## ĐẠI HỌC QUỐC GIA TP.HCM TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

**KHOA CÔNG NGHỆ THÔNG TIN**

**-------------------------------------**

BÁO CÁO ĐỒ ÁN

**BỘ MÔN: NHẬP MÔN MÃ HÓA MẬT MÃ**

# ĐỒ ÁN 1

**Thành viên:**

* CHÂU LÝ PHƯƠNG TRINH – 19120694
* TRƯƠNG THỤY KHÁNH THỊNH – 19120670
* TÔN THẤT TIẾN – 19120681
* NGUYỄN QUỐC TUẤN – 19120702
* TRẦN VIẾT TUẤN - 19120705

# TP.HCM 01/2022

**MỤC LỤC**

1. **Thông tin nhóm, công việc của từng thành viên và đánh giá**
2. **Thông tin nhóm**

Các thành viên trong nhóm

* Châu Lý Phương Trinh - 19120694
* Trương Thụy Khánh Thịnh - 19120670
* Tôn Thất Tiến - 19120681
* Nguyễn Quốc Tuấn - 19120702
* Trần Viết Tuấn - 19120705

1. **Bảng phân chia công việc**

| Thành viên | Phân chia công việc |
| --- | --- |
| Châu Lý Phương Trinh |  |
| Trương Thụy Khánh Thịnh |  |
| Tôn Thất Tiến |  |
| Nguyễn Quốc Tuấn |  |
| Trần Viết Tuấn |  |

1. **Đánh giá tổng quan toàn bộ project**

| Đã hoàn thành | Mức độ hoàn thành |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

1. **Protocol được sử dụng trong đồ án**
2. **Tổng quan**

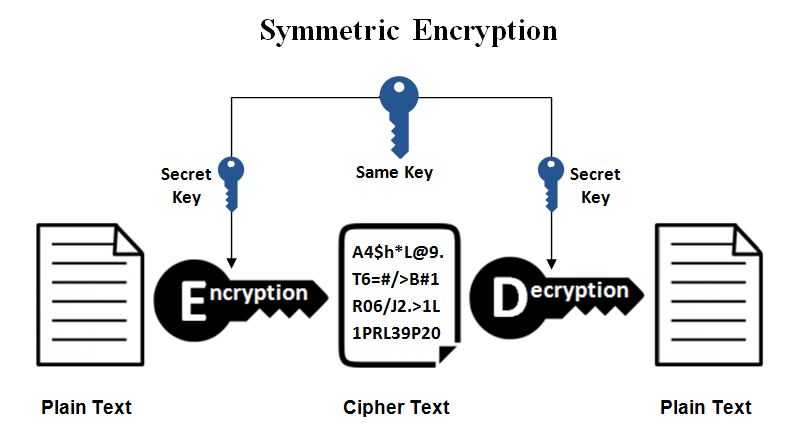
Với sự phát triển của công nghệ thông tin, môi trường của chúng ta được bao quanh bởi dữ liệu kỹ thuật số. Khi dữ liệu trở nên quan trọng, chúng dễ bị tấn công từ bên ngoài. Điều này có thể tránh được bằng cách sử dụng mã hóa mật mã cung cấp tính bảo mật, tính toàn vẹn và tính sẵn sàng. Ở khuôn khổ đồ án này, chúng em xây dựng một hệ thống lưu trữ file an toàn ở mức độ sơ khai.

Mã hóa file là một cách để dễ dàng bảo vệ sự an toàn của dữ liệu cá nhân hoặc tổ chức. Các thuật toán mã hóa đại diện như mã bất đối xứng RSA và mã đối xứng AES không có khả năng đáp ứng các tiêu chí về độ tin cậy và bảo mật của mã hóa file khi được sử dụng riêng lẻ. Để giải quyết vấn đề này, ta kết hợp cả hai thuật toán trên. Trong khi AES là một thuật toán mã hóa có ưu điểm về mặt tốc độ thì RSA là thuật toán mã hóa có độ an toàn cao. Thực tế cho thấy RSA và AES không chỉ mã hóa các tệp mà còn cung cấp các lợi ích về tính hiệu quả và khả năng bảo vệ của thuật toán.

