

**TRƯỜNG ĐẠI HỌC LÂM NGHIỆP**

**KHOA KT & QTKD**

&

****

**ĐỒ ÁN**

**MÔN AN TOÀN BẢO MẬT THÔNG TIN**

**ĐỀ TÀI: NGHIÊN CỨU VỀ MÃ HÓA DỮ LIỆU VÀ CÁC THUẬT TOÁN THÔNG DỤNG**

**Giảng viên hướng dẫn: Mai Hà An**

**Người thực hiện: Trần Xuân Thái**

**Mã sinh viên : 2174801040133**

**LỜI NÓI ĐẦU**

Hiện nay, các công nghệ tiên tiến phát triển ngày càng mạnh mẽ và được ứng dụng ngày càng nhiều vào các lĩnh vực kinh tế, sản xuất cũng như đời sống thường nhật của con người. Một điểm tiêu biểu trong việc phát triển các công nghệ đó phải kể đến việc ứng dụng công nghệ thông tin vào hầu khắp các hoạt động. Nhờ đó công việc được thực hiện nhanh, chính xác và đạt kết quả cao hơn rất nhiều.

Do đó nhóm đề tài chọn thực hiện đề tài “**Nghiên cứu về mã hóa dữ liệu và các thuật toán thông dụng** ”. mục tiêu của báo cáo này là phân tích, thiết kế để xây dựng được dữ liệu mã hóa, giúp mọi người hiểu rõ hơn về mã hóa dữ liệu và các thuật toán về kiến trức cũng như trong cuộc sống

**LỜI CẢM ƠN**

Nhóm em xin chân thành cảm ơn các thầy cô giáo Trường Đại Học Lâm Nghiệp và đặc biệt là các thầy cô giáo nghành Hệ Thống Thông Tin đã dạy cho nhóm có được những kiến thức cơ bản vững chắc để phục vụ cho việc hoàn thành bài tập lớn này.

Đặc biệt, trong thời gian làm bài tập lớn chúng em đã được sự giảng dạy của **Thầy Mai Hà An** đã cho chúng em các kiến thức về phân tích và thiết kế hệ thống thông tin. Xin chân thành cảm ơn về những kiến thức mà các thầy đã dành cho chúng em, bổ sung cho chúng em những kiến thức cơ bản, cho chúng em những lời khuyên, sự góp ý để chúng em có thể hoàn thành bài tập lớn và bước đầu xây dựng được một phần mềm hoàn chỉnh đầu tiên của nhóm một cách nhanh chóng và hiệu quả nhất.

Trong quá trình làm bài tập lớn “**Nghiên cứu về Mã hóa dữ liệu và các thuật toán thông dụng**”, Em đã cố gắng hết sức để hoàn thiện chương trình một cách tốt nhất. Nhưng do kiến thức còn hạn chế, thời gian làm bài tập lớn có hạn và kinh nghiệm thực tế chưa nhiều nên chúng em không thể tránh được những sai sót. Vì thế Em rất mong nhận được sự góp ý của thầy và các bạn để bài tập lớn của em trở nên hoàn thiện hơn.

Em xin chân thành cảm ơn!

**Sinh viên thực hiện**:

1. Trần Xuân Thái – K66B\_HTTT
2. Thiết kế PowerPoint : Trần Xuân Thái
3. Báo Cáo và demo : Trần Xuân Thái

MỤC LỤC

[**LỜI NÓI ĐẦU**](file:///C:\Users\Admin\AppData\Local\Temp\Rar$DIa7792.48221\baoCao.docx#_heading=h.gjdgxs)

[**LỜI CẢM ƠN**](file:///C:\Users\Admin\AppData\Local\Temp\Rar$DIa7792.48221\baoCao.docx#_heading=h.30j0zll)

[**CHƯƠNG 1: GIỚI THIỆU**](file:///C:\Users\Admin\AppData\Local\Temp\Rar$DIa7792.48221\baoCao.docx#_heading=h.1fob9te)

**[1.1](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)****[Mô tả tổng quát về mã hóa dữ liệu](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

[**[1.2 Trình bày lý do để sử dụng các thuật toán mã hóa](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**](file:///C:\Users\Admin\AppData\Local\Temp\Rar$DIa7792.48221\baoCao.docx#_heading=h.3znysh7)

**[1.3 Đặc điểm của một thuật toán mã hóa hiệu qủa](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

**[CHƯƠNG 2: CÁC LOẠI MÃ HÓA DỮ LIỆU](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

[**[2.1 Mã hóa đối xứng và mã hóa không đối xứng](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**](file:///C:\Users\Admin\AppData\Local\Temp\Rar$DIa7792.48221\baoCao.docx#_heading=h.3znysh7)

[**[2.2 Mã hóa cổ điển và mã hóa dữ liệu 1 chiều](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**](file:///C:\Users\Admin\AppData\Local\Temp\Rar$DIa7792.48221\baoCao.docx#_heading=h.1fob9te)

**[CHƯƠNG 3: THUẬT TOÁN MÃ HÓA THÔNG DỤNG](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

[**[3.1 AES (Advanced Encryption Standard )](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**](file:///C:\Users\Admin\AppData\Local\Temp\Rar$DIa7792.48221\baoCao.docx#_heading=h.3znysh7)

**[3.2 RSA (Rivest-Shamir-Adleman)](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

**[3.3 DES (Data Encrytion Standard)](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

**[3.4 Blowfish](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

**[CHƯƠNG 4 : ỨNG DỤNG CỦA MÃ HÓA DỮ LIỆU](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

[**[4.1 Sử dụng mã hóa trong các lĩnh vực như tài chính , y tế , ngân hàng điện tử ,v.v….](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**](file:///C:\Users\Admin\AppData\Local\Temp\Rar$DIa7792.48221\baoCao.docx#_heading=h.1fob9te)

[**[4.2 Bảo vệ dữ liệu cá nhân và quyền riêng tư](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**](file:///C:\Users\Admin\AppData\Local\Temp\Rar$DIa7792.48221\baoCao.docx#_heading=h.1fob9te)

**[CHƯƠNG 5 : KẾT LUẬN](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

[**[5.1 Tóm tắt kết quả nghiên cứu](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**](file:///C:\Users\Admin\AppData\Local\Temp\Rar$DIa7792.48221\baoCao.docx#_heading=h.1fob9te)

