**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG TP HỒ CHÍ MINH**

**KHOA CÔNG NGHỆ THÔNG TIN**



----o0o----

**HỌC PHẦN: MẬT MÃ HỌC**

**ĐỀ TÀI: THUẬT TOÁN MÃ HÓA CAESER**

|  |  |
| --- | --- |
| **DANH SÁCH THÀNH VIÊN NHÓM 3** | |
| Họ và Tên | MSSV |
| Lý Tiến Đạt (NT) | 2033216386 |
| Lê Quốc Anh | 2033216341 |

**GVHD: Phạm Tuấn Khiêm**

*Tp.HCM Ngày 01 tháng 10 năm 2024*

**LỜI CAM ĐOAN**

Nhóm chúng em xin cam đoan đây là bài báo cáo đồ án của nhóm chúng em. Các số liệu, kết quả bên trong “Bài báo cáo tiểu luận” điều là trung thực và rõ ràng.

Chúng em xin cam đoan rằng mọi sự giúp đỡ cho việc thực hiện “Bài báo cáo tiểu luận” này đã được cảm ơn và các thông tin được trích dẫn trong báo cáo đã được chỉ rõ nguồn gốc.

## Nhóm sinh viên thực hiện Báo cáo

*(Đã ký và và ghi rõ họ tên)*

**LỜI CẢM ƠN**

Qua một thời gian nghiên cứu, phân công công việc và tiến hành thực hiện đến nay, đề tài “Thuật toán mã hóa Caeser” đã hoàn thành. Chúng em xin chân thành cảm các thầy cô đã trang bị kiến thức quý báu cho chúng em trong suốt quá trình học. Đặc biệt là các thầy các cô trong khoa Công nghệ thông tin đã tận tình giảng dạy, chỉ bảo, trang bị cho chúng em những kiến thức cần thiết nhất trong suốt quá trình học tập và nghiên cứu tại khoa, đã tạo mọi điều kiện thuận lợi giúp chúng em.

Chúng em cũng đặc biệt xin chân thành cảm ơn giảng viên Phạm Tuấn Khiêm đã tận tình giảng dạy và hướng dẫn chúng em hoàn thành tốt đề tài này và một thành phần không thể thiếu được chính là sự nỗ lực của các thành viên trong nhóm.

Trong quá trình thực hiện đề tài, chúng em không tránh khỏi những thiếu xót cũng như những hạn chế nhất định. Chúng em mong nhận được sự đóng góp ý kiến, chỉ bảo tận tình của thầy và các bạn để đề tài của chúng em hoàn thiện hơn và thiết thực hơn.

**MỤC LỤC**

[LỜI CẢM ƠN 2](#_Toc32308)

[I. PHẦN MỞ ĐẦU 4](#_Toc15892)

[A. GIỚI THIỆU VỀ ĐỀ TÀI 4](#_Toc14577)

[B. LÝ DO CHỌN ĐỀ TÀI 5](#_Toc19023)

[C. LỊCH SỬ RA ĐỜI CỦA THUẬT TOÁN CAESAR 6](#_Toc15361)

[II. PHẦN NỘI DUNG TỔNG QUAN CHUNG 7](#_Toc12924)

[A. GIỚI THIỆU VỀ MÃ HÓA VÀ LỢI ÍCH CỦA MÃ HÓA. 7](#_Toc30088)

[1. Giới thiệu về mã hóa: 7](#_Toc23897)

[2. Lợi ích của mã hóa đem lại: 8](#_Toc26040)

[B. TỔNG QUAN VỀ THUẬT TOÁN MÃ HÓA CAESAR 12](#_Toc21784)

[1. Khái niệm cơ bản về thuật toán Caesar 12](#_Toc21937)

[2. Phương pháp mã hóa Caesar: 14](#_Toc28454)

[3. Ưu điểm và nhược điểm: 14](#_Toc31419)

[4. Ứng dụng và tác động của thuật toán Caesar 15](#_Toc4881)

[III. PHẦN THỰC NGHIỆM 18](#_Toc4099)

[A. XÂY DỰNG WEBSITE MÃ HÓA VÀ GIẢI MÃ THUẬT TOÁN CAESAR 18](#_Toc8640)

[1. Mã hóa của thuật toán Caesar 18](#_Toc891)

[2. Giải mã của thuật toán Caesar 18](#_Toc18274)

[3. Website minh họa thuật toán Caesar 19](#_Toc30358)

[4. Đẩy website ra Internet 20](#_Toc30358)

[IV. TÀI LIỆU KHAM THẢO 22](#_Toc5553)

## PHẦN MỞ ĐẦU

### GIỚI THIỆU VỀ ĐỀ TÀI

- Sự phát triển nhanh chóng của internet đã tác động đến cả công việc kinh doanh và tiêu dùng với sự hứa hẹn về việc thay đổi cách mà con người sống và làm việc. Nhưng mối lo ngại lớn nhất được đề cập đến là việc bảo mật trên Internet, đặc biệt là khi các thông tin mang tính nhạy cảm được gửi đi trên mạng xã hội. Quá trính mã hóa trong máy tính dựa vào khoa học mật mã (Cyptography) đã được con người sử dụng từ lâu đời. Trước thời đại số hóa, người sử dụng mật mã nhiều nhất vẫn là chính phủ, chủ yếu là trong mục đích quân sự. Hầu hết các phương pháp mã hóa hiện nay là dựa vào các máy tính, đơn giản là do các mã do con người sinh ra rất dễ bị phá hủy bởi các công cụ máy tính.

- Ứng dụng của khoa học mật mã không chỉ đơn thuần là mã hóa và giải mã những thông tin bao gồm nhiều vấn đề khác cần được nghiên cứu và giải quyết như chứng thực nguồn gốc nội dung thông tin(kỹ thuật chữ ký số), chứng nhận xác thực về người sở hữu mã hóa(chứng nhận khóa công cộng), các quy trình trao đổi thông tin và thực hiện giao dịch điện tử trên an toàn trên mạng.

- Bảo mật thông tin luôn đóng vai trò vô cùng quan trọng, đặc biệt trong việc bảo vệ các thông điệp nhạy cảm khỏi các mối đe dọa bên ngoài. Từ thời cổ đại đến kỷ nguyên số hiện nay, nhu cầu về các phương pháp mã hóa và giải mã thông tin để bảo vệ dữ liệu đã trở nên cấp thiết. Một trong những thuật toán mã hóa cổ điển và đơn giản nhất là thuật toán Caesar, được đặt theo tên của Julius Caesar, người đã sử dụng nó để mã hóa các thông điệp quân sự, nhằm bảo mật thông tin chiến lược khỏi tay kẻ thù.

- Thuật toán Caesar, dù rất đơn giản, đã đặt nền móng cho sự phát triển của các thuật toán mã hóa hiện đại. Với cơ chế dịch chuyển các ký tự trong bản rõ dựa trên một khoảng dịch nhất định, thuật toán này là công cụ mạnh mẽ trong thời đại của Caesar. Mục tiêu nghiên cứu của tiểu luận này là tìm hiểu chi tiết nguyên lý hoạt động của thuật toán Caesar, phân tích các ưu nhược điểm của nó, và khám phá ứng dụng của thuật toán trong lĩnh vực mật mã học, cả trong lịch sử và hiện nay.

