**Kế Hoạch Thực Hiện Dự Án**

**Nhóm:Tú Anh,Tuấn Đạt, Đức Anh**

Đề tài: Viết chương trình mã hóa và giải mã thông tin truyền qua mạng bằng thuật toán RSA.

Nội dung trình bày;

I.Tổng quan về thuật toán RSA

RSA là một thuật toán mã hóa đối xứng được phát triển bởi Ronald Rivest, Adi Shamir và Leonard Adleman vào năm 1977. RSA là viết tắt của tên ba người phát minh thuật toán này.

Thuật toán RSA dựa trên việc tìm các số nguyên tố lớn và tính toán các phép tích và lũy thừa trên các số đó. Thuật toán RSA là một trong những thuật toán mã hóa đối xứng phổ biến nhất hiện nay. Nó được sử dụng trong nhiều ứng dụng, bao gồm bảo mật thông tin trong các hệ thống điện toán đám mây, chữ ký số, mã hóa truyền thông và các ứng dụng bảo mật khác.

1.1 cơ chế hoạt động

1. Tìm hai số nguyên tố lớn p và q.

2. Tính n = p \* q và ϕ(n) = (p-1) \* (q-1).

3. Chọn một số e thỏa mãn 1 < e < ϕ(n) và e và ϕ(n) là hai số nguyên tố cùng nhau.

4. Tính d sao cho e\*d ≡ 1 (mod ϕ(n)).

5. Khóa công khai là cặp số (n, e), khóa bí mật là cặp số (n, d).

6. Để mã hóa một thông điệp m, tính c = m^e (mod n).

7. Để giải mã một thông điệp đã được mã hóa c, tính m = c^d (mod n).

II.các bước thực hiện

Mã hóa và giải mã thông tin truyền qua mạng là quá trình chuyển đổi thông tin từ dạng thông thường sang dạng không đọc được (mã hóa), và sau đó chuyển truyền thông tin đã mã hóa đó từ nguồn đến đích, rồi chuyển đổi thông tin từ dạng không đọc được sang dạng thông thường (giải mã) để đọc được thông tin gốc.

Một cách thường được sử dụng để mã hóa thông tin truyền qua mạng là sử dụng một cặp khóa công khai và khóa bí mật. Thuật toán RSA là một ví dụ của phương pháp này.

Khi A muốn gửi thông tin cho B, A sẽ sử dụng khóa công khai của B để mã hóa thông tin của mình trước khi gửi đi. B sẽ sử dụng khóa bí mật của mình để giải mã thông tin khi nhận được.

Quá trình này được thực hiện bằng cách sử dụng một thuật toán mã hóa và giải mã đối xứng, tức là cùng một khóa được sử dụng để mã hóa và giải mã thông tin. Khi sử dụng thuật toán RSA, cặp khóa công khai và khóa bí mật không giống nhau, và quá trình mã hóa và giải mã không sử dụng cùng một khóa.

Quá trình mã hóa và giải mã thông tin truyền qua mạng bằng RSA có thể được mô tả như sau:

1. Khởi tạo cặp khóa công khai và khóa bí mật: B tạo ra một cặp khóa công khai và khóa bí mật, lưu khóa công khai và giữ khóa bí mật cho mình.

2. Mã hóa thông tin: A sử dụng khóa công khai của B để mã hóa thông tin mà cô muốn gửi đi.

3. Gửi thông tin đã mã hóa: A gửi thông tin đã mã hóa cho B.

4. Giải mã thông tin: B sử dụng khóa bí mật của mình để giải mã thông tin.

Trong quá trình này, thông tin đã mã hóa được truyền qua mạng và chỉ có thể được giải mã bởi B, người duy nhất có khóa bí mật phù hợp với khóa công khai đã được sử dụng để mã hóa thông tin.

III. Lợi ích

Bảo mật thông tin: Việc sử dụng mã hóa và giải mã thông tin truyền qua mạng giúp đảm bảo tính bảo mật của thông tin, tránh được các cuộc tấn công mạng như giả mạo, tấn công trung gian, đánh cắp thông tin... Nó giúp người dùng yên tâm và tin tưởng khi sử dụng các dịch vụ trực tuyến.

Bảo vệ quyền riêng tư: Mã hóa thông tin trước khi truyền qua mạng giúp bảo vệ quyền riêng tư của người dùng, tránh được việc bị giám sát hoặc theo dõi thông tin truyền qua mạng.

Đảm bảo tính toàn vẹn của thông tin: Mã hóa thông tin cũng giúp đảm bảo tính toàn vẹn của thông tin, tránh được việc thông tin bị sửa đổi hoặc thay đổi trên đường truyền.

Bảo vệ truyền tải tài liệu nhạy cảm: Mã hóa thông tin cũng giúp bảo vệ truyền tải các tài liệu nhạy cảm, tránh được việc các tài liệu này bị lộ ra bên ngoài hoặc bị truy cập trái phép.

Bảo vệ các giao dịch tài chính: Việc sử dụng mã hóa và giải mã thông tin truyền qua mạng cũng giúp bảo vệ các giao dịch tài chính trực tuyến, đảm bảo rằng các thông tin nhạy cảm như số thẻ tín dụng, số tài khoản ngân hàng... được bảo vệ khỏi các cuộc tấn công mạng.