K1 = K2: Mã hóa đối xứng

K1 <> K2: mã hóa bất đối xứng

Hack mũ trắng version 13: có sử dụng AI, có đề cập “How to attack AI system”

Các loại mã hóa

1. Phương thức mã hóa  
   a. thay thế

b. đổi vị trí

c.kết hợp

1. Số lượng khóa  
   a. một khóa (mã hóa đối xứng)

b.hai khóa

c.không có khóa (Hash function: công cụ md5sum -> hash string -> kiểm tra xem có sự thay đổi của hacker?)

1. Cách xử lý dữ liệu  
   a.mã hóa khối (mã hóa 1 khối = mã hóa dòng)

b.mã hóa dòng

Caesar cipher

Ci = (Pi + K) mod 26

i thuộc [0, n), n = chiều dài Plaintext

Vigenere cipher bản chất là caesar cipher : mỗi ký tự mã hóa với 1 khóa K khác. (có nhiều khóa K)

Ci = (Pi + Kj) mod 26

i thuộc [0, n), n = chiều dài Plaintext

j thuộc [0, m), m = chiều dài Key

j = i mod m

Playfair cipher: ma trận 5x5

Cùng cột -> kề dưới

Cùng dòng -> kề phải

Khác dòng, khác cột -> kí tự đối diện ở góc khi tạo thành hình vuông