### LÝ DO CHỌN ĐỀ TÀI

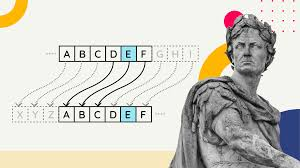
Thuật toán Caesar là một trong những thuật toán mã hóa cổ điển và đơn giản nhất, nhưng nó đã đặt nền móng quan trọng cho sự phát triển của các phương pháp mã hóa hiện đại. Dù không còn được sử dụng rộng rãi trong môi trường bảo mật thông tin ngày nay, nhưng việc nghiên cứu và hiểu rõ thuật toán Caesar giúp cung cấp cái nhìn sâu sắc về cách thức hoạt động cơ bản của mã hóa đối xứng.

Nghiên cứu thuật toán Caesar giúp người học làm quen với những nguyên lý cốt lõi của mật mã học, như mã hóa, giải mã, và cách thông tin được bảo vệ trước các cuộc tấn công. Đề tài này không chỉ giúp tiếp cận các khái niệm căn bản trong lĩnh vực bảo mật thông tin mà còn làm rõ vai trò lịch sử của các phương pháp mã hóa đơn giản, từ đó xây dựng nền tảng để hiểu rõ hơn về các thuật toán phức tạp hơn được sử dụng trong thế giới số hiện nay.

Nó cho tính an toàn khi truyền dữ liệu. Gửi dữ liệu cá nhân không chỉ gặp rủi ro khi được truyền qua Internet. Mặc dù đã cố gắng hết sức, nhưng vẫn có khả năng máy tính bị nhiễm phần mềm độc hại mà phần mềm diệt vi-rút không bắt được. Nếu đúng như vậy, phần mềm độc hại có thể bắt đầu tìm kiếm dữ liệu nhạy cảm trên máy tính của bạn và gửi nó cho tội phạm mạng đang chạy phần mềm độc hại. Vậy nên việc chúng ta mã hóa các ký tự bằng ceasar giúp bảo mật thông tin 1 cách triệt để.

### LỊCH SỬ RA ĐỜI CỦA THUẬT TOÁN CAESAR

Thuật toán Caesar, hay còn gọi là Caesar Cipher, xuất hiện từ thời La Mã cổ đại và được đặt theo tên của Julius Caesar, nhà lãnh đạo quân sự và chính trị nổi tiếng. Caesar sử dụng thuật toán này để bảo vệ các thông điệp quân sự quan trọng, nhằm tránh rơi vào tay kẻ thù trong các chiến dịch của ông. Với mục tiêu giữ bí mật thông tin trên chiến trường, Caesar đã phát minh ra phương pháp dịch chuyển mỗi ký tự trong bản rõ theo một khoảng nhất định trong bảng chữ cái, thường là dịch 3 vị trí. Mặc dù đơn giản, nhưng thuật toán này đã giúp bảo vệ các thông điệp quan trọng khỏi bị kẻ thù giải mã. Đây được coi là một trong những hệ thống mã hóa cổ xưa đầu tiên, tạo tiền đề cho sự phát triển của các kỹ thuật mã hóa phức tạp hơn sau này.



## PHẦN NỘI DUNG TỔNG QUAN CHUNG

### GIỚI THIỆU VỀ MÃ HÓA VÀ LỢI ÍCH CỦA MÃ HÓA.

#### Giới thiệu về mã hóa:

- Mã hóa là cách xáo trộn dữ liệu chỉ để hai bên trao đổi thông tin có thể hiểu được. Về mặt kỹ thuật, đó là quá trình chuyển đổi văn bản gốc sang bản mã. Nói một cách đơn giản hơn, mã hóa lấy dữ liệu có thể đọc được và thay đổi nó để đữ liệu này không giống như ban đầu. Mã hóa yêu cầu sử dụng khỏa mã hóa: một tập hợp các giá trị toán học mà cả người gửi và người nhận tin nhắn được mã hóa đều biết. Mặc dù dữ liệu được mã hóa xuất hiện ngẫu nhiên, mã hóa tiến hành theo cách hợp lý, có thể dự đoán được, để bên nhận sử dụng khóa để mã hóa dữ liệu, biến nó trở lại thành bản dữ liệu ban đầu.



Mã hóa an toàn thực sự sẽ đủ phức tạp để bên thứ ba không thể giải mã được bằng brute force, nói cách khác, bằng cách đoán. Dữ liệu có thể được mã hóa “ở trạng thái nghỉ”, khi nó được lưu trữ hoặc “quá cảnh” trong khi nó đang được truyền đi nơi khác.

#### Lợi ích của mã hóa đem lại:

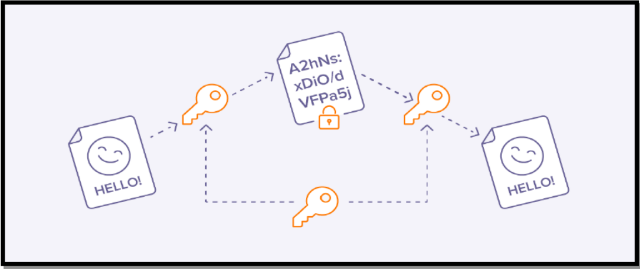
- Các doanh nghiệp đã đầu tư vào hệ thống phát hiện và tường lửa bảo mật CNTT chu vi truyền thống đang tiếp tục tìm kiếm thêm thứ gì đó để bảo vệ dữ liệu của họ. Giữa tin tặc bên ngoài và nhân viên nội bộ, bảo vệ dữ liệu ở tất cả các trạng thái là nhiệm vụ quá cao đối với hầu hết các giải pháp cũ. Để chống lại xu hướng này, các doanh nghiệp đang xem xét việc bảo vệ dữ liệu và cụ thể là các giải pháp mã hóa dữ liệu là giải pháp triển khai tiếp theo của họ. Encryption có thể là một lựa chọn tuyệt vời cho các doanh nghiệp đang chuyển một lượng lớn dữ liệu và muốn chắc chắn rằng họ có thể giữ an toàn cho bản thân khỏi bị đánh cắp dữ liệu tiềm ẩn. Các vấn đề với các giải pháp mã hóa quá nặng hoặc ảnh hưởng tiêu cực đến trải nghiệm người dùng một cách tiêu cực giờ đã là quá khứ.

- Vi phạm dữ liệu là một vấn đề thực sự đối với các doanh nghiệp thuộc mọi quy mô, mặc dù nhiều doanh nghiệp nhỏ hơn đã lầm tưởng rằng đó là một vấn đề chủ yếu ảnh hưởng đến các thương hiệu lớn hơn. Có rất nhiều lợi ích mà mã hóa có thể mang lại cho công ty của bạn, ngoài những lợi ích mà bạn có thể đã nghi ngờ. Nếu bạn đang xem xét mã hóa cho doanh nghiệp của mình, bạn nên tỉnh đến những lợi ích này trước khi đưa ra quyết định của mình.