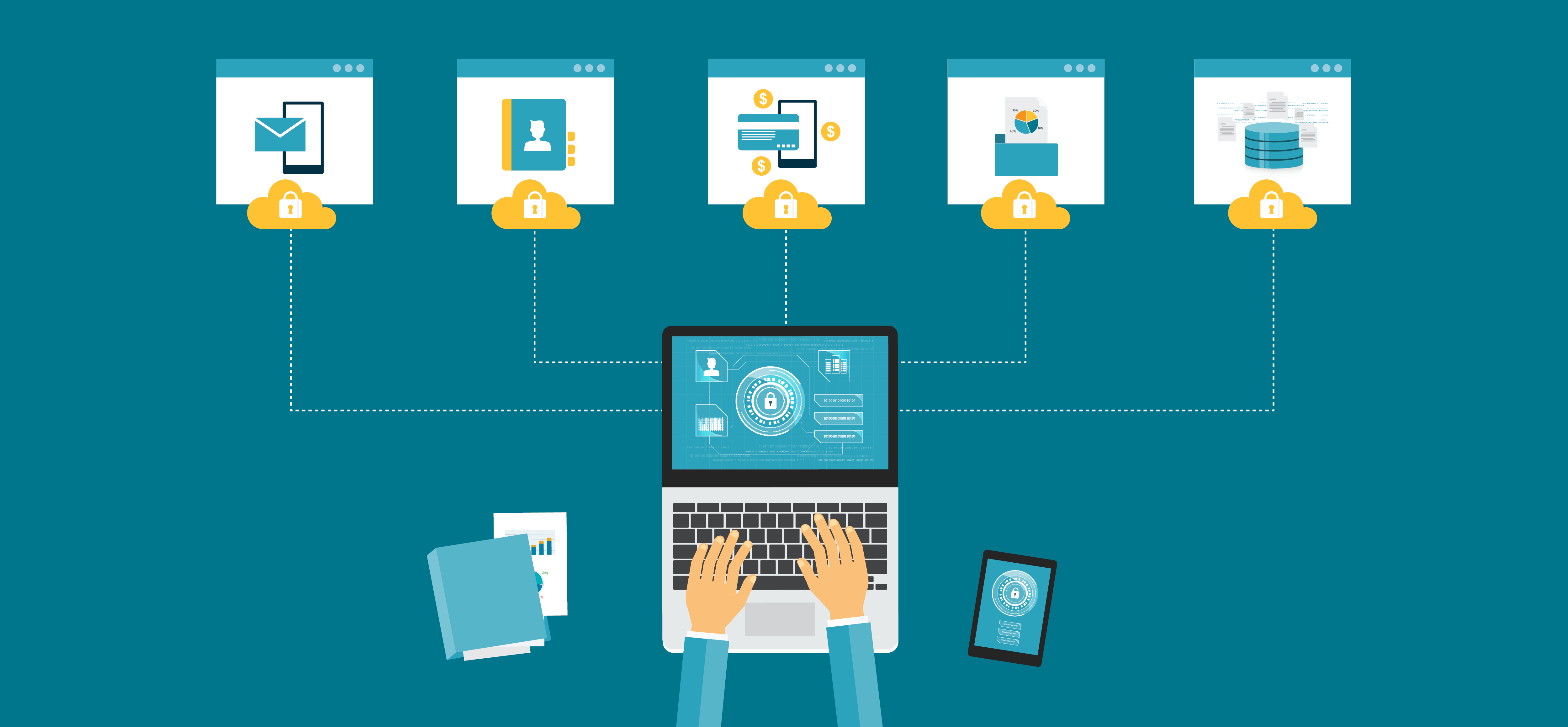
**[5.2 Những hướng phát triển của mã hóa dữ liệu](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

**[TÀI LIỆU THAM KHẢO](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**

**[CHƯƠNG 1 : GIỚI THIỆU   
  
1.1](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)****[Mô tả tổng quát về mã hóa dữ liệu](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)**  [- Mã hóa dữ liệu là gì ?](file:///C:\\Users\\Admin\\AppData\\Local\\Temp\\Rar$DIa7792.48221\\baoCao.docx" \l "_heading=h.3znysh7)

**[Mã hoá dữ liệu](https://www.sapo.vn/blog/ma-hoa-du-lieu" \t "_self)** hay còn được biết đến tên gọi Data Encryption là một trong những hình thức bảo mật thông tin bằng cách chuyển tất cả các thông tin, dữ liệu từ dạng bình thường sang một dạng khác. Hầu hết mọi người sẽ chọn mã hoá thông tin sang dạng code hoặc các ký tự đặc biệt và chỉ những người được phân quyền truy cập mới có thể đọc và giải mã những thông tin này.

Trên thực tế, vẫn có một vài trường hợp hy hữu, dữ liệu đã được mã hoá vẫn bị những hacker chuyên nghiệp đột nhập và lấy cắp. Tuy nhiên, xét về mặt bằng chung, mã hóa dữ liệu hiện vẫn đang là một trong những hình thức bảo mật có tính an toàn và hiệu quả cao nhất. Bạn có thể lựa chọn các loại mã hoá dữ liệu phù hợp với mục đích và nhu cầu của mình như: mã hóa bất đối xứng, mã hoá đối xứng, mã hoá cổ điển…

**Mã hóa dữ liệu là gì ?**

Thông thường phương pháp mã hóa dữ liệu được phân chia thành 4 loại chính: 1. Mã hóa cổ điển; 2. Mã hóa đối xứng; 3. Mã hóa bất đối xứng; 4. Mã hóa nguồn mở

**1.2 Trình bày lý do sử dụng các thuật toán mã hóa**

Các thuật toán mã hóa được sử dụng để bảo vệ thông tin cá nhân và tài sản của người dùng trên internet. Khi thông tin được mã hóa, nó sẽ trở nên khó đọc và không thể sử dụng được cho đến khi được giải mã. Điều này giúp người dùng tránh được các cuộc tấn công mạng và bảo vệ thông tin của mình khỏi những kẻ xấu có ý định lấy cắp thông tin cá nhân hoặc tài sản.

 **Hình ảnh mình họa trình bày các lý do sử dụng mã hóa.**

Các lý do sử dụng các thuật toán mã hóa bao gồm:

* Bảo vệ thông tin cá nhân và tài sản của người dùng trên internet.

- Ngăn chặn các cuộc tấn công mạng và bảo vệ thông tin khỏi những kẻ xấu có ý định lấy cắp thông tin cá nhân hoặc tài sản.

- Bảo vệ quyền riêng tư của người dùng trên internet.

- Đảm bảo an toàn cho các giao dịch trực tuyến và thanh toán điện tử.

- Bảo vệ các thông tin quan trọng của doanh nghiệp và tổ chức khỏi các cuộc tấn công mạng

**1.3 Đặc điểm của một thuật toán mã hóa hiệu quả**

- **Ưu và Nhược điểm khi sử dụng các thuật toán mã hóa :**

Mã hoá dữ liệu có những ưu điểm và hạn chế như sau:

* **Ưu điểm**

+ Bảo vệ và lưu trữ dữ liệu một cách tốt nhất

+ Tránh sự xâm nhập của kẻ gian

* **Hạn chế**

+ Hao tốn tài nguyên của CPU trong quá trình xử lý dữ liệu

+ Tốc độ mã hoá và giải mã mất khá nhiều thời gian

+ Làm chậm quy trình làm việc của hệ thống

+ Nhiều loại mã hóa dữ liệu hiện đại tốn khá nhiều dung lượng vậy nên lưu trữ và truyền tải dữ liệu sẽ khá lâu.

**Một thuật toán mã hóa hiệu quả có những đặc điểm sau:**

* Khóa bí mật phải được giữ bí mật và không được tiết lộ cho bất kỳ ai ngoại trừ người được ủy quyền.
* Khóa bí mật phải có độ dài đủ lớn để tránh bị tấn công brute-force.
* Khóa bí mật phải được tạo ra ngẫu nhiên và không được lặp lại.
* Thuật toán mã hóa phải được thiết kế sao cho khó bị tấn công và phải có khả năng chống lại các cuộc tấn công phổ biến như tấn công brute-force, tấn công dictionary, tấn công MITM