1. **Giao thức mật mã**

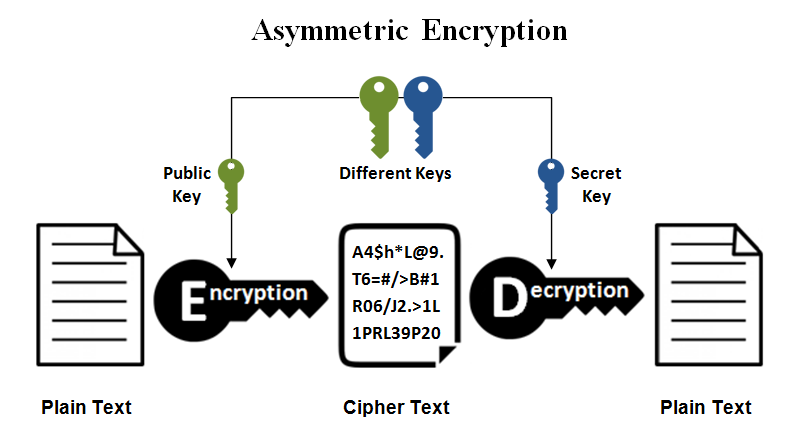
Trong hệ thống an ninh mạng, mật mã đóng một vai trò quan trọng để truyền thông tin an toàn. Có hai các loại thuật toán mật mã: đối xứng và không đối xứng.

Trong mật mã đối xứng, thể hiện ở Hình 1, một khóa bí mật được sử dụng cho cả mã hóa và giải mã. Vấn đề với phương pháp này là bạn phải thông báo khóa bí mật một cách an toàn cho người nhận dự định. Thuật toán đối xứng nhanh chóng và đơn giản để thực hiện vì chúng sử dụng kích thước khóa nhỏ.



Hình 1. Mã hóa đối xứng

Mật mã không đối xứng, được hiển thị trên Hình 2, sử dụng một cặp khóa: một khóa công khai để mã hóa thông điệp tại người gửi và một khóa riêng tư chỉ người nhận mới biết để giải mã thông điệp đã mã hóa. Các thuật toán bất đối xứng an toàn hơn nhưng yêu cầu một lượng lớn phép tính vì chúng sử dụng kích thước khóa lớn để mã hóa



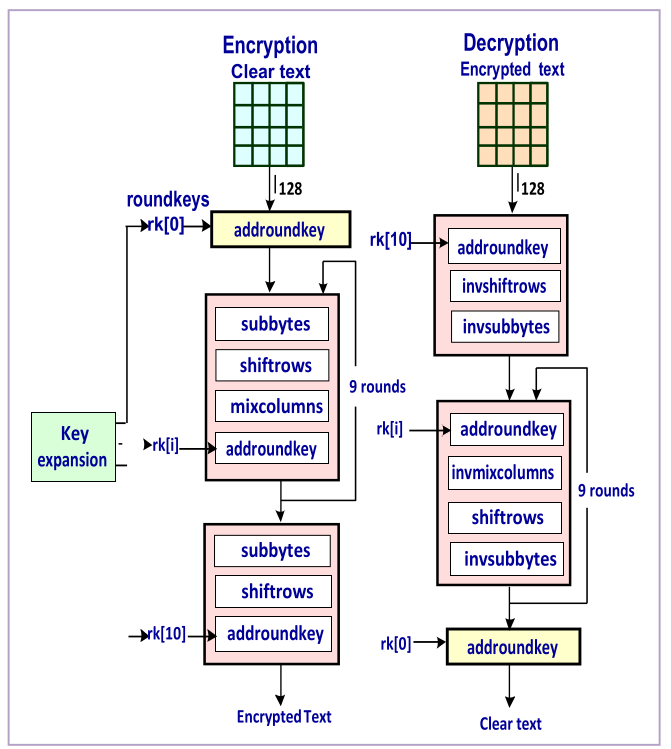
Hình 2. Mã bất đối xứng

1. **Mã đối xứng AES**

AES (Advanced Encryption Standard) là một thuật toán dùng cho mã hóa dữ liệu. AES thuộc họ mã hóa đối xứng, làm việc với các khối dữ liệu có độ dài cố định (128 bits). AES có 3 loại kích cỡ của key, được trình bày ở bảng sau

