**Nhóm HKT**

Mô tả thuật toán mã hóa Vigenere và thuật toán mã hóa RSA

|  |  |
| --- | --- |
| Danh sách thành viên | Nội dung công việc |
| 44.01.104.188 - Lâm Phát Tài | Tìm hiểu và cài đặt demo |
| 44.01.104.196 - Nguyễn Xuân Tính | Tìm hiểu và cài đặt demo |
| 44.01.104.112 - Lâm Hoàng Khánh | Tìm hiểu và cài đặt demo |
| 44.01.104.200 - Bùi Chí Tùng | Tìm hiểu thuật toán và mô tả word |
| 44.01.104.081 - Võ Tuấn Hào | Tìm hiểu thuật toán |

# **Thuật toán Vigenere**

Mật mã Vigenère là tập hợp các quy tắc thay thế chữ cái đơn trong bảng chữ cái tiếng Anh qua việc sử dụng 26 mật mã Caesar với các bước dịch chuyển từ 0 đến 25 tương ứng từ chữ ‘a’ đến chữ ‘z’. Cụ thể, bản mã Vigenère được lập theo công thức sau:

ci = (pi + ki) mod 26, i=1,…,l

trong đó, C = {c1…cl} là bản mã, P={p1…pl} là bản gốc, K = {k1…kl} là dãy khóa và l là độ dài bản rõ. Tương tự, bản gốc P có thể được tính nếu biết khóa và bản mã theo công thức:

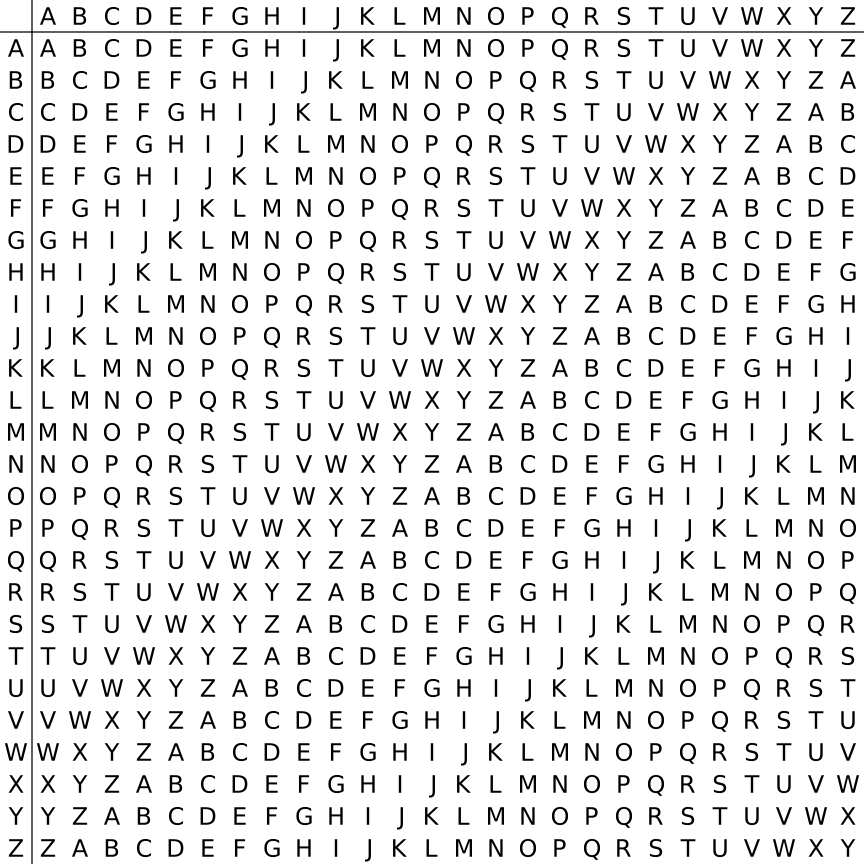
pj = (cj – kj) mod 26, j = 1,…,l

Mật mã Vigenère không thể phá vỡ trong trường hợp sử dụng các khóa đủ dài. Nhưng với các khóa ngắn hoặc nếu nhà thám mã có nhiều bản mã so với độ dài khóa thì khá dễ để phá vỡ. Việc thám mật mã Vigenère thường tiến hành theo hai bước là: xác định độ dài chu kỳ của khóa trước, sau đó tìm khóa cụ thể.

Việc mã hóa Vigenere được thực hiện với 2 bước:

Bước 1: Trước hết ta sẽ nhân chuỗi khóa lên để nó có cùng độ dài với chuỗi cần mã hóa

Bước 2: Bắt đầu từ trái qua phải, lấy ký tự của key làm dòng, ký tự của chuỗi cần mã hóa là cột và dóng vào trong bảng mã(hình trên) ta được một ký tự, ký tự đó chính là ký tự đã được mã hóa.



Ví dụ với từ plain text: BAOMATANNINHMANG và key: HKT

B1: Trước hết ta sẽ nhân chuỗi HKT này lên để nó có cùng độ dài với chuỗi cần mã hóa:

BAOMATANNINHMANG

HKTHKTHKTHKTHKTH

B2: Đối chiếu với bảng từ đó ta có được chuỗi đã được mã hóa như sau: IKHTKMHXGPXATKGN

# **Thuật toán mã hóa RSA**

RSA là một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa

Quá trình hoạt động của thuật toán:

1. **Sinh khóa**

Sinh khóa làm nhiệm vụ tìm kiếm được 1 bộ phận có 3 số tự nhiên e, d, n cần thỏa mãn công thức sau đây:

Med trùng m mod n

Trong đó, giá trị d cần phải được bảo mật 1 cách tuyệt đối để khi có biết các giá trị khác là n, e hay m thì cũng không có cách nào để tìm được giá trị của d. Với công thức này, khóa RSA sẽ có cơ chế sinh hóa theo quy trình:

* Chọn ra 2 số nguyên tố là p và q.
* Tính phương trình: n=pq. Giá trị của n đóng vai trò modulus ở cả 2 loại private key và public key.
* Có một vài giả nguyên tố dựa trên Carmichael sẽ được tính toán và giữ bí mật.
* Chọn lấy 1 số e ở khoảng 1 và giữ nguyên tố n sao cho ước chung lớn nhất của 2 số này có giá trị bằng 1. Nghĩa là, giá trị e và giả nguyên tố n có cùng nguyên tố với nhau.
* Giá trị của d trùng với 1/e, viết theo 1 cách khác là de trùng 1. Số tự nhiên d lúc này chính là nghịch đảo của modulo của e theo công thức modulo mod λ(n).

Lúc này, Public Key được tìm ra chính là bộ số (n,e) còn và private key bộ số (n,d). Nhiệm vụ của bạn là cần phải giữ cẩn thận private key và số nguyên tố p,d từ đó việc tính toàn các khóa sẽ trở nên một cách dễ dàng.

1. **Mã hóa và giải mã**

Nếu có M thì chuyển nó sang thành số tự nhiên m ở khoảng (0, n) và có thể đảm bảo giá trị m và n có cùng nguyên tố. Bạn hãy thêm kỹ thuật padding vào, sau đó có thể tiến hành mã hóa m để chuyển m thành c. Bạn có thể áp dụng theo công thức sau:

c ≡ me mod n

c sẽ được chuyển tới người nhận. Người nhận lúc này sẽ có nhiệm vụ là giải mã c để có thể lấy được giá trị của m bằng công thức sau:

cd ≡ mde ≡ m mod n

Sau đó, lấy giá trị m, bạn đảo ngược padding lại nhé thì sẽ lấy được thông tin gốc