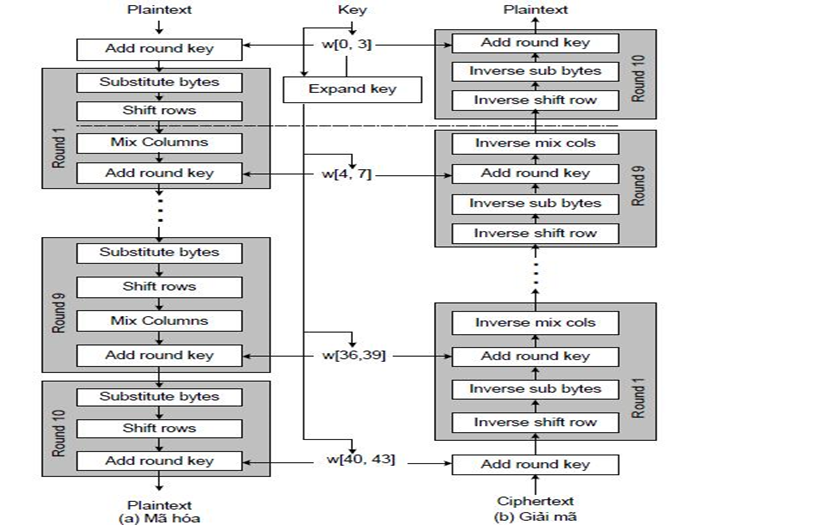
**CHƯƠNG 2 : CÁC LOẠI MÃ HÓA DỮ LIỆU**

**2.1 Mã hóa đối xứng và Mã hóa không đối xứng**

* **Mã hóa đối xứng :** là một phương pháp mật mã trong đó một khóa duy nhất chịu trách nhiệm mã hóa và giải mã dữ liệu. Các bên liên quan chia sẻ khóa, mật khẩu hoặc cụm mật khẩu đó và họ có thể sử dụng nó để giải mã hoặc mã hóa bất kỳ thư nào họ muốn. [Theo Dự án bảo mật ứng dụng web mở](https://www.owasp.org/index.php/Guide_to_Cryptography#Symmetric_Cryptography)  (OWASP), một số thuật toán phổ biến nhất được sử dụng cho mật mã đối xứng bao gồm Tiêu chuẩn mã hóa dữ liệu (DES), sử dụng khóa 56 bit, Triple DES, áp dụng thuật toán DES ba lần với các chìa khóa; và Tiêu chuẩn Mã hóa Nâng cao (AES), một thuật toán mà Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ khuyến nghị các ứng dụng mới sử dụng để lưu trữ và truyền dữ liệu một cách an toàn.

***Mô hình mã hóa đối xứng***

* **Các thuật toán mã hóa đối xứng :**
* Thuật toán đối xứng có thể được chia ra làm hai thể loại, mật mã luồng (stream ciphers) và mật mã khối (block ciphers). Mật mã luồng mã hóa từng bit của thông điệp trong khi mật mã khối gộp một số bit lại và mật mã hóa chúng như một đơn vị. Cỡ khối được dùng thường là các khối 64 bit. Thuật toán tiêu chuẩn mã hóa tân tiến (Advanced Encryption Standard), được NIST công nhận tháng 12 năm 2001, sử dụng các khối gồm 128 bit
* Các thuật toán đối xứng thường không được sử dụng độc lập.Trong thiết kế của các hệ thống mật mã hiện đại, cả hai thuật toán bất đối xứng (*asymmetric*) (dùng chìa khóa công khai) và thuật toán đối xứng được sử dụng phối hợp để tận dụng các ưu điểm của cả hai. Những hệ thống sử dụng cả hai thuật toán bao gồm những cái như SSL (*Secure Sockets Layer*), PGP (*Pretty Good Privacy*) và GPG (*GNU Privacy Guard*) v.v. Các thuật toán chìa khóa bất đối xứng được sử dụng để phân phối chìa khóa mật cho thuật toán đối xứng có tốc độ cao hơn.
* Một số ví dụ các thuật toán đối xứng nổi tiếng và khá được tôn trọng bao gồm Twofish, Serpent, AES (còn được gọi là Rijndael), Blowfish, CAST5, RC4, Tam phần DES (*Triple DES*), và IDEA (*International Data Encryption Algorithm – Thuật toán mật mã hóa dữ liệu quốc tế*).

*Ví dụ hình ảnh minh họa về mô hình thuật toán mã hóa AES*

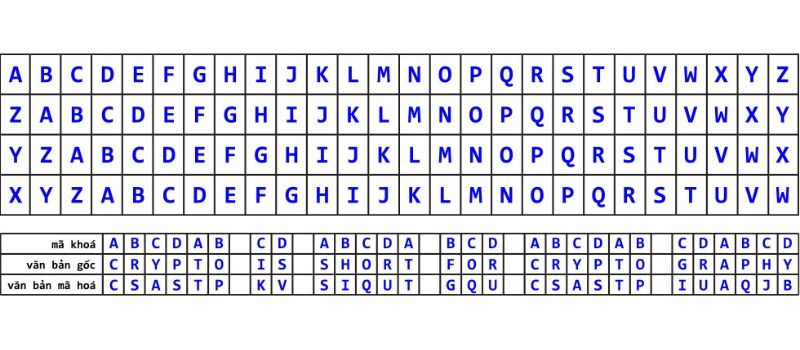
* **Tốc độ :**
* Các thuật toán đối xứng nói chung đòi hỏi công suất tính toán ít hơn các thuật toán khóa bất đối xứng (*asymmetric key algorithms*). Trên thực tế, một thuật toán khóa bất đối xứng có khối lượng tính toán nhiều hơn gấp hằng trăm, hằng ngàn lần một thuật toán khóa đối xứng (*symmetric key algorithm*) có chất lượng tương đương.
* **Về hạn chế :**
* Hạn chế của các thuật toán khóa đối xứng bắt nguồn từ yêu cầu về *sự phân hưởng chìa khóa bí mật*, mỗi bên phải có một bản sao của chìa. Do khả năng các chìa khóa có thể bị phát hiện bởi đối thủ mật mã, chúng thường phải được bảo an trong khi phân phối và trong khi dùng. Hậu quả của yêu cầu về việc lựa chọn, phân phối và lưu trữ các chìa khóa một cách không có lỗi, không bị mất mát là một việc làm khó khăn, khó có thể đạt được một cách đáng tin cậy.
* Để đảm bảo giao thông liên lạc an toàn cho tất cả mọi người trong một nhóm gồm n người, tổng số lượng chìa khóa cần phải có là \begin{matrix} \frac {n{(n-1})}{2} \end{matrix}
* Hiện nay người ta phổ biến dùng các thuật toán bất đối xứng có tốc độ chậm hơn để phân phối chìa khóa đối xứng khi một phiên giao dịch bắt đầu, sau đó các thuật toán khóa đối xứng tiếp quản phần còn lại . Vấn đề về bảo quản sự phân phối chìa khóa một cách đáng tin cậy cũng tồn tại ở tầng đối xứng, song ở một điểm nào đấy, người ta có thể kiểm soát chúng dễ dàng hơn. Tuy thế, các khóa đối xứng hầu như đều được sinh tạo tại chỗ.
* Các thuật toán **khóa đối xứng** không thể dùng cho mục đích xác thực (*authentication*) hay mục đích chống thoái thác (*non-repudiation*) được.
* **Mã hóa không đối xứng ( mã hóa công khai ) :** Là thuật toán  trong đó việc mã hóa và giãi mã dùng hai khóa khác nhau là pulic key(khóa công khai hay khóa công cộng) và private key (khóa riêng ).
* Nếu dung public key để mã hóa thì private key sẽ dùng để giải mã và ngược lại