#### 2.1 Bảo vệ dữ liệu hoàn chỉnh

- Một giải pháp mã hóa hoàn chỉnh cung cấp cho các doanh nghiệp và chủ sở hữu của họ sự an tâm vì nó bảo vệ dữ liệu ở mọi trạng thái - ở trạng thái nghỉ và khi đang chuyển. Mặc dù các giải pháp bảo mật ngoại vi có thể khiến việc truy cập dữ liệu từ bên ngoài trở nên khó khăn hơn, nhưng một khi mạng bị xâm phạm, dữ liệu của bạn chỉ an toàn như mã hóa dữ liệu mà bạn sử dụng. Với giải pháp mã hóa phù hợp, bạn có thể trải qua mỗi ngày khi biết rằng dữ liệu của minh an toàn và không có cách nào hợp lý mà tin tặc có thể có được trong tay dữ liệu thô. Tôi sẽ không sử dụng một chương trình kiểu brute-force hơn cả đời để giải mã thành công tất cả thông tin.



- Mặc dù có những phương tiện khác mà dữ liệu có thể bị truy cập, nhưng thực hiện một bước đơn giản để mã hóa sẽ giúp làm cho công việc trở nên quá khó khăn đối với những tin tặc thường quan tâm đến việc nhắm mục tiêu doanh nghiệp của bạn.

#### 2.2. Bảo mật trên nhiều thiết bị

- Với việc điện thoại thông minh và các thiết bị di động khác trở nên phổ biển trong những năm gần đây, nhiều công ty đã phải vật lộn để tìm ra giải pháp giữ cho dữ liệu được lưu trữ và truyền qua các thiết bị này an toàn trước khả năng bị đánh cắp. May mắn thay, phần mềm mã hóa dữ liệu sẽ cho phép bạn đảm bảo rằng tất cả dữ liệu, trên bất kỳ thiết bị nào, đều được mã hóa hoàn toàn với các biện pháp bảo vệ tương tự như bạn sẽ tìm thấy trong dữ liệu được lưu trữ trên máy tính để bàn. Mã hóa dữ liệu sẽ giúp xử lý một tình huống căng thẳng, không thể tránh khỏi và giúp nó có thể kiểm soát được, đồng thời mang lại sự yên tâm. Trên hết, xác thực thiết bị có thể loại bỏ nguy cơ xâm nhập từ những người dùng không mong muốn.



#### 2.3. Di chuyển dữ liệu một cách an toàn

- Một trong những khía cạnh dễ bị tấn công nhất của dữ liệu xuất hiện trong quá trình vận chuyển. Mặc dù SSL / TLS là tiêu chuẩn công nghiệp cho dữ liệu đang chuyển động, nó có nhiều nhược điểm đối với bảo mật dữ liệu của bạn. Một giải pháp mã hóa hiệu quả giúp đảm bảo rằng dữ liệu được bảo vệ mọi lúc, mọi nơi và chuyển động. Các tệp được chia sẻ hoặc tải lên hệ thống đám mây phải đảm bảo rằng các tệp vẫn an toàn trong suốt quá trình vận chuyển.

#### 2.4. Tính toàn vẹn được duy trì

- Một trong những lo lắng mà nhiều tổ chức thuộc mọi quy mô đều chia sẻ là liệu quá trình mã hóa có ảnh hưởng đến tính toàn vẹn của dữ liệu của họ hay không. Mặc dù đánh cắp dữ liệu là một vấn đề rất phổ biến, nhưng một cách khác để tin tặc thực hiện hành vi gian lận dữ liệu là làm thay đổi dữ liệu có sẵn. Mã hóa giữ cho dữ liệu của bạn an toàn không bị thay đổi và người nhận dữ liệu sẽ có thể xem liệu nó có bị giả mạo hay không. Thay đổi dữ liệu là điều mà các doanh nghiệp thường bỏ qua khi họ đang tìm cách giữ an toàn cho dữ liệu của mình.

- Bảo vệ dữ liệu cơ bản là hoàn toàn cần thiết cho doanh nghiệp của bạn. Đối với những người muốn thực hiện bước tiếp theo hoặc đang khôi phục sau sự cố đánh cắp dữ liệu của chính họ, mã hóa là một trong những phương pháp tốt nhất để đảm bảo rằng dữ liệu của bạn vẫn an toàn. Nó cho phép bạn đạt được bảo mật hoàn toàn trên tất cả các thiết bị, gửi và nhận dữ liệu một cách an toàn và đảm bảo tính toàn vẹn tuyệt đối, bất cứ khi nào tệp được truy cập hoặc chia sẻ. Nếu bạn quan tâm đến việc bảo vệ doanh nghiệp của mình khỏi tác động của việc vi phạm dữ liệu, thì phần mềm mã hóa là một khoa đầu tư tuyệt vời.

### TỔNG QUAN VỀ THUẬT TOÁN MÃ HÓA CAESAR

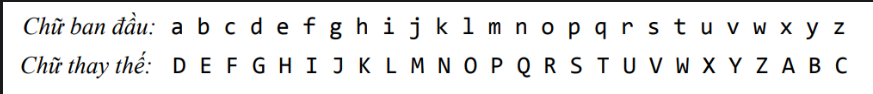
#### Khái niệm cơ bản về thuật toán Caesar

Trong mật mã học, mật mã Caesar (Xê da), còn gọi là mật mã dịch chuyển, là một trong những mật mã đối xứng đơn giản và được biết đến nhiều nhất. Hệ mã Caesar là một hệ mã hóa thay thế đơn âm, làm việc trên bẳng chữ cái tiếng Anh 26 ký tự. Đó là một dạng của mật mã thay thế, trong đó mỗi ký tự trong văn bản được thay thế bằng một ký tự cách nó một đoạn trong bảng chữ cái để tạo thành bản mã.

**Ví dụ về mật mã Caesar:**

Mã hoá caesar bằng cách thay thế các ký tự trong bản rõ bằng ký tự đứng sau nó k vị trí trong bảng chữ cái.

***Giả sử k=3***, ta có bảng chuyển đổi như sau:



Đối với bảng mã tiếng anh (ABCDEFGHI...), nếu độ dịch là 3, A sẽ được thay bằng D, B sẽ được thay bằng E, ..., W sẽ thay bằng Z, X sẽ thay bằng A, Y sẽ thay bằng B và Z thay bằng C. Phương pháp được đặt tên theo Caesar, vị hoàng đế đã sử dụng nó thường xuyên trong công việc. Không gian bản rõ P là các từ cần được mà hóa được tạo từ bảng chữ cái A. Không gian bản rỏ C là các từ đã được mã hóa.

**Trong đó:** N = 26 nếu hệ mã Caesar sử dụng trên bảng chữ cái tiếng Anh (nếu sử dụng trên bảng chữ cái khác thì N sẽ thay đổi). k : tương ứng với số thứ tự chữ cái trong bảng mã (ví dụ : a = 0, b = 1 ....)

Ta có bản rõ: **TOIYEUVIETNAM**

Như vậy, bản mã chiếu theo bảng chuyển đổi kia nếu k = 3 sẽ là:

**WRLBHXYLHWQDP**

Để giải mã, ta thực hiện ngược lại bằng cách chuyển dịch từng kí tự của bản mã lùi về k vị trí.

***Còn nếu k = 4***:

Bản rõ : **TOIYEUVIETNAM** Khóa **k = 4**



Vậy bản mã là : **YSMBYZWMIYREQ**

Quá trình giải mã thì ngược lại với quá trình mã hóa.