| Type | Key size (bits) | Block size (bits) | Number of rounds |
| --- | --- | --- | --- |
| AES-128 | 128 | 128 | 10 |
| AES-192 | 192 | 128 | 12 |
| AES-256 | 256 | 128 | 14 |

Các bits của một khối dữ liệu 128 bits được thay thế bằng một ma trận 4x4, với mỗi ô của ma trận tương ứng với 1 bytes. Hình bên dưới minh họa thuật toán AES



Hệ mã AES được chia làm 3 phần chính:

* Phần khởi tạo (mở rộng khóa, thêm khóa vòng)
* Phần lặp - được gọi là các round (SubBytes, ShiftRows, MixColumns, AddRoundKey). Với khóa dài 128 bits, ta cần 9 vòng lặp
* Phần cuối (SubBytes, ShiftRows và AddRoundKey)

Việc mở rộng khóa được thực hiện khi bắt đầu mã hóa. Trong phép toán XOR mật mã giữa khóa 128 bit và ma trận trạng thái 4 × 4 (khối 128 bit dữ liệu) được thực hiện. Sau đó, chín lần lặp thường được gọi là vòng được thực hiện. Số lượng vòng phụ thuộc về độ dài của khóa, đối với khóa 128 bit, nó là 9. Mỗi vòng bao gồm sự thay thế các byte trong ma trận trạng thái (SubBytes), xoay các hàng (ShiftRows) và thay thế các cột (MixColumns). Ma trận được kết hợp với khóa của vòng (Add Round Key), ở cuối mỗi vòng. Phần cuối cùng bao gồm việc thay thế các byte, xoay các hàng và lần bổ sung cuối cùng của khóa vòng. Các bytes của bản mã được lưu trữ trong ma trận kết quả.

Thuật toán AES có kết quả ấn tượng, tương đối đơn giản về mặt tốc độ mã hóa. Nó kế thừa giá trị của tốc độ mã hóa DES và có tốc độ tăng nhanh. Nó có hiệu quả mã hóa tốt và lý tưởng cho khối lượng dữ liệu được mã hóa và giải mã. So với thuật toán DES và 3DES thuật toán, thuật toán AES được cải tiến về mặt bảo mật và tính bảo mật của nó tương đối cao, nhưng vẫn thấp hơn nhiều so với thuật toán RSA; về mặt độ dài khóa, thuật toán AES cải thiện vấn đề độ dài DES không đủ, được tăng lên từ 56 bit của thuật toán DES thành 128/192/256 bit.

Tuy nhiên, thuật toán AES vẫn có một số thiếu sót trong quản lý khóa, làm cho quản lý bảo mật và phân phối các khóa trở nên khó hơn. Vì AES sử dụng cùng một chìa khóa trong việc mã hóa và giải mã dữ liệu, nó là cần thiết để truyền khóa giữa người gửi và người nhận đảm bảo rằng thông tin về khóa bên thứ ba không thể lấy được, nếu không thông tin có thể bị bẻ khóa. Mỗi ​​lần hai các bên sử dụng thuật toán AES, họ sử dụng một khóa duy nhất mà người khác không biết. Điều này sẽ làm tăng số lượng khóa và gây ra trở ngại về mặt quản lý.