* **An toàn**
* Về khía cạnh an toàn, các thuật toán mật mã hóa bất đối xứng cũng không khác nhiều với các thuật toán mã hóa đối xứng. Có những thuật toán được dùng rộng rãi, có thuật toán chủ yếu trên lý thuyết; có thuật toán vẫn được xem là an toàn, có thuật toán đã bị phá vỡ… Cũng cần lưu ý là những thuật toán được dùng rộng rãi không phải lúc nào cũng đảm bảo an toàn. Một số thuật toán có những chứng minh về độ an toàn với những tiêu chuẩn khác nhau. Nhiều chứng minh gắn việc phá vỡ thuật toán với những bài toán nổi tiếng vẫn được cho là không có lời giải trong thời gian đa thức . Nhìn chung, chưa có thuật toán nào được chứng minh là an toàn tuyệt đối (như hệ thống mật mã sử dụng một lần). Vì vậy, cũng giống như tất cả các thuật toán mật mã nói chung, các thuật toán mã hóa khóa công khai cần phải được sử dụng một cách thận trọng.
* **Ứng dụng**
* Ứng dụng rõ ràng nhất của mật mã hóa khóa công khai là bảo mật: một văn bản được mã hóa bằng khóa công khai của một người sử dụng thì chỉ có thể giải mã với khóa bí mậtcủa người đó.
* Các thuật toán tạo chữ ký số khóa công khai có thể dùng để nhận thực. Một người sử dụng có thể mã hóa văn bản với khóa bí mật của mình. Nếu một người khác có thể giải mãvới khóa công khai của người gửi thì có thể tin rằng văn bản thực sự xuất phát từ người gắn với khóa công khai đó.
* Các đặc điểm trên còn có ích cho nhiều ứng dụng khác như: tiền điện tử, thỏa thuận khóa…
* **Điểm yếu**
* Tồn tại hả năng một người nào đó có thể tìm ra được khóa bí mật. Không giống với hệ thống mật mã sử dụng một lần (one-time pad) hoặc tương đương, chưa có thuật toán mã hóa khóa bất đối xứng nào được chứng minh là an toàn trước các tấn công dựa trên bản chất toán học của thuật toán. Khả năng một mối quan hệ nào đó giữa 2 khóa hay điểm yếu của thuật toán dẫn tới cho phép giải mã không cần tới khóa hay chỉ cần khóa mã hóa vẫn chưa được loại trừ. An toàn của các thuật toán này đều dựa trên các ước lượng vềkhối lượng tính toán để giải các bài toán gắn với chúng. Các ước lượng này lại luôn thay đổi tùy thuộc khả năng của máy tính và các phát hiện toán học mới.
* Khả năng bị tấn công dạng **kẻ tấn công đứng giữa** (man in the middle attack): kẻ tấn công lợi dụng việc phân phối khóa công khai để thay đổi khóa công khai. Sau khi đã giả mạo được khóa công khai, kẻ tấn công đứng ở giữa 2 bên để nhận các gói tin, giải mã rồi lại mã hóa với khóa đúng và gửi đến nơi nhận để tránh bị phát hiện. Dạng tấn công kiểu này có thể phòng ngừa bằng các phương pháp trao đổi khóa an toàn nhằm đảm bảo nhận thực người gửi vàtoàn vẹn thông tin. Một điều cần lưu ý là khi các chính phủ quan tâm đến dạng tấn công này: họ có thể thuyết phục (hay bắt buộc) nhà cung cấp chứng thực số xác nhận một khóa giả mạo và có thể đọc các thông tin mã hóa.
* **Khối lượng tính toán**
* Để đạt được độ an toàn tương đương đòi hỏi khối lượng tính toán nhiều hơn đáng kể so với thuật toán mật mã hóa đối xứng. Vì thế trong thực tế hai dạng thuật toán này thường được dùng bổ sung cho nhau để đạt hiệu quả cao. Trong mô hình này, một bên tham gia trao đổi thông tin tạo ra một khóa đối xứng dùng cho phiên giao dịch. Khóa này sẽ được trao đổi an toàn thông qua hệ thống mã hóa khóa bất đối xứng. Sau đó 2 bên trao đổi thông tin bí mật bằng hệ thống mã hóa đối xứng trong suốt phiên giao dịch.

**2.2 Mã Hóa Cổ Điển và Mã Hóa Dữ Liệu Một Chiều**

* **Mã Hóa Cổ Điển :** Loại mã hóa dữ liệu này xuất hiện đầu tiên, quy trình hoạt động đơn giản nhất nhưng cũng là loại mã hóa có độ bảo mật thấp nhất. Người sử dụng dạng mã hoá này không cần phải tạo key bảo mật, thay vào đó chỉ cần tìm hiểu thông tin và kiến thức cơ bản về các thuật toán đơn thuần là 90% đã có thể giải mã. Chính bởi vậy, mã hoá dạng cổ điển hiện không còn được áp dụng phổ biến vì sản phẩm công nghệ sẽ rất dễ trở thành “miếng mồi béo bở” của những hacker.



* **Mã Hóa Dữ Liệu Một Chiều :**

Đúng như tên gọi, mã hóa dữ liệu một chiều là người dùng chỉ có thể mã hoá nó mà không cần giải mã. Thông thường, dạng mã hoá này sẽ được ứng dụng để kiểm tra tính toàn vẹn của dữ liệu, chữ ký điện tử, lưu trữ mật khẩu…Hai thuật toán được sử dụng trong loại mã hoá này là MD5 và SHA. Nhìn chung mã hóa dữ liệu một chiều rất dễ cài đặt nhưng ngoài những trường hợp đặc thù thì mã hóa dữ liệu một chiều gần như rất ít được ứng dụng.



**CHƯƠNG 3 : THUẬT TOÁN MÃ HÓA THÔNG DỤNG**

**3.1 AES (Advanced Encryption Standard )**

## Mã hóa AES  là gì?



**Advanced Encryption Standard (AES) hay còn được gọi là tiêu chuẩn mã hóa nâng cao theo phương pháp mật mã khối**. Với ưu thế bảo mật cao nó đã được chính phủ Hoa Kỳ lựa chọn để bảo vệ [dữ liệu](https://bkhost.vn/blog/data-du-lieu/), thông tin cho các tổ chức, doanh nghiệp mà người dùng.

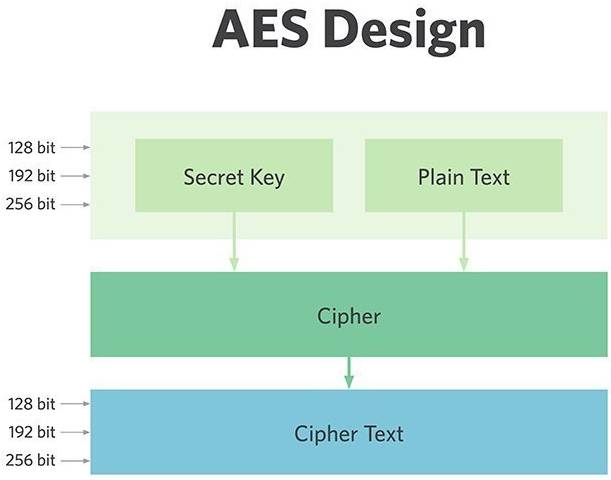
Các tác vụ của AES được thực hiện ở cả phần cứng và phần mềm trên nhiều thiết bị để [mã hóa](https://bkhost.vn/blog/ma-hoa/) dữ liệu nhạy cảm. Sự có mặt của nó đã góp phần bảo đảm an toàn cho máy tính của chính phủ, [an ninh mạng](https://bkhost.vn/blog/an-ninh-mang-cyber-security/) và tạo một rào chắn vững chắc để bảo vệ dữ liệu.

Năm 1997 AES lầm đầu tiên được công bố bởi Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST). Tại thời điểm đó Tiêu chuẩn mã hóa dữ liệu [DES](https://bkhost.vn/blog/thuat-toan-ma-hoa-des/) xuất hiện những lỗ hổng vì thế AES được nghiên cứu và phát triển để thay thế cho nó.

NIST đã rất tự tin khi tuyên bố rằng AES chính là giải pháp tốt nhất để bảo vệ thông tin nhạy cảm cho chính phủ trong thế kỷ XXI. Đặc biệt so với các tiêu chuẩn khác thì AES có khả năng thực hiện tác vụ trong môi trường hạn chế như thẻ thông minh.

## AES hoạt động như thế nào?

AES gồm ba mật mã khối AES-128, AES-192, AES-256 tương ứng với độ dài của key là 128 bit, 192 bit và 256 bit. Số vòng của key khác nhau, cụ thể 10 vòng cho 128 bit, 12 vòng cho 192 bit và 14 vòng cho 256 bit. Mỗi vòng đều thực hiện ba bước thay thế, biến đổi và hòa trộn khối plain text (văn bản thuần túy) đầu vào để biến nó thành Ciphertext (văn bản đã mã hóa).



Thông tin được chính phủ phân loại theo ba cấp độ: bảo mật, bí mật, tối mật. Tất cả các độ dài của key từ 128, 192 và 256 bit đều được dùng ở cấp độ bảo mật, bí mật. Riêng với những thông tin tối mật để đảm bảo không xảy ra bất cứ sai sót nào phải cần đến key 192 hoặc 256 bit. Mật mã sẽ dùng một key riêng tư để mã hóa và giải mã dữ liệu và tất nhiên cả người gửi và người nhận đều phải nhận biết và sử dụng được key này.

