1. Giải thuật:
   1. Mô tả:

Từ ma trận suy ra được vị trí theo hàng và cột của mỗi ký tự ở plaintext sau đó ghi thành 2 hàng (1 hàng ghi vị trí hàng, 1 hàng ghi vị trí cột của các ký tự). Chia 2 hàng này thành các cặp ký tự số (nếu có ký tự lẻ cuối cùng ở hàng thứ nhất thì nó sẽ được ghép với ký tự đầu tiên của hàng 2). Sau đó chuyển từng cặp ký tự số này thành chữ cái dựa trên ma trận (với ký tự số đầu tiên của cặp tương ứng với hàng còn ký tự sau tương ứng với cột), ta được chuỗi mã hóa.

1. Tổng hợp các giải thuật mã hóa đã học:

|  |  |
| --- | --- |
| **Tên** | **Đặc điểm** |
| Mã thay thế đơn giản | * Sử dụng hoán vị * Biểu diễn chuỗi 26 ký tự |
| Mã thay thế n gram | * Thay thế các ký tự * Khóa là một hoán vị 26n n-gram khác nhau |
| Mã hoán vị bật d | * Lấy hoán vị áp dụng vào khối |
| Vigenère | * Khóa bao gồm chuỗi d ký tự * Được cộng modulo 26 * Các ký tự trắng giữ nguyên không cộng |
| Caesar | * Giống vigenère * d = 1 |
| One-time pad | * Sử dụng phép xor * Gồm plaintext và key |
| Mã hóa affine cipher | * Là mã thay thế * Dạng ax + b (mod 26) * Với a = 1 ta có mã dịch chuyển |
| Playfair | * Mã đa ký tự * Dựa trên ma trận xây dựng từ một khóa * Các ký tự trong ma trận khóa không trùng nhau |
| Mã Hill | * Sử dụng m ký tự liên tiếp nhau của plaintext * Thay thế m ký tự với phương trình tuyến tính * Chọn ma trận Hill làm khóa |
| DES | * Khóa có độ dài 56 bit, dữ liệu 64 bit * Là mã hóa khóa bất đối xứng * Dùng chung một khóa để giải mã hay mã hóa |
| AES | * Mã hóa khóa đối xứng * Lặp lại nhiều lần các bước xử lý * Kích thước input = 128 bit * Kích thước khóa = 128/192/256 bit * Một khóa con là một cột gồm 4 bytes * Ma trận đầu vào là ma trận trạng thái * Ma trận trạng thái sẽ biến đổi trong quá trình mã hóa. * Gồm 4 hàm |
| RSA | * Có 2 khóa: bí mật và công khai * Khóa sử dụng cố định trong quá trình giải mã và mã hóa * Khóa công khai được công bố rộng rãi để giải mã |