1. **Mã bất đối xứng RSA**

Hệ thống mật mã RSA là một hệ thống mật mã khóa công khai, được phát minh bởi ba nhà mật mã học Ron Rivest, Adi Shamir và Len Adleman năm 1970. RSA được sử dụng để cung cấp quyền riêng tư, đảm bảo tính xác thực của dữ liệu kỹ thuật số. Hệ thống mật mã RSA có hai khóa tương ứng, đó là khóa công khai và khóa cá nhân. Khóa công khai có thể được thông báo công khai và được sử dụng để mã hóa một bản rõ hoặc hình ảnh. Tuy nhiên, khóa bí mật tương ứng

sẽ được sử dụng để giải mã văn bản mật mã. Các khóa của RSA được tạo ra như sau:

* Mỗi người chọn hai số nguyên tố lớn p và q để lập thành R = pq.
* Tìm hàm phi của Euler φ (R) = φ (pq) = φ (p) φ (q) = (p-1) (q-1).
* Mọi người chọn hai số nguyên dương e và d sao cho d là nghịch đảo của e môđun φ (R).
* Mọi người thông báo cặp (e, R) là khóa công khai của họ và giữ là cặp

(d, R) bí mật, là khóa riêng của họ

**Quy trình mã hóa cho hệ thống mật mã RSA như sau:**

* Khóa công khai của người nhận dự định (e, R) được sử dụng bởi người gửi.
* Để mã hóa một bản rõ có thể là một tin nhắn hoặc một hình ảnh, người gửi tạo thành các khối bản rõ, X, sao cho một số nguyên không âm X nhỏ hơn R.
* Người gửi sử dụng thuật toán mã hóa sau để mã hóa X: E (X) = C ≡ Xe

(mod R). C này là bản mã tương ứng với X và được gửi đến người nhận.

**Quá trình giải mã cho hệ thống mật mã RSA như sau:**

* Để giải mã khối bản mã C, thuật toán giải mã sau là được áp dụng trên mọi khối C: D (C) = X ≡ Cd (mod R).

**Đánh giá mức độ an toàn của hệ mã RSA:**

RSA là thuật toán mã hóa khóa công khai có ảnh hưởng nhất. Nó dựa trên phân tích số nguyên lớn. Các khóa của thuật toán RSA xuất hiện theo cặp và quá trình mã hóa dữ liệu được thực hiện bằng khóa cá nhân và khóa công khai. Khóa công khai là công khai, có thể được biết bởi bất kỳ ai, được sử dụng để mã hóa dữ liệu và xác minh chữ ký; khóa cá nhân giải mã và ký vào dữ liệu. Nhìn chung, lợi thế lớn nhất của thuật toán RSA là nó có khả năng quản lý khóa tốt các chức năng và bảo mật. Tính bảo mật của thuật toán RSA cao hơn nhiều so với thuật toán AES. Khóa công khai được sử dụng để mã hóa và khóa cá nhân được sử dụng để