## Các tiêu chí cần có ở AES

NIST đưa ra yêu cầu đối với AES đó là phải sử dụng phương pháp mã hóa khối với độ dài của key là 128, 192 và 256 bit để mã hóa và giải mã dữ liệu. Ngoài ra AES phải đáp ứng được những tiêu chí sau:

* **Bảo vệ**: Đây là một trong những tính năng hàng đầu AES cần phải có để đánh bại các đối thủ khác. Nó phải có khả năng chống lại các cuộc tấn công mạnh, quy mô lớn.
* **Chi phí**: AES mở ra nhiều cơ hội cho người dùng bằng cách phát hành trên toàn cầu và miễn phí bản quyền.
* **Khả năng thực hiện**: Linh hoạt, phù hợp và đơn giản chính là 3 yếu tố quan trọng hội tụ ở AES để đáp ứng trọn vẹn nhu cầu của người dùng.

## Chọn thuật toán AES mới

* Để có được một thuật toán đạt tới độ hoàn hảo vào tháng 8 năm 1999 NIST đã chọn MARS, RC6, Rijndael, Serpent, Twofish để phân tích. Tất cả 5 thuật toán trên đã được thử nghiệm trong ANSI, các ngôn ngữ như Java và C. Chúng được so sánh với nhau dựa vào các yêu tố như tốc độ mã hóa, mức độ tin cậy, thời gian thiết lập key và thuật toán, mức độ chống lại các cuộc công.
* Sau quá trình làm việc nghiêm túc, vào tháng 10 năm 2000 các thành viên của cộng đồng mật mã toàn cầu đã chọn Rijndael làm thuật toán đề xuất cho AES. Tháng 12 năm 2001 nó được Bộ trưởng Thương mại Hoa Kỳ chấp nhận và năm 2002 chính thức có hiệu lực như một tiêu chuẩn của chính phủ liên bang.
* Tháng 6 năm 2004, AES được chính phủ Mỹ thông báo với công chúng và được ứng dụng để bảo vệ thông tin đã phân loại. Kể từ đó AES phủ sóng ở nhiều lĩnh vực và nó được NSA (cơ quan an ninh Quốc gia Hoa Kỳ) chọn để bảo vệ hệ thống an ninh cho chính phủ và đất nước. Có thể khẳng định khi AES được chính phủ Hoa Kỳ sử dụng thành công đã tạo được tiếng vang rất lớn. Nó nhanh chóng được các tổ chức tư nhân săn đón để tạo “bức [tường lửa](https://bkhost.vn/blog/firewall/)” bảo vệ những dữ liệu mật.

## Sự khác biệt giữa AES-128 và AES-256 là gì?

* Hầu hết các chuyên gia đều khẳng định rằng khi sử dụng AES thì mọi thông tin đều an toàn trước các cuộc tấn công bạo lực. Và tất nhiên để không xảy ra bất cứ vấn đề gì đòi hỏi kích thước key được sử dụng cho mã hóa AES phải có độ dài đủ lớn.
* Thực tế cho thấy mã hóa 256 bit khó đoán hơn rất nhiều so với key 128 bit. Vì lẽ đó mà nó rất mạnh mẽ và bảo vệ dữ liệu trước các cuộc tấn công brute – force. Trong tương lai thì chưa thể biết được nhưng hiện tại việc phá vỡ thuật toán này là điều không tưởng. Và có thể xem AES-256 là giải pháp hoàn hảo để các tổ chức [bảo mật dữ liệu](https://bkhost.vn/blog/cac-giai-phap-bao-mat-co-so-du-lieu/) của mình.
* Tuy nhiên một điểm hạn chế của key 256bit đó là nó đòi hỏi sức mạnh xử lý cao hơn key 128 bit và chắc chắn rằng thời gian để thực thi cũng lâu hơn. Do đó đối với các thiết bị nhỏ hoặc với nguồn điện tải trọng thấp thì nên cân nhắc sử dụng key 128 bit.

## Sự khác biệt giữa AES và RSA là gì?

* AES được cá nhân, tổ chức sử dụng để bảo vệ những dữ liệu ở trạng thái nghỉ (dữ liệu lưu trữ trong kho). Ứng dụng của AES có thể kể đến như: tự mã hóa ổ đĩa, mã hóa lưu trữ, mã hóa cơ sở dữ liệu. Trong khi đó [RSA](https://bkhost.vn/blog/rsa/) lại được ứng dụng để kết nối các website trong các trình duyệt và nhiều lĩnh vực khác.
* Một điểm khác biệt nữa đó là trong khi AES sử dụng key riêng tư thì RSA lại dùng key công khai. Bên cạnh đó hiệu suất hoạt động của RSA chậm hơn so với AES. Vì thế giải pháp tốt nhất để bảo vệ việc truyền dữ liệu từ ở khoảng cách xa đó là kết hợp cả mã hóa RSA với AES.

## AES có an toàn không?

* AES nếu được triển khai đúng quy trình thì sẽ đảm bảo an toàn tuyệt đối. Thế nhưng một điều cần lưu ý đó là bất kỳ một hệ thống nào cũng có thể bị tấn công nếu hacker biết được key mã hóa. Do đó các key mã hóa AES phải được bảo vệ bằng nhiều cách khác nhau như dùng [mật khẩu](https://bkhost.vn/blog/password/) mạnh, xác thực, tường lửa hay phần mềm chống độc hại. Ngoài ra các tổ chức phải đào tạo nhân viên để nâng cao nhận thức của họ trong việc bảo mật thông tin, tránh bị kẻ xấu lợi dụng.

**3.2 RSA (Rivest-Shamir-Adleman)**

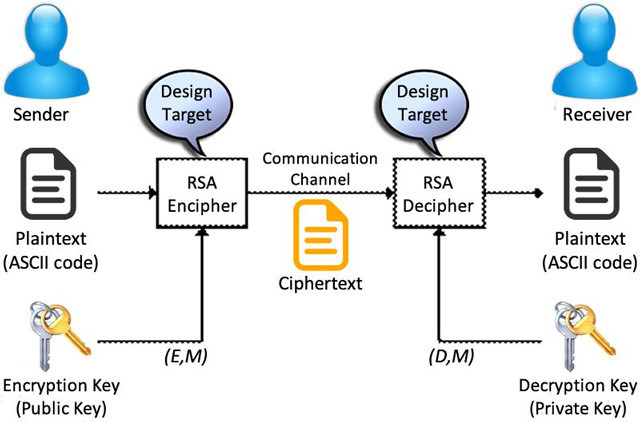
[Thuật toán RSA được phát minh vào năm 1978 bởi Ron Rivest, Adi Shamir và Leonard Adleman](https://ichi.pro/vi/giai-ma-thuat-toan-rsa-260334254953362), Thuật toán RSA được sử dụng trong mật mã học và là một thuật toán mã hóa khóa công khai. Độ dài của khóa RSA được đo bằng số bit của nó. Ví dụ, một khóa RSA 2048 bit có độ dài 2048 bit. Thuật toán RSA thường được sử dụng với các khóa có độ dài từ 1024 đến 4096 bit

**Thuật Toán RSA là gì?**

Thuật toán RSA (Rivest-Shamir-Adleman) là một thuật toán mã hóa khóa công khai được sử dụng rộng rãi trong mật mã học. Thuật toán này được đặt tên theo ba nhà khoa học máy tính người Mỹ: Ron Rivest, Adi Shamir và Leonard Adleman. Thuật toán RSA sử dụng một cặp khóa để thực hiện quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa. [Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng](https://vietnix.vn/rsa/" \t "_blank)

* **Cách thức hoạt động của thuật toán RSA là gì?**
* Thuật toán RSA sử dụng một cặp khóa để thực hiện quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa. Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. [Thuật toán RSA hoạt động như sau](https://muaban.net/blog/rsa-118289/" \t "_blank):

1. Một cặp khóa (public key, private key) được tạo ra bằng cách chọn hai số nguyên tố lớn và tính toán.
2. Public key được công bố và private key được giữ bí mật.
3. Để mã hóa thông điệp, người gửi sử dụng public key để mã hóa thông điệp.
4. Để giải mã thông điệp, người nhận sử dụng private key để giải mã.