#### Phương pháp mã hóa Caesar:

Phương pháp mã hoá Ceasar được biểu diễn như sau:

Sơ đồ hệ mật mã: S=(P,C,K,E,D).

Trong đó P=C=K=Z26, với mỗi khoá k∈K hàm mã hoá một ký tự xi∈P và hàm giải mã một ký tự yi∈C xác định theo công thức:

**Mã hoá**: **yi=eK(xi)=(xi+k)(modn) (n=26)**

**Giải mã**: **xi=dK(yi)=(yi−k)(modn) (n=26)**

#### Ưu điểm và nhược điểm:

*Ưu điểm:*

* Đơn giản, dễ hiểu, dễ triển khai: Thuật toán Caesar có cấu trúc rất đơn giản, chỉ dựa vào việc dịch chuyển các ký tự trong bảng chữ cái. Điều này giúp cho thuật toán dễ dàng được hiểu và triển khai mà không cần đến kiến thức chuyên sâu về toán học hay công nghệ.
* Phù hợp cho mục đích giáo dục và nghiên cứu cơ bản về mật mã học: Caesar Cipher thường được sử dụng như một công cụ giảng dạy để minh họa các nguyên lý cơ bản của mã hóa và bảo mật thông tin. Các sinh viên và người mới bắt đầu có thể học được khái niệm mã hóa đối xứng thông qua thuật toán này.

*Nhược điểm:*

* Bảo mật yếu, dễ bị tấn công bằng brute force: Vì chỉ có 25 khóa dịch chuyển có thể sử dụng (trong bảng chữ cái 26 chữ cái), thuật toán Caesar rất dễ bị phá vỡ bằng phương pháp brute force, tức là thử tất cả các khóa dịch chuyển có thể để giải mã thông điệp.
* Dễ bị phá vỡ bằng phân tích tần suất: Trong các ngôn ngữ tự nhiên như tiếng Anh, tần suất xuất hiện của các chữ cái thường không đồng đều. Ví dụ, chữ "E" là chữ cái xuất hiện nhiều nhất. Kẻ tấn công có thể dựa vào sự phân bố tần suất của các chữ cái để đoán khóa dịch chuyển và giải mã thông điệp, đặc biệt khi bản mã chứa một lượng lớn văn bản.

#### Ứng dụng và tác động của thuật toán Caesar

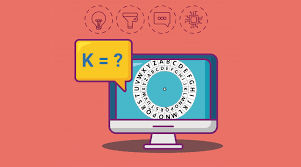
*Ứng dụng trong lịch sử:*

* Caesar Cipher trong quân sự cổ đại: Julius Caesar đã sử dụng thuật toán này để mã hóa các thông điệp quân sự, nhằm ngăn chặn kẻ thù dễ dàng đọc được những thông tin quan trọng trong chiến trận. Nhờ vào sự dịch chuyển các ký tự trong thông điệp, chỉ những người nắm rõ khóa mã hóa mới có thể giải mã và hiểu được nội dung thông tin, điều này giúp đảm bảo an toàn cho các chiến lược quân sự của Caesar.
* Mật mã học cổ đại: Sau thời của Julius Caesar, thuật toán này tiếp tục được sử dụng bởi các nền văn minh cổ đại khác cho các mục đích tương tự, như truyền thông tin mật, đặc biệt trong bối cảnh các chiến tranh và liên lạc chiến lược. Mặc dù thuật toán rất đơn giản, nó là một trong những cách tiếp cận đầu tiên trong việc mã hóa thông tin.



*Tác động đến sự phát triển của mật mã học:*

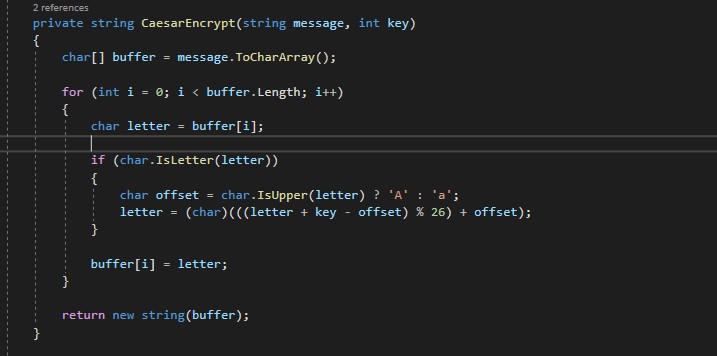
* Ảnh hưởng đến các phương pháp mã hóa thay thế: Caesar Cipher là một trong những thuật toán đầu tiên thuộc nhóm mã hóa thay thế, nơi các ký tự trong bản rõ được thay thế bằng các ký tự khác theo quy luật nhất định. Thuật toán này đã đặt nền tảng cho sự phát triển của các phương pháp mã hóa thay thế phức tạp hơn như Vigenère Cipher hay Playfair Cipher, giúp tăng cường bảo mật.
* Nền tảng cho các thuật toán mã hóa hiện đại: Mặc dù Caesar Cipher không còn được sử dụng rộng rãi trong các hệ thống bảo mật hiện đại do tính bảo mật thấp, nhưng nó đã giúp giới thiệu các nguyên tắc cơ bản của mã hóa và giải mã đối xứng. Điều này trở thành tiền đề để phát triển các thuật toán mã hóa mạnh mẽ hơn, như AES (Advanced Encryption Standard) hay DES (Data Encryption Standard), những phương pháp mã hóa được sử dụng phổ biến trong thời đại kỹ thuật số hiện nay.



## PHẦN THỰC NGHIỆM

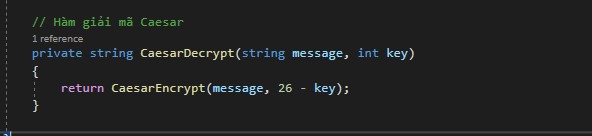
### XÂY DỰNG WEBSITE MÃ HÓA VÀ GIẢI MÃ THUẬT TOÁN CAESAR

#### Mã hóa của thuật toán Caesar



Hàm mã hóa này sẽ nhận một chuỗi đầu vào và một giá trị khóa. Tiếp theo nó chuyển toàn bộ chuỗi thành một mảng các ký tự, kiểm tra xem có kí tự nào là số hay không (nếu là số thì giữ nguyên)  
Xác định chữ cái là chữ hoa hay thường sau đó tính toán vị trí của chữ cái đó dựa theo bảng mã ASCII và chuyển chúng lại thành chuỗi

