Chương 2 **Kỹ thuật mã hóa cổ điển**

Tìm hiểu về: **mã hóa đối xứng**, **kỹ thuật thay thế**, **kỹ thuật chuyển vị**, **Steganography**(loại này là chèn thông điệp vào bức thư, hình ảnh, chèn vào những thứ quen thuộc mà không ai ngờ tới).

Có 2 yêu cầu cho việc bảo mật mã hóa:

Cần 1 giải thuật mã hóa hóa mạnh.

Người gửi và người nhận phải trao đổi khóa 1 cách an toàn và phải giữ bí mật khóa. Nếu 1 người khám phá ra khóa và biết giải thuật, tất cả giao tiếp sẽ bị phá vỡ.

Phân loại:

Theo tổ chức mã hóa: thay thế và chuyển vị, kết hợp.

Theo khóa: 1, 2.

Theo xử lý plaintext:block(khối), stream(bit).

Tân công Crytanalysis(phân tích mã hóa) và Brute-force(Quét cạn):

Crytanalysis: Tấn công dựa vào tính chất của thuật toán cộng với một số kiến thức về các đặc điểm chung của các bản rõ. Tấn công khai thác các đặc điểm của thuật toán để cố gắng để suy luận một bản rõ cụ thể hoặc để suy ra khóa được sử dụng.( dựa vào điểm yếu của thuật toán)

Brute-force: Kẻ tấn công cố gắng mỗi khóa có thể trên một phần của ciphertext cho đến khi thu được 1 plaintext. Tính trung bình, một nửa trong số tất cả các khóa có thể phải cố gắng để đạt được thành công.( dựa vào điểm yếu của khóa).

Kỹ thuật thay thế:

Là một trong đó các chữ cái của plaintext được thay thế bằng chữ cái khác hoặc bằng các con số hoặc ký hiệu

Plaintext được xem như là một chuỗi các bit, sau đó thay thế bao gồm việc thay thế các mẫu bit plaintext với các mẫu ciphertext bit.

Kỹ thuật chuyển vị:

Một loại rất khác nhau của bản đồ là đạt được bằng cách thực hiện một số loại hoán vị trên các chữ cái trên plaintext.

**Rail Fence:**

For example, to encipher the message “meet me after the toga party” with rail fence of depth 2, we write the following(chuyển vị)

m e m a t r h t g p r y

e t e f e t e o a a t

 The encrypted message is:

MEMATRHTGPRYETEFETEOAAT

**Caesar Cipher(thay thế):**

plain: meet me after the toga party .

cipher: PHHW PH DIWHU WKH WRJD SDUWB .

**Monoalphabetic Ciphers:**

Dễ phá vì ảnh hưởng tần suất xuất hiện của chữ cái.

**Playfair Ciphers:**

Dựa vào matrix 5x5.

**Vigenère Cipher:**

Ma trận bảng chữ cái.

**Steganography:**

Một thay thế cho mã hóa.

Giấu sự tồn tại của tin:

sử dụng mực vô hình, trốn trong LSB trong hình ảnh đồ họa hoặc file âm thanh, ẩn trong "tiếng ồn" .