[Một nhược điểm lớn của mã hoá RSA đó là tốc độ mã hoá chậm hơn nhiều so với mã hoá DES](https://viblo.asia/p/rsa-va-nhung-dieu-thu-vi-m68Z0apAlkG). [Tuy nhiên, để tăng tốc độ, người mã hoá sẽ mã hoá tài liệu bằng một mã hoá khác nhưng khoá sẽ được mã hoá bằng RSA](https://viblo.asia/p/rsa-va-nhung-dieu-thu-vi-m68Z0apAlkG" \t "_blank)

Trong mật mã học, 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[**1**](https://bing.com/search?q=Thu%E1%BA%ADt+to%C3%A1n+RSA+c%C3%B3+b%E1%BA%A3o+m%E1%BA%ADt+kh%C3%B4ng%3f). Tuy nhiên, do thuật toán đã được công bố trước khi có đăng ký bảo hộ nên sự bảo hộ hầu như không có.

## ****Cách mã hóa RSA hoạt động trong thực tế :****

* Các phần trên sẽ cung cấp cho bạn một hiểu biết hợp lý về cách thức hoạt động của phép toán đằng sau mã hóa public key nhưng nó có thể hơi khó hiểu.
* Trong các bước được liệt kê ở trên, chúng tôi đã chỉ ra cách hai người giao tiếp với nhau an toàn mà không cần chia sẻ mã trước đó. Đầu tiên, mỗi người cần thiết lập cặp key của riêng mình và chia sẻ public key với nhau. Hai người cần giữ bí mật về private key của họ để thông tin liên lạc của họ được bảo mật.



* Khi người gửi có public key của người nhận, họ có thể sử dụng key đó để mã hóa dữ liệu mà họ muốn bảo mật. Khi nó đã được mã hóa bằng public key, nó chỉ có thể được giả mã bằng private key từ cùng một cặp key. Ngay cả cùng một public key cũng không thể được sử dụng để giải mã dữ liệu. Điều này là do các thuộc tính của chức năng hàm trapdoor mà đã được đề cập.
* Khi người nhận nhận được tin nhắn được mã hóa, họ sử dụng private key của mình để truy cập dữ liệu. Nếu người nhân muốn gửi lại thông tin liên lạc theo cách an toàn, thì họ có thể mã hóa tin nhắn của mình bằng public key. Một lần nữa, khi nó đã được mã hóa bằng public key, cách duy nhất để thông tin có thể được truy cập là thông qua private key.
* Theo cách này, mã hóa RSA có thể được sử dụng bởi các bên chưa biết trước đây để gửi dữ liệu một cách an toàn. Em mong các bạn hiểu rõ về cách thức hoạt động của mã hóa RSA và có thể áp dụng thành công thuật toán này để bảo mật dữ liệu của bạn.

**3.3 DES (Data Encrytion Standard)**

## Data Encryption Standard (DES) là gì?

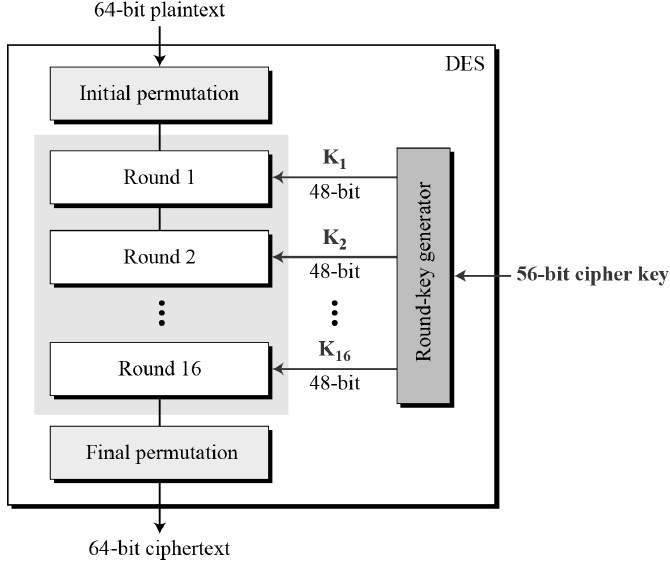


**Data Encryption Standard (DES) hay còn được gọi là Tiêu chuẩn mã hóa dữ liệu bằng phương pháp khóa đối xứng**. Vào đầu những năm 1970 DES được nghiên cứu và công bố bởi các nhà nghiên cứu của IBM.

Năm 1977 nó chính thức được Viện tiêu chuẩn và công nghệ quốc gia Hoa Kỳ (NIST) thông qua để bảo vệ những [dữ liệu](https://bkhost.vn/blog/data-du-lieu/) mật cho chính phủ. Thế nhưng sau vài thập niên khả năng phát triển của DES không khả quan và nó đã chính thức ngừng hoạt động vào năm 2005.

Với sự phê duyệt của chính phủ Hoa Kỳ DES nhanh chóng phổ biến ở nhiều ngành nghề khác nhau nhất là những lĩnh vực cần mã hóa mạnh như dịch vụ tài chính. Bên cạnh đó DES còn được ứng dụng ở thẻ thông minh, thẻ sim, modem, [bộ định tuyến](https://bkhost.vn/blog/router-bo-dinh-tuyen/)…

## Nguyên lý hoạt động của DES



Để thực hiện thao tác mã hóa và giải mã tin nhắn DES sử dụng cùng một key riêng tư. Và tất nhiên key này cả người nhận và người gửi đều nhận biết và sử dụng được. Từ khi ra đời nó đã trở thành thuật toán khóa đối xứng nhằm mục đích mã hóa dữ liệu điện tử. Hiện tại nó đã bị thay thế bởi tiêu chuẩn mã hóa nâng cao AES với tính năng bảo mật tốt hơn. Dưới đây là một số tính năng cơ bản tác động tới cách thức hoạt động của DES:

* **Key mật mã**: DES sử dụng phương pháp mật mã khối, điều này có nghĩa là mỗi khối dữ liệu sẽ được áp dụng bởi một key mật mã và thuật toán. DES sẽ nhóm plain text (văn bản thuần túy) thành các khối 64 bit. Bằng cách kết hợp và hoán vị các khối của plain text sẽ được chuyển đổi thành Ciphertext (văn bản đã mã hóa).
* **Vòng mã hóa**: Dữ liệu sẽ được DES mã hóa 16 lần với bốn chế độ khác nhau. Từng khối riêng lẻ sẽ được mã hóa hoặc bắt buộc các khối mật mã phải phụ thuộc vào những khối trước đó. Riêng về giải mã thì đơn giản chỉ là nghịch đảo của mã hóa, tức là quy trình thực hiện tương tự nhưng đảo ngược thứ tự các key.
* **Phím 64 bit**: Thực tế cho thấy mặc dù DES sử dụng key 64 bit nhưng có 8 bit trong số đó đã được dùng để kiểm tra chẵn lẻ. Vì lẽ đó là key hiệu dụng chỉ có 56 bit.
* **Thay thế và hoán vị**: Đây là hai quy trình mà Ciphertext phải trải qua trong quá trình mã hóa.
* **Khả năng tương thích ngược** (tương thích với phiên bản cũ): Trong một số trường hợp DES cũng cung cấp khả năng này.

