modification to make $\mathcal{L}_{\text{real}}$ secure.**

- **Chỉnh sửa:** Sử dụng một **PRF** để tạo ra một luồng khóa duy nhất cho mỗi thông điệp dựa trên nonce R.
- **Lược đồ Đã Chỉnh sửa (sử dụng PRF):**

$$\text{ENCRYPT}(M):$$

$$R \leftarrow \{0,1\}^n \quad \text{(Nonce duy nhất)}$$

$$\mathbf{S} := \mathbf{PRF}(K, R) \quad \text{(Luồng Khóa Giả Ngẫu nhiên)}$$

$$C_1 := R$$

$$C_2 := \mathbf{S} \oplus M$$

$$\text{return } (C_1, C_2)$$

- **Chứng minh:** Vì PRF(K, R) là không thể phân biệt về mặt tính toán với một luồng khóa ngẫu nhiên thực sự cho mỗi thông điệp (do R là duy nhất), lược đồ này đạt được bảo mật IND-CPA bằng cách loại bỏ đường tấn công tuyến tính K.

4 Application of Cryptographic Principles (30 points)

A. **One-Time Pad in the Real World**

- **Vấn đề 1: Supply Chain Security (Key Integrity).**
  - *Rủi ro:* Ổ USB 1TB dễ bị **can thiệp vật lý** hoặc **thay thế** trong quá trình vận chuyển. Kẻ tấn công có thể thay thế pad ngẫu nhiên bằng một **Pad Đã Biết** hoặc **pad bị sai lệch**, làm tổn hại đến tính bảo mật trước khi sử dụng.
  - *Cải tiến:* Sử dụng **Hardware Security Module (HSM)** cho quản lý khóa và áp dụng **MAC Lý thuyết Thông tin** cho pad (nếu có thể) hoặc sử dụng **Key Exchange (PQC KEM) Hậu Lượng tử** an toàn để thiết lập vật liệu khóa qua kênh mạng.
- **Vấn đề 2: Synchronization and Key Reuse.**
  - *Rủi ro:* Cơ chế "đánh dấu đã sử dụng" phải được **đồng bộ hóa hoàn hảo**. Nếu đồng bộ hóa thất bại hoặc một thông điệp được gửi lại, pad sẽ bị **tái sử dụng**, dẫn đến tấn công tử huyệt $M_1 \oplus M_2$, phá vỡ tính bảo mật.
  - *Cải tiến:* **Quản lý nghiêm ngặt các chỉ mục sử dụng**. Mỗi thông điệp phải bao gồm một **Pad Index/Nonce** duy nhất, và người nhận phải kiểm tra tính duy nhất của chỉ mục. Toàn bộ gói (Index + Ciphertext) phải được bảo vệ bằng một **MAC Lý thuyết Thông tin**.
- **Vấn đề 3: Usability and Availability.**
  - *Rủi ro:* Yêu cầu phân phối USB vật lý và "yêu cầu ổ đĩa mới" khi sử dụng đến 80% là một **rào cản lớn về khả năng sử dụng**, dẫn đến **thời gian chết**. Điều này khuyến khích người dùng vi phạm các quy tắc (ví dụ: sao chép pad bất hợp pháp).
  - *Cải tiến:* Áp dụng một lược đồ **Mật mã Tính toán** an toàn (ví dụ: **AES − 256 − GCM**) thay vì OTP cho dữ liệu hàng loạt.

B. **Symmetric Encryption Protocol Analysis**

A. **Analyze the claimed confidentiality properties.**

- **Kết luận: KHÔNG** cung cấp Perfect Secrecy hoặc IND-CPA đã tuyên bố.
- **Chứng minh:** Khóa K là **khóa tĩnh** được **tái sử dụng** cho mọi thông điệp ($C = K \oplus M$). Điều này cho phép kẻ tấn công phục hồi $M_1 \oplus M_2$ từ $C_1 \oplus C_2$, phá vỡ tính bảo mật.

B. **Identify at least three major security vulnerabilities.**

- **Lỗ hổng 1: Tái sử dụng Khóa** (Lỗi chí mạng).
- **Lỗ hổng 2: Thiếu Tính toàn vẹn/Xác thực**: Dễ bị **Tấn công Malleability/Bit-Flipping** vì không có MAC để xác minh tính xác thực của thông điệp.
- **Lỗ hổng 3: Phân phối Khóa Tập trung là Điểm lỗi Duy nhất**: Toàn bộ bảo mật khóa dựa vào "kênh bí mật tuyệt đối do máy chủ công ty thiết lập". Sự thỏa hiệp của máy chủ sẽ làm thỏa hiệp khóa của tất cả người dùng.

C. **Explain whether generating new keys daily would address the vulnerabilities.**

- **Kết luận: KHÔNG, nó không đủ.**
- **Giải thích:** Thay đổi khóa hàng ngày chỉ giới hạn **phạm vi** của tấn công Tái sử dụng Khóa trong một ngày; $M_1 \oplus M_2$ vẫn có thể được phục hồi cho các thông điệp gửi trong cùng một ngày. Nó **không giải quyết** được các lỗ hổng Thiếu Tính toàn vẹn hoặc Lỗi Tập trung.

D. **Propose a modified protocol that would significantly improve security.**

- **Lược đồ Đề xuất:** Sử dụng **AES − 256 − GCM** (Authenticated Encryption with Associated Data - AEAD).
- **Chứng minh (Nguyên tắc Bảo mật):**

A. **Tính bảo mật (IND-CPA):** GCM sử dụng một **Nonce** (IV) duy nhất để đảm bảo luồng khóa cho mỗi thông điệp là duy nhất, ngăn chặn các cuộc tấn công tái sử dụng khóa.

B. **Tính toàn vẹn và Xác thực:** GCM là chế độ AEAD, tạo ra một **Thẻ Xác thực** để ngăn chặn **Tấn công Malleability/Bit-Flipping**.

Bonus Challenge (20 extra points)

The Discrete Logarithm Problem (DLP) and its Impact.

A. **Select one modern cryptographic protocol that relies on the hardness of DLP:** **Diffie-Hellman Key Exchange (DH Key Exchange)**.

B. **The specific impact on the protocol's security.**
- **Tác động:** Giao thức **bị phá vỡ hoàn toàn**. Kẻ tấn công (Eve) quan sát các giá trị công khai $A = g^a$ và $B = g^b$ có thể sử dụng bộ giải DLP hiệu quả để tìm ra các số mũ riêng tư a và b.
- **Kết quả:** Eve tính toán bí mật chung $K = g^{ab}$, làm tổn hại hoàn toàn quá trình **thiết lập khóa**.

C. **How the protocol would need to be modified to remain secure.**
- **Chỉnh sửa:** Giao thức phải được **thay thế** bằng một **Cơ chế Đóng gói Khóa (KEM) Mật mã Hậu Lượng tử (PQC)**.
- **Ví dụ:** Sử dụng Kyber (một KEM dựa trên lattice) để đóng gói và trao đổi khóa phiên đối xứng một cách an toàn.

D. **Whether any alternative mathematical problems could serve as suitable replacements.**
- **Thay thế Phù hợp: Bài toán Học với Lỗi (LWE)** (Learning With Errors), là nền tảng của mật mã dựa trên lattice (Kyber) và được coi là **kháng lượng tử**.