1. **Giải thuật:**

**Mô tả:**

***Lập bảng ma trận 5x5***

Ma trận được lập dựa trên key là “keyword”, sau đó đưa từng kí tự và lập nên bảng ma trận giống với thuật toán mã hoá Playfair. Điểm đặc biệt là các con số ở trên thứ tự hàng và cột sẽ được đặt ngẫu nhiên không theo thứ tự.

***Lập bảng chuyển từ plaintext sang Rows và Columns***

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 tính từ trái sang phải bắt đầu từ hàng Rows sau đó đến hàng Columns (nếu có ký tự lẻ cuối cùng ở hàng thứ nhất thì nó sẽ được ghép với ký tự đầu tiên của hàng thứ hai để thành một cặp).

***Dò để tìm ra Ciphertext***

Sau đó dò để chuyển từng cặp ký tự số này thành chữ cái dựa trên ma trận đã lập (với ký tự số đầu tiên của cặp tương ứng với vị trí hàng còn ký tự sau tương ứng với vị trí cột), ta được chuỗi Ciphertext.

**Thực hiện lại giải thuật**

Lập ma trận khoá khác với key là TSHCUI

|  |  |
| --- | --- |
|  | **2 3 1 5 4** |
| **1**  **3**  **4**  **2**  **5** | T S H C U  I A B D E  F G K L M  N O P Q R  V W X Y Z |

Lấy Plaintext là **tang dung cam**

Từ đó ta có được bảng chuyển đổi

|  |  |
| --- | --- |
| **Plaintext:** | **tang dung cam** |
| **Rows:**  **Columns:** | 1324 3124 134  2323 5423 534 |

Dựa vào giải thuật ta sẽ ra được Ciphertext là: **SRBR SFID FDE**

1. **Bảng tổng hợp:**

|  |  |  |
| --- | --- | --- |
| **Tên** | **Đặc điểm** | **Độ an toàn** |
| 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 | - Độ an toàn của DSA phụ thuộc vào kích thước khóa và các tham số cụ thể.  - Các khóa DSA hiện đại thường có kích thước từ 2048 bit trở lên. DSA an toàn nếu được triển khai đúng cách và sử dụng với các tham số an toàn. |
| 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 (AES-128, AES-192, AES-256) * Một khóa con là một cột gồm 4 bytes (128 bit) * Ma trận đầu vào là ma trận trạng thái * Ma trận trạng thái này sẽ biến đổi trong quá trình mã hóa. | - AES được coi là một trong những thuật toán mã hóa mạnh nhất hiện nay.  - Các kích thước khóa thông dụng là 128, 192, và 256 bit. AES-256 được xem là cực kỳ an toàn và khó bị tấn công trong thời điểm hiện tại. |
| 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 cho mọi ngươif và được dùng để mã hoá. Những thông tin được mã hoá bằng khoá công khai chỉ có thể được giải mã bằng khoá bí mật tương ứng | - Độ an toàn của RSA phụ thuộc vào kích thước khóa.  - Khóa RSA thông dụng hiện nay thường có kích thước từ 2048 đến 4096 bit.  - RSA an toàn nếu được sử dụng với kích thước khóa đủ lớn và các tham số an toàn. |