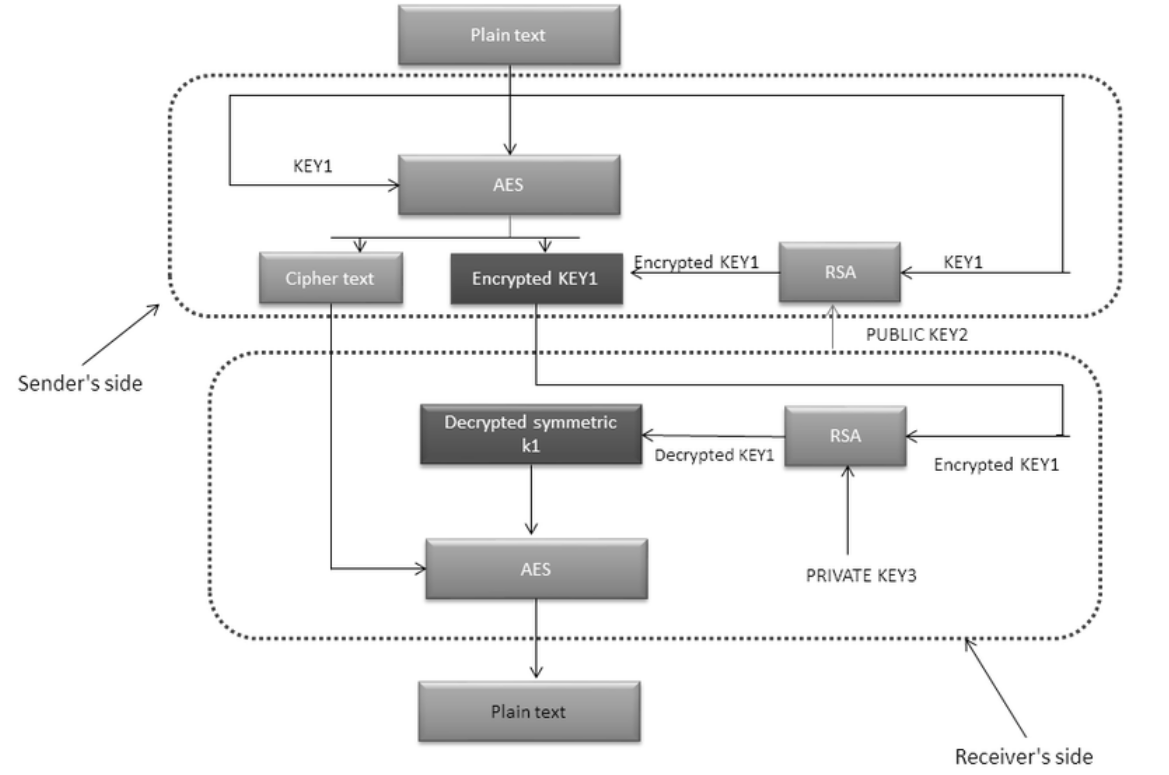
giải mã và khóa mã hóa không nhất quán với khóa giải mã. Nếu một bản rõ nhất định là được mã hóa bằng một khóa nhất định, nó phải sử dụng chìa khóa tương ứng để giải mã nó, điều này tăng cường bảo mật rất lớn. Tính bảo mật của hệ thống mật mã thuật toán RSA phụ thuộc vào độ khó của nghịch đảo hàm toán học của thuật toán mã hóa. Nó được gọi là khó khăn của thừa số hóa các số lớn. Khóa càng dài càng khó bị bẻ.

Mặc dù nó có tính bảo mật cao, nhưng thuật toán RSA có nhiều bất cập trong hiệu suất. Thuật toán RSA dựa trên các số lớn, dẫn đến chậm tốc độ hoạt động và hiệu quả thấp. Nó chỉ phù hợp để mã hóa một lượng nhỏ dữ liệu.

1. **Hệ mã “lai” AES và RSA**

Hệ mật mã đối xứng và không đối xứng có những ưu và nhược điểm riêng. Hệ thống mật mã đối xứng nhanh hơn đáng kể so với hệ thống không đối xứng, nhưng yêu cầu tất cả các bên bằng cách nào đó phải chia sẻ bí mật (chìa khóa). Hệ thống mật mã không đối xứng an toàn và cho phép cơ sở hạ tầng khóa công khai và hệ thống khóa trao đổi, nhưng với cái giá phải trả là tốc độ vì chúng sử dụng các khóa kích thước lớn.

Một hệ thống mật mã hỗn hợp kết hợp các mật mã đối xứng và bất đối xứng để hưởng lợi từ sự nhanh chóng của cái này và tính bảo mật của cái kia. Nó mang lại hiệu quả và hiệu suất tốt hơn. Hệ thống mật mã kết hợp được thể hiện trong Hình 3, bao gồm việc tạo ra một khóa bí mật ngẫu nhiên cho một mật mã đối xứng, và sau đó mã hóa khóa này thông qua mật mã không đối xứng bằng cách sử dụng khóa công khai của người nhận. Bản thân thông điệp sau đó được mã hóa bằng cách sử dụng mật mã đối xứng và khóa bí mật. Cả hai mã hóa khóa bí mật và tin nhắn được mã hóa sau đó sẽ được gửi đến người nhận.



Hình 3. Hybrid Cryptosystem

## Hướng dẫn sử dụng chương trình

## Mở rộng

1. **Tài liệu tham khảo**