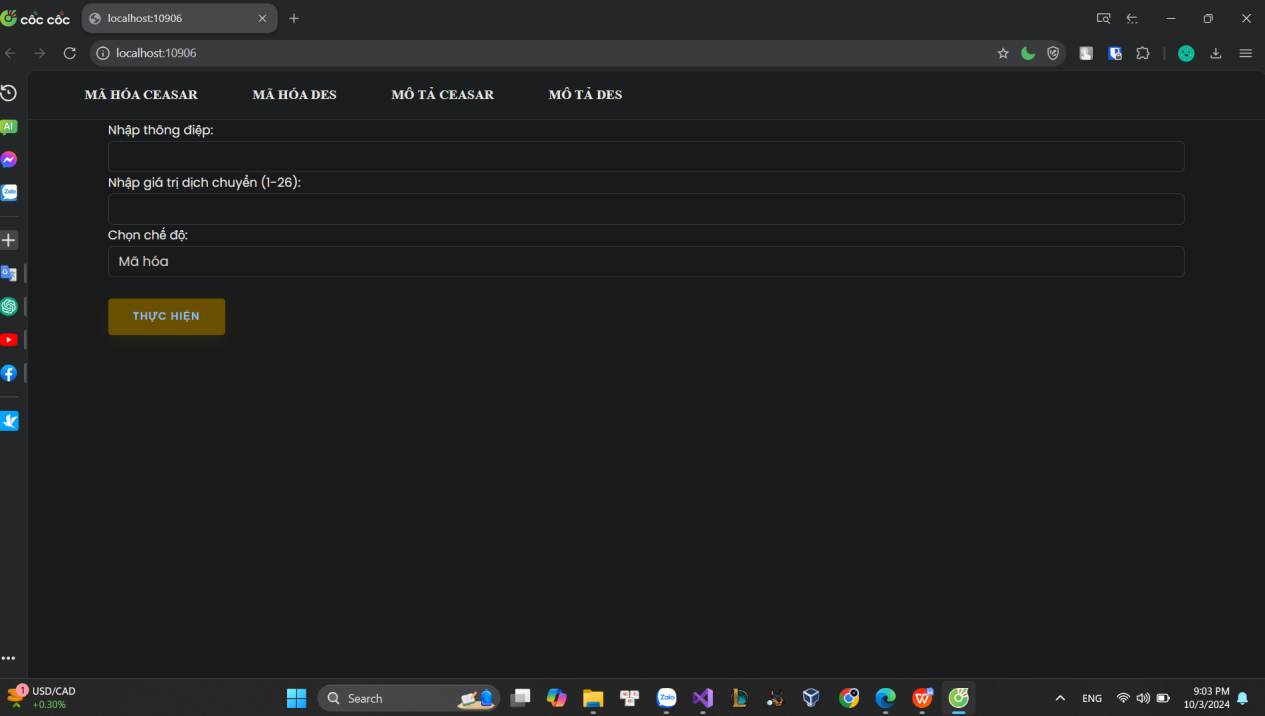
#### Giải mã của thuật toán Caesar



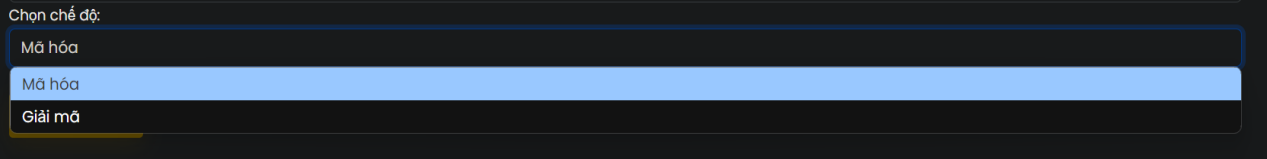
Hiểu đơn giản hàm mã hóa này sẽ lấy vị trí hiện tại của ký tự trừ đi giá trị khóa để quay lại giá trị ban đầu