## Vì sao DES không an toàn?

* Với bất cứ mật mã nào thì các tấn công brute-force (tấn công bạo lực) bằng cách thử từng phím một cho đến khi đạt được mục tiêu cũng gây ra những trở ngại lớn. Cách tốt nhất để ngăn chặn được đó là phải tăng độ dài của key. Trong khi đó kích thước của key DES là 56 bit nên nhiều chuyên gia bảo mật nghi ngờ trong tương lai nó sẽ bị phá vỡ bởi những kẻ xấu.
* Mặc dù nhiều người đặt nghi vấn nhưng DES vẫn là một tiêu chuẩn mã hóa được sử dụng phổ biến cho đến năm 1990. Đến năm 1998, chỉ trong vòng 56 giờ một máy tính của Tổ chức Biên giới Điện tử (EFF) đã giải mã thành công thông điệp mã hóa DES. Và chỉ sau đó một năm bằng cách kết hợp sức mạnh của hàng nghìn máy tính EFF đã giảm thời gian mã hóa xuống chỉ còn 22 giờ.
* Kể từ đó có khá nhiều dịch vụ bẻ khóa DES ra đời. Nổi bật hơn hết là ở website crack.sh với lời cam kết thực hiện việc đó trong vòng 26 giờ. Như vậy có thể thấy DES đã không còn an toàn như trước kia và việc thay thế nó là điều cần thiết.

## Kế thừa DES :

* Năm 1997, 15 thuật toán đã được NIST bắt đầu bình chọn, đánh giá để tìm người kế nhiệm thay cho DES, Năm 2001, mật mã Rijndael đã chính thức trở thành AES mới để bảo mật thông tin cho chính phủ Mỹ và các tổ chức tư nhân.
* Tháng 5 năm 2005 Tiêu chuẩn mã hóa dữ liệu (FIPS 46 – 3) đã bị hủy bỏ hoàn toàn. Sau đó một thời gian Triple DES (3DES) – một phiên bản của DES cũng không được người dùng tin tưởng nữa.

## Ngày nay DES được sử dụng như thế nào?

## Thuật toán mã hoá khối và một số trường hợp tấn công trong CTF (Phần 1)

* DES và 3DES là các tiêu chuẩn đã ngừng hoạt động nhưng người dùng vẫn có thể dùng chúng và đồng nghĩa với đó là phải chấp nhận rủi ro. Trước đây DES được dùng ở các giao dịch tài chính của chính phủ Mỹ thì bây giờ nó chỉ được áp dụng cho các dịch vụ tài chính và các ngành công nghiệp khác.
* Tóm lại DES vẫn được dùng ở mức hạn chế. Ngày nay nó được sử dụng để các chuyên gia giảng dạy, đào tạo về mật mã. Trong học thuật công nghệ này vẫn có giá trị để chứng minh một số vấn đề liên quan đến mật mã kỹ thuật số.

## Di sản của DES

* Trước khi DES được công bố thì khái niệm mật mã chỉ tồn tại ở chính phủ và các tổ chức tình báo. Qua đó có thể thấy DES đã trở thành quá khứ nhưng sự xuất hiện của nó đã tạo tiền đề thúc đẩy việc nghiên cứu mật mã và cho ra đời các thuật toán mạnh mẽ hơn.

## Tổng kết về DES

* Trên đây chúng tôi đã cung cấp những thông tin liên quan tới Data Encryption Standard (DES). Sự kết thúc của DES là khởi đầu cho những tiêu chuẩn mới. Vì thế chúng ta nên trân trọng những giá trị mà nó đã từng mang lại cho cộng đồng.

**3.4 Blowfish**

Blowfish là một thuật toán mã hóa khối đối xứng được thiết kế bởi Bruce Schneier vào năm 1993 và được sử dụng trong nhiều bộ mã hóa và sản phẩm mã hóa khác nhau. [Blowfish cung cấp tốc độ mã hóa tốt trong phần mềm và không có phương pháp phân tích mật mã hiệu quả nào được tìm thấy cho đến nay**1**](https://en.wikipedia.org/wiki/Blowfish_%28cipher%29). [Blowfish là một trong những thuật toán khối an toàn đầu tiên không phải là đối tượng của bất kỳ bằng sáng chế nào**2**](https://www.techtarget.com/searchsecurity/definition/Blowfish). [Blowfish được sử dụng rộng rãi trong các ứng dụng như TLS, SSH, IPsec và OpenVPN**1**](https://en.wikipedia.org/wiki/Blowfish_%28cipher%29).

### **Blowfish là gì?**

Blowfish là một [mật mã khối](https://www.techtarget.com/searchsecurity/definition/block-cipher) 64 bit có độ dài thay đổi, đối xứng. Được thiết kế bởi Bruce Schneier vào năm 1993 như một "thuật toán có mục đích chung", nó nhằm cung cấp một giải pháp thay thế nhanh, miễn phí, thả vào cho các thuật toán mã hóa Tiêu chuẩn mã hóa dữ liệu ([DES)](https://www.techtarget.com/searchsecurity/definition/Data-Encryption-Standard) và Thuật [toán](https://www.techtarget.com/whatis/definition/algorithm) mã hóa dữ liệu quốc tế ([IDEA](https://www.techtarget.com/searchsecurity/definition/International-Data-Encryption-Algorithm)).

Blowfish nhanh hơn đáng kể so với DES và IDEA và không được cấp bằng sáng chế và có sẵn miễn phí cho tất cả các mục đích sử dụng. Tuy nhiên, nó không thể thay thế hoàn toàn DES do kích thước khối nhỏ, được coi là không an toàn.

[Twofish](https://www.techtarget.com/searchsecurity/definition/Twofish), người kế nhiệm của nó, đã giải quyết vấn đề bảo mật với kích thước khối lớn hơn 128 bit. Tuy nhiên, mã hóa Blowfish đầy đủ chưa bao giờ bị phá vỡ và thuật toán được bao gồm trong nhiều bộ mật mã và các sản phẩm mã hóa có sẵn ngày nay.

### **Ưu điểm của Blowfish :**

Một trong những mật mã khối nhanh nhất và nhỏ gọn nhất được sử dụng công cộng, Blowfish sử dụng khóa mã hóa đối xứng để biến dữ liệu thành bản mã. Gần ba thập kỷ sau khi được phát triển lần đầu tiên, Blowfish vẫn được sử dụng rộng rãi vì nó mang lại những ưu điểm sau:

* Nhanh hơn và hiệu quả hơn nhiều so với các thuật toán DES và IDEA;
* không được cấp bằng sáng chế và có thể được sử dụng tự do bởi bất kỳ ai ngay cả khi không có giấy phép;
* Mặc dù giai đoạn khởi tạo phức tạp trước khi mã hóa, quá trình mã hóa dữ liệu hiệu quả trên các bộ vi xử lý lớn;
* Cung cấp bảo mật mở rộng cho phần mềm và ứng dụng được phát triển bằng [Java](https://www.theserverside.com/definition/Java);
* Cung cấp quyền truy cập an toàn cho các công cụ [sao lưu](https://www.techtarget.com/searchdatabackup/definition/backup)
* Hỗ trợ [xác thực người dùng](https://www.techtarget.com/searchsecurity/definition/user-authentication) an toàn để truy cập từ xa.

### **Nhược điểm của Blowfish :**

Có một số nhược điểm khi sử dụng Blowfish để mã hóa, bao gồm:

* Tốc độ bị ảnh hưởng khi thay đổi phím.
* Lịch trình quan trọng mất nhiều thời gian.
* Kích thước khối nhỏ 64 bit khiến thuật toán dễ bị tấn công sinh nhật, một lớp [tấn công brute-force](https://www.techtarget.com/searchsecurity/definition/brute-force-cracking).
* Mỗi khóa mới yêu cầu xử lý sơ bộ tương đương với 4 KB văn bản, điều này ảnh hưởng đến tốc độ của nó, khiến một số ứng dụng không thể sử dụng được.

### **Ứng dụng của Blowfish :**

Blowfish phù hợp cho một loạt các ứng dụng, bao gồm:

* Mã hóa hàng loạt
* Tạo bit ngẫu nhiên
* Mã hóa gói
* [Băm](https://searchsqlserver.techtarget.com/definition/hashing) và quản lý mật khẩu
* Bộ xử lý di động
* Mã hóa email, tệp hoặc đĩa
* Sao lưu dữ liệu
* [Vỏ bảo mật](https://www.techtarget.com/searchsecurity/definition/Secure-Shell)
* Blowfish được sử dụng bởi nhiều sản phẩm phổ biến, chẳng hạn như CryptoDisk, PasswordWallet, Access Manager, Symantec NetBackup và SplashID. Nhiều nền tảng truyền thông xã hội và trang web thương mại điện tử cũng sử dụng Blowfish để bảo vệ dữ liệu người dùng.

