**INTRODUCTION**

*1. Khái niệm:* Cryptography là bộ môn khoa học cho phép tính toán, giao tiếp, xác minh và ủy quyền an toàn và riêng tư trong sự hiện diện của cá bên không đáng tin cậy, có hành vi thù địch và những người tham gia không tin tưởng lẫn nhau.

*2. Các hoạt động mã hóa đang diễn ra bây giờ:*

- Kết nối Wifi (WPA3)

- Kết nối di động (5G AES)

- Thông báo ứng dụng (TLS)

- Nhận diện khuôn mặt (Secure enclave – bộ xử lý riêng của iPhone để xử lý thông tin sinh trắc học của người dùng)

- Làm mới ứng dụng nền

*3. Mục tiêu của bảo mật:*

- Tính bảo mật (Confidentiality)

- Tính xác thực(Authentication)

- Tính toàn vẹn (Integrity)

*4. Điều kì diệu của mật mã học:*

- Bảo mật giao tiếp thông qua một kênh không an toàn.

- Chứng minh thông tin đó là đúng mà không cần phải tiết lộ chúng.

- Chứng minh được tính toán mà không cần làm lại.

*5. Các vấn đề khó trong mật mã học:*

- Nguyên thủy không đối xứng:

+ Vì có một “khóa công khai” và “khóa riêng tư” cho mỗi tổ chức. Đại số, giả sử rằng độ khó của các bài toán (như vừa thấy vừa rồi)

**\* RSA:** [**RSA (mã hóa) – Wikipedia tiếng Việt**](https://vi.wikipedia.org/wiki/RSA_(m%C3%A3_h%C3%B3a))

- Nguyên thủy đối xứng:

+ Vì không có “khóa bí mật”. Không phải đại số nhưng không có cấu trúc, nhưng về khả năng chống chịu được hiểu của họ đối với n nhiều năm phân tích mật mã.

**\* AES (Advanced Encryption Standard):** [Advanced Encryption Standard – Wikipedia tiếng Việt](https://vi.wikipedia.org/wiki/Advanced_Encryption_Standard)

**\* SHA-2:** [**SHA-2 - Wikipedia**](https://en.wikipedia.org/wiki/SHA-2)