#### Website minh họa thuật toán Caesar

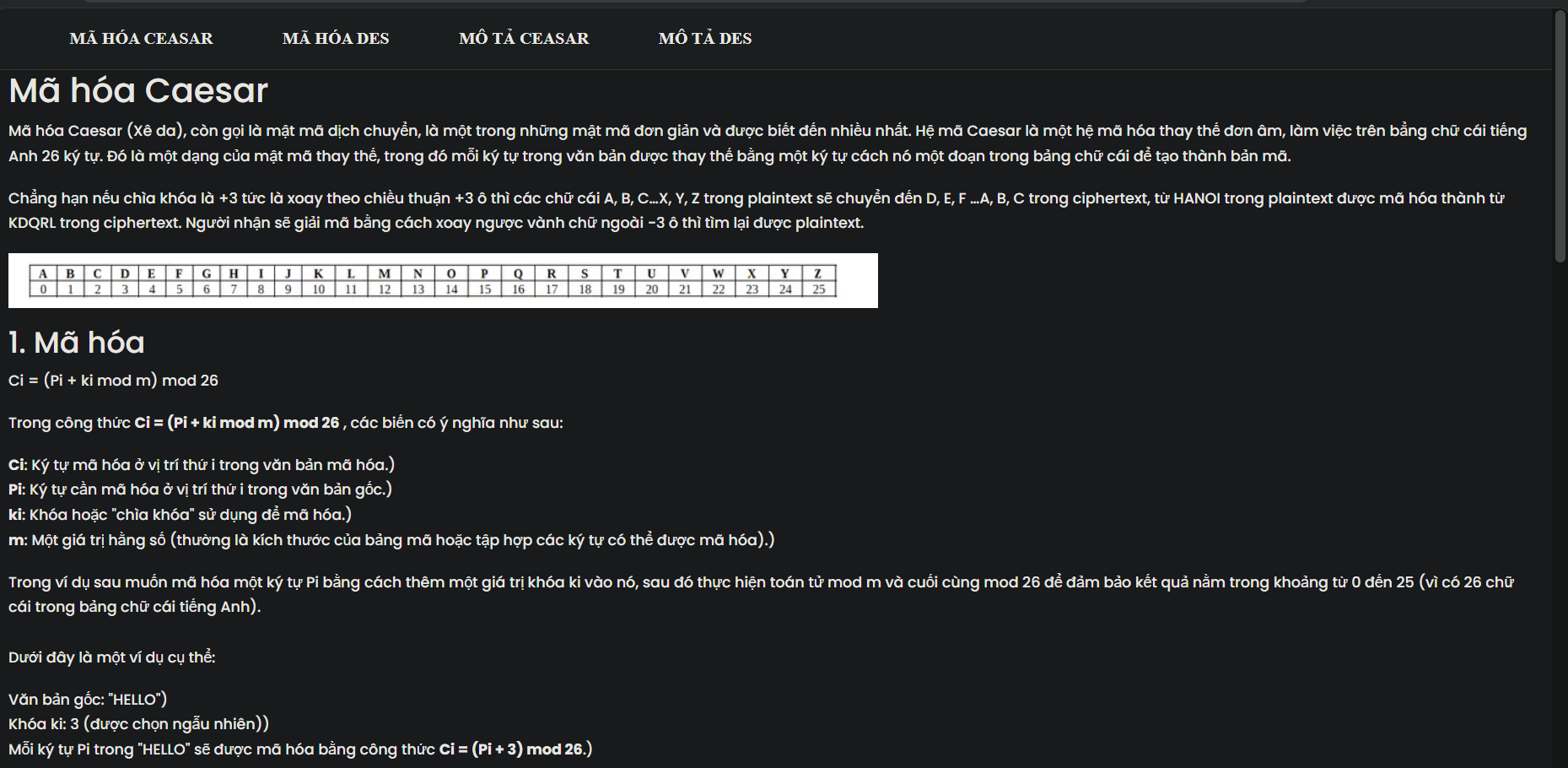
Trang chủ của website



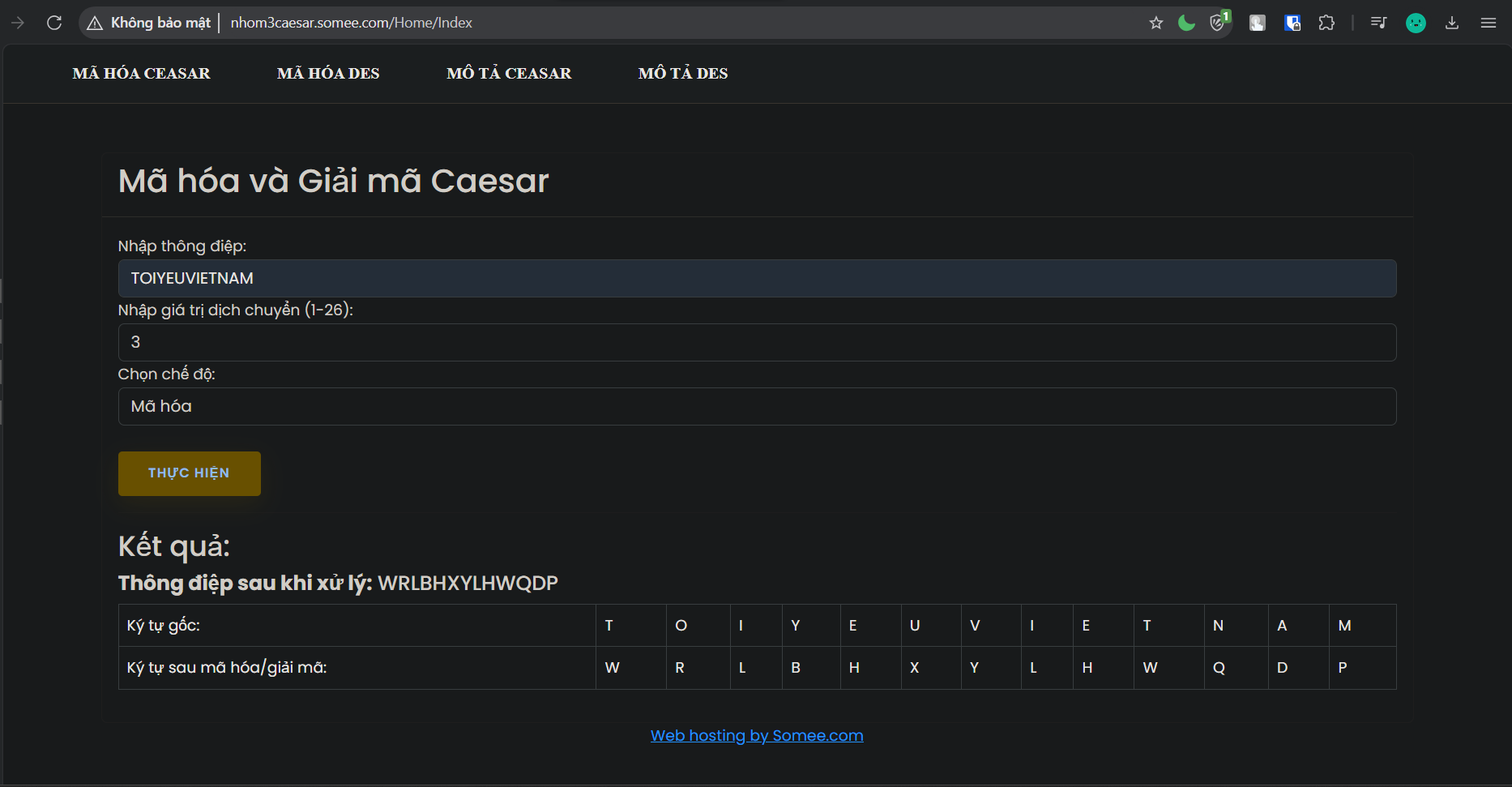
Chọn chế độ thực hiện

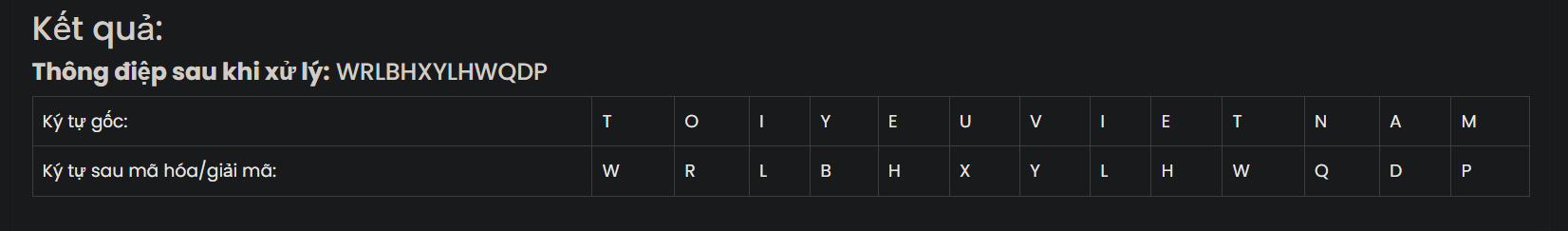


Mô tả thuật toán Caesar tại website