**CHƯƠNG 4 : ỨNG DỤNG CỦA MÃ HÓA DỮ LIỆU**

**Ứng dụng của mã hóa dữ liệu đối với doanh nghiệp**

* Mã hoá dữ liệu đóng vai trò then chốt đối với các doanh nghiệp, đặc biệt là trong thời đại công nghệ số phổ biến như hiện nay. Cụ thể, việc ứng dụng mã hóa dữ liệu sẽ đem lại những lợi ích tuyệt vời sau đây:
* Đảm bảo tất cả những thông tin của doanh nghiệp trên internet đều được bảo mật một cách tuyệt đối.
* Hạn chế thấp nhất nguy cơ bị kẻ xấu tấn công đánh cắp dữ liệu. Điều này không chỉ ảnh hưởng đến kinh tế mà trong trường hợp nghiêm trọng còn liên quan đến pháp luật.
* Chỉ những người được cung cấp thông tin mới có thể truy cập vào tài nguyên dữ liệu, từ đó dễ dàng phân quyền và quản lý nhân sự.
* Các thuật toán sẽ cung cấp cho doanh nghiệp những yếu tố bảo mật then chốt nhằm xác thực và đảm bảo tính nguyên vẹn của dữ liệu trong quá trình trao đổi.
* Trong trường hợp dữ liệu của bạn bị thất lạc hoặc đánh cắp, đối thủ cũng sẽ tốn rất  nhiều thời gian và công sức mới có thể mở khoá được dữ liệu. Đây là thời gian vừa đủ để bạn có thể làm việc với cơ quan chức năng hoặc tìm cách lấy lại trước khi tất cả thông tin bị xâm nhập.

*Mã hoá dữ liệu giúp mọi thông tin của doanh nghiệp được bảo mật*

**ỨNG DỤNG CỦA MÃ HÓA TRONG Y TẾ :**

* Ứng dụng mã hóa dữ liệu trong y tế là một trong những cách để bảo vệ thông tin y tế của bệnh nhân. Mã hóa dữ liệu y tế giúp bảo vệ thông tin cá nhân của bệnh nhân và ngăn chặn việc truy cập trái phép vào thông tin y tế của họ. Ngoài ra, mã hóa dữ liệu y tế cũng giúp cho việc chia sẻ thông tin y tế giữa các bác sĩ và các cơ sở y tế trở nên dễ dàng và an toàn hơn.
* Tuy nhiên, việc áp dụng mã hóa dữ liệu trong y tế cũng đòi hỏi sự chú ý đến các vấn đề liên quan đến quyền riêng tư và an ninh mạng

Các loại mã hóa dữ liệu trong y tế bao gồm:

* Mã số chẩn đoán: được sử dụng để xác định bệnh, rối loạn và các triệu chứng.
* Mã số thủ tục: là những con số hoặc mã chữ và số được sử dụng để xác định các biện pháp can thiệp y tế cụ thể được thực hiện bởi các chuyên gia y tế.
* Mã số dược phẩm.
* Mã địa hình.

ỨNG DỤNG CỦA MÃ HÓA TRONG NGÂN HÀNG ĐIỆN TỬ :



* Trong các ngân hàng điện tử, mã hóa dữ liệu được sử dụng để bảo vệ thông tin của khách hàng. [Các ngân hàng cần mã hóa các dữ liệu, thông tin liên quan đến khách hàng theo các tiêu chuẩn mã hóa như TLS, AES256 khi lưu trữ và giao dịch với khách hàng để bảo vệ dữ liệu](https://digital.fpt.com.vn/linh-vuc/ngan-hang-bao-ve-du-lieu-nguoi-dung-nhu-the-nao.html" \t "_blank)

**CHƯƠNG 5 : KẾT LUẬN**

5.1 Tóm tắt kết quả nghiên cứu

* Qua quá trình nghiên cứu và tìm hiểu về mã hóa dữ liệu và các thuật toán thông dụng cho mình thấy được Mã hoá dữ liệu đóng vai trò vô cùng quan trọng trong việc bảo mật và lưu trữ thông tin đặc biệt là đối với các doanh nghiệp đang thực hiện chuyển đổi số. Tuỳ vào mục đích và nhu cầu khác nhau mà bạn có thể lựa chọn các loại mã hóa dữ liệu khác nhau như: mã hoá đối xứng, bất đối xứng, cổ điển, một chiều.
* Mã hoá dữ liệu sẽ giúp hệ thống của doanh nghiệp được vận hành một cách hiệu quả và an toàn hơn, tránh nguy cơ bị kẻ gian tấn công đánh cắp dữ liệu gây thiệt hại nặng nề cho cả hai bên là doanh nghiệp và khách hàng.
* Hiểu được ưu và nhược điểm của các mã hóa và thuật toán để áp dụng sao cho phù hợp với từng lĩnh vực trong cuộc sống giúp người dung tăng cường nhận thức an toàn thông tin để chủ động bảo vệ thông tin và tài khoản cá nhân
* Hy vọng những thông tin trên đã giúp bạn hiểu hơn mã hóa dữ liệu là gì, các loại mã hóa dữ liệu phổ biến và những lợi ích mà mã hóa dữ liệu mang lại không chỉ cho cá nhân mà có cả doanh nghiệp. Chúc các bạn đã có thêm nhiều thông tin hữu ích và hẹn gặp lại trong những bài thuyết trình sắp tới.
* 5.1 Những phương hướng phát triển của mã hóa dữ liệu
* Mã hóa dữ liệu là một trong những phương pháp bảo mật đang được sử dụng phổ biến nhất hiện nay. [Đặc biệt trong thời đại công nghệ số ngày càng phát triển mạnh mẽ, các doanh nghiệp hoạt động kinh doanh đều coi bảo mật thông tin chính là tiêu chí ưu tiên hàng đầu cần được thực hiện](https://bizfly.vn/techblog/ma-hoa-du-lieu.html" \t "_blank)[**1**](https://bizfly.vn/techblog/ma-hoa-du-lieu.html).

Các phương hướng phát triển của mã hóa dữ liệu bao gồm :

* Mã hóa đa chế độ (Multiple modes of operation)
* Mã hóa đa khối (Multiple block cipher)
* Mã hóa đa khóa (Multiple key cipher)
* Mã hóa đa chức năng (Multiple function cipher)
* Mã hóa đa bản (Multiple version cipher)
* Mã hóa đa cấu trúc (Multiple structure cipher)
* Mã hóa đa kích thước khối (Multiple block size cipher)

TÀI LIỆU THAM KHẢO

* DƯỚI ĐÂY LÀ 1 SỐ TÀI LIỆU THAM KHẢO BỔ SUNG VỀ NGHIÊN CỨU MÃ HÓA DỮ LIỆU VÀ CÁC THUẬT TOÁN MÃ HÓA :

TÀI LIỆU 1 : [Mã hóa dữ liệu là gì? 4 loại mã hoá dữ liệu phổ biến (sapo.vn)](https://www.sapo.vn/blog/ma-hoa-du-lieu)

TÀI LIỆU 2 : [[Kiến thức cơ bản] Mã hoá là gì, những thông tin đầy đủ về mã hóa (techsignin.com)](https://www.techsignin.com/khai-niem-ve-ma-hoa/)

TÀI LIỆU 3: Cuốn sách Môn học An Toàn Bảo Mật Thông Tin ( hiện có ở thư viện Trường ĐH Lâm Nghiệp)

TÀI LIỆU 4 : [Mã hóa dữ liệu là gì? Lợi ích mã hóa dữ liệu vào thực tế mà bạn phải biết! (onetel.com.vn)](https://onetel.com.vn/ma-hoa-du-lieu/)