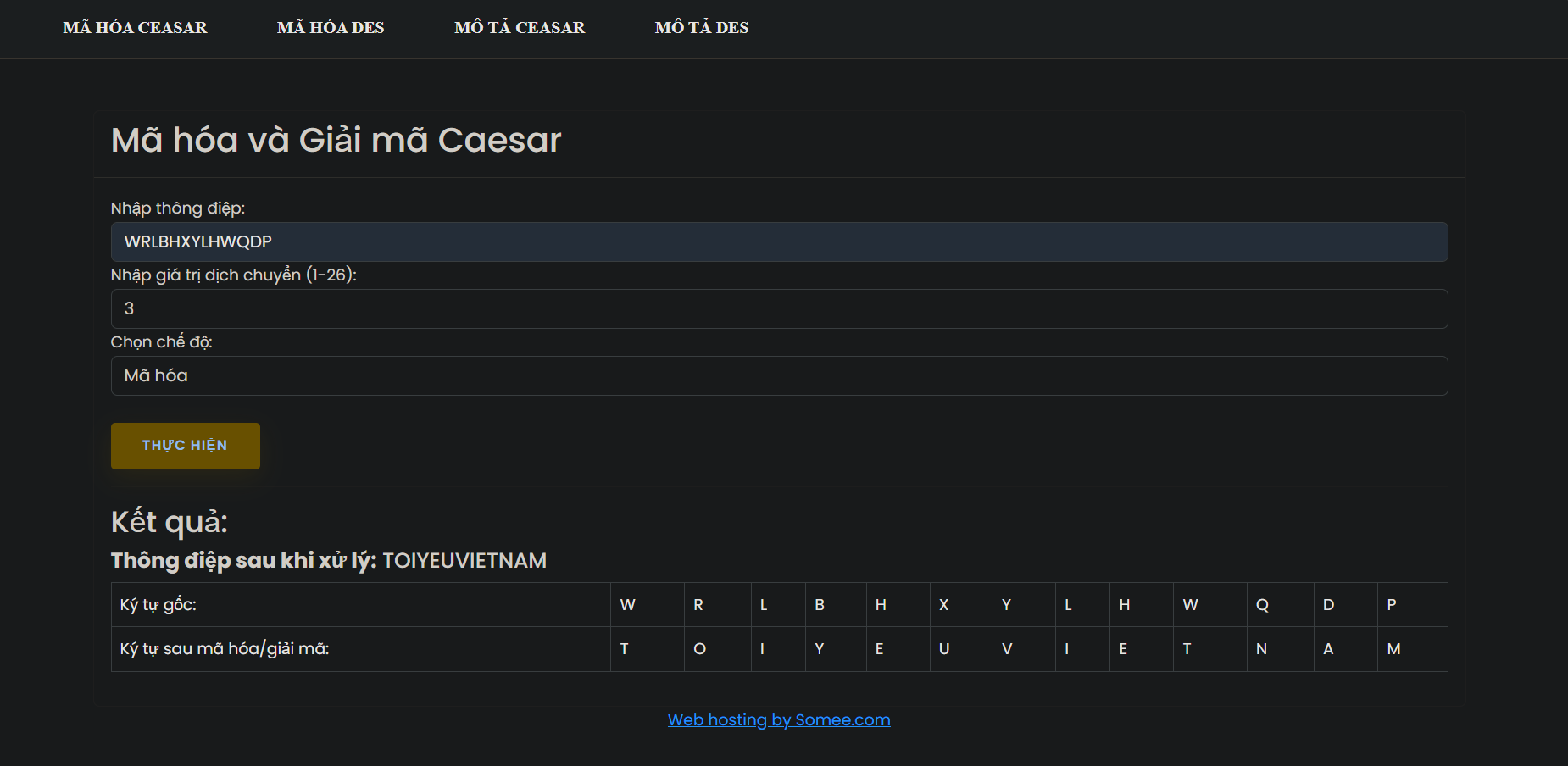


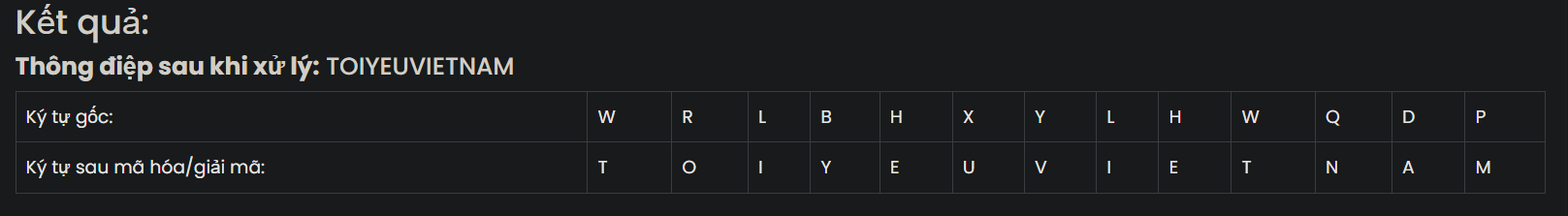
Mã hóa thông điệp





Giải mã thông điệp



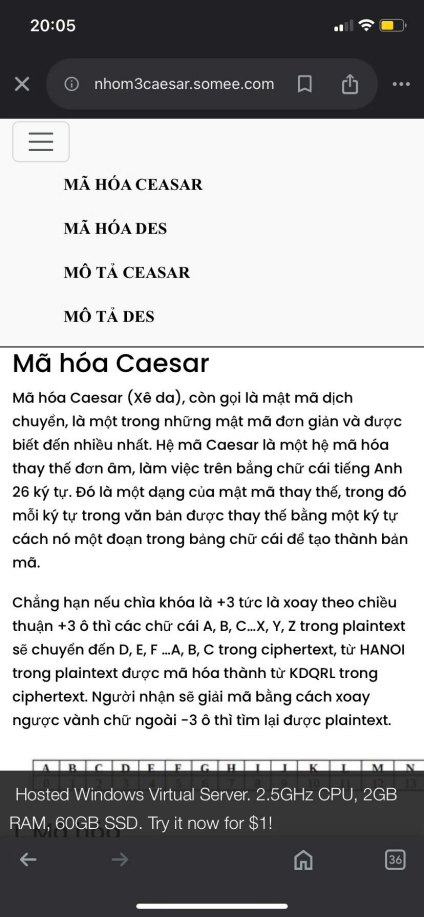


Hoàn thành

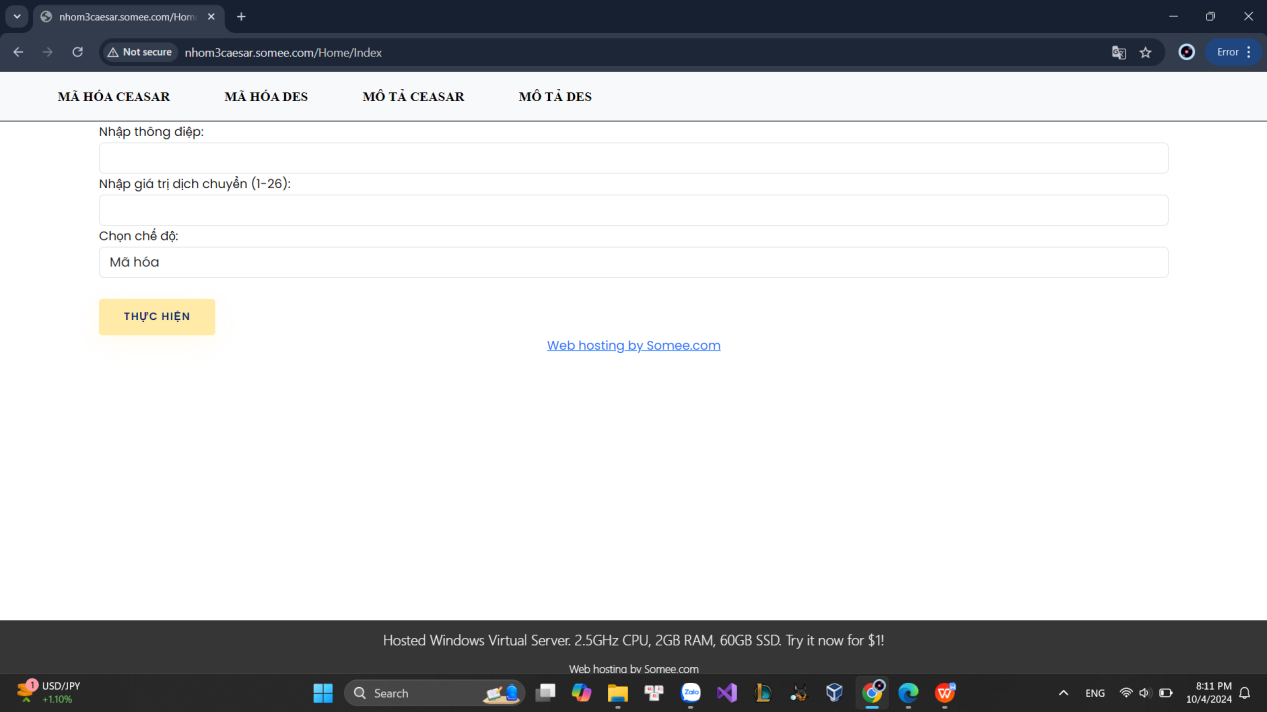
#### Đẩy website ra Internet:

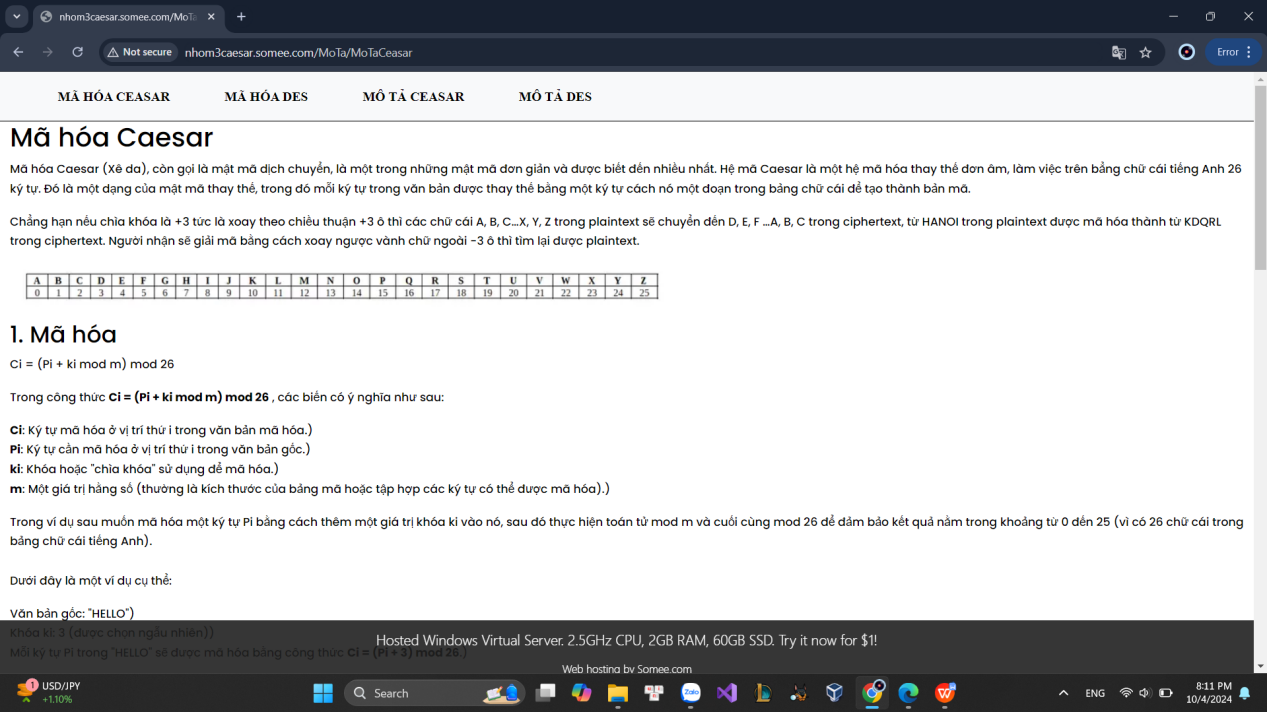
Giao diện trên điện thoại

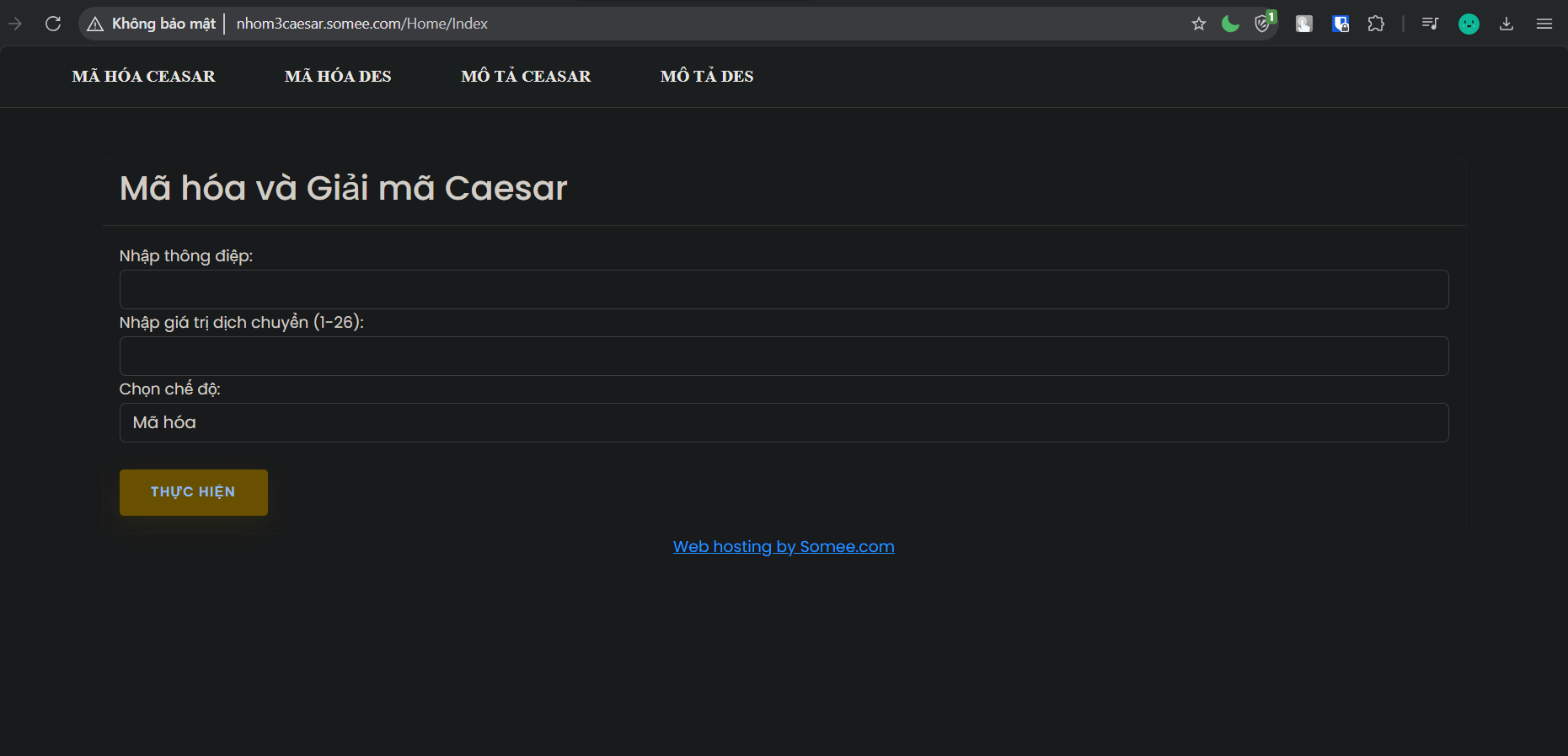




Giao diện trên máy tính:







Link website: <http://nhom3caesar.somee.com/>

## TÀI LIỆU KHAM THẢO

* *Sách Mật Mã Học Trường Đại Học Công Thương*
* *Schneier, Bruce. "Applied Cryptography." John Wiley & Sons, 1996.*
* *Stallings, William. "Cryptography and Network Security." Pearson, 2017.*
* *Singh, Simon. "The Code Book." Fourth Estate, 1999.*
* *<https://www.youtube.com/watch?v=Wkj-FO47yNY>*