# Lab 8: Mã hóa đối xứng

## Mục tiêu

**Phần 1: Vigenère Cipher**

Sử dụng một thông điệp được mã hóa, một khóa mật mã và hình vuông Vigenère để giải mã thông điệp.

Tạo một thông điệp được mã hóa bằng Vigenère Cipher và giải mã nó

1. Làm việc với bạn của mình và thống nhất về mật khẩu bí mật.
2. Tạo một thông điệp bí mật bằng cách sử dụng Vigenère cipher và khóa.
3. Trao đổi thông điệp và giải mã chúng bằng cách sử dụng khóa chia sẻ trước.
4. Sử dụng công cụ giải mã Vigenère tương tác để xác minh việc giải mã.

**Phần 2: Hệ mã DES**

Tìm hiểu và cài đặt chương trình mã hóa bằng DES.

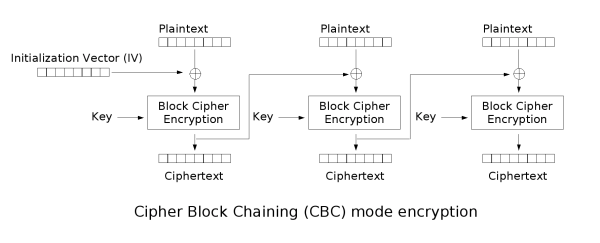
**Ghi chú**: Sinh viên có thể làm việc theo nhóm 2 người trong phần 1 nhưng vẫn nộp bài riêng.

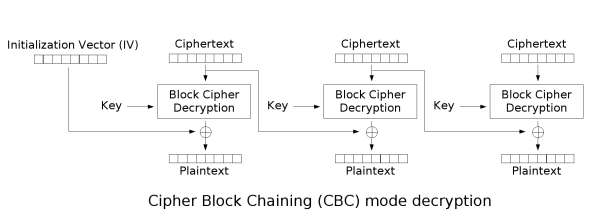
## Bối cảnh

Mã hóa là một cơ sở quan trọng trong việc bảo mật thông tin. Trong mã hóa đối xứng, người gửi và người nhận phải thống nhất một khóa bí mật chung trước. Thông điệp sau đó sẽ được mã và giải mã bằng khóa chung này. Có nhiều hệ mã đối xứng được sử dụng, tuy nhiên, trong bài này ta sẽ khảo sát về hệ mã Vigenère Cipher và DES.

Data Encryption Standard (DES) là hệ mã đối xứng theo khối (block cipher) dựa trên ý tưởng về mã hóa tích (product cipher) với Key là 56 bit và Block là 64 bit. Hệ mã này được IBM phát triển từ phương pháp Lucifer, chính thức công bố năm 1975, được chọn là Chuẩn xử lý thông tin liên bang (Federal Information Processing Standard - FIPS) năm 1976.

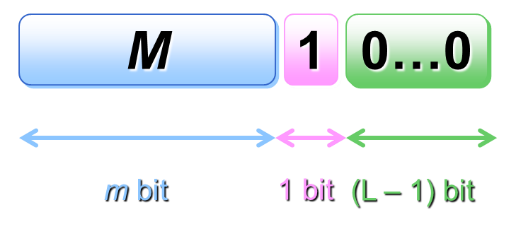
Trong mã hóa, thường dữ liệu được chia thành từng đoạn (block) có kích thước cố định. Để mã hóa các thông điệp dài (có thể chia thành nhiều block), có thể sử dụng các kiểu thao tác khác nhau (**modes of operation)** khác nhau. Tất cả các kiểu mã hóa (ngoại trừ ECB) đều sử dụng vector khởi tạo (initialization vector - IV) như một dummy block để việc xử lý khối đầu tiên không khác biệt so với việc xử lý các khối tiếp thao, đồng thời tăng tính ngẫu nhiên của quy trình mã hóa. IV không cần giữ bí mật, tuy nhiên, cần đảm bảo là hạn chế việc sử dụng lại cùng giá trị IV với cùng 1 khóa.



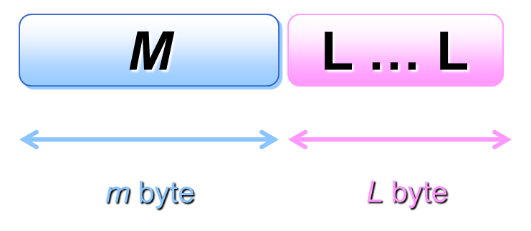


**Padding Scheme** là cách bổ sung thông tin để khối dữ liệu có kích thước phù hợp cho việc mã hóa. Yêu cầu ngoài việc khối dữ liệu sau khi bổ sung có kích thước phù hợp với việc mã hóa, thì còn có thể dễ dàng khôi phục chính xác dữ liệu sau khi giải mã (cắt bỏ chính xác các dữ liệu bổ sung thêm vào).

**Bit Padding** có kích thước khối dữ liệu “chuẩn” là *n* bit, khối dữ liệu gốc *M* có kích thước *m* bit (*m* ≤ *n*) thì khối dữ liệu sau khi padding được mô tả như sau, với *L* = *n* – (*m* mod *n*).



**Byte Padding (PKCS5)** có kích thước khối dữ liệu “chuẩn” là *n* byte (*n* < 256), khối dữ liệu gốc *M* có kích thước *m* byte (*m* ≤ *n*) thì khối dữ liệu sau khi padding được mô tả như sau, với *L* = *n* – (*m* mod *n*).



## Tài nguyên yêu cầu

Thiết bị người dùng cuối có truy cập Internet.

Môi trường lập trình với một ngôn ngữ lập trình cụ thể.

## Phần 1: Vigenère Cipher

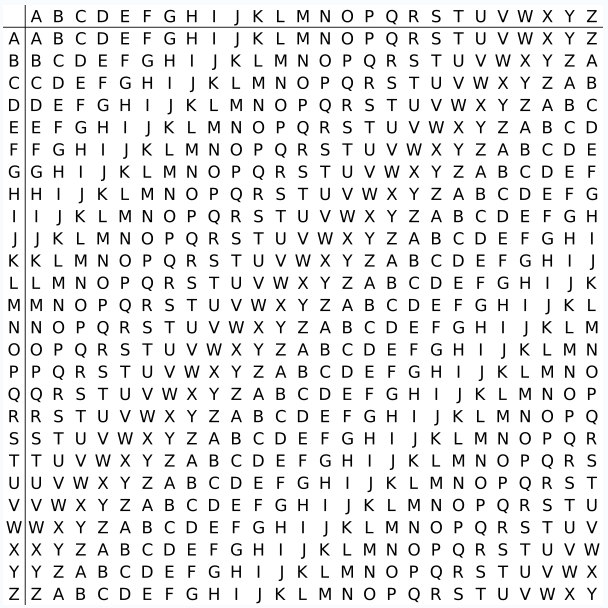
### Giải mã một thông điệp được mã hóa trước bằng cách sử dụng Vigenère Cipher

Trong Phần 1, bạn sẽ phân tích một thông điệp được mã hóa và giải mã nó bằng cách sử dụng một khóa mật mã và hình vuông mã hóa Vigenère.

Thông điệp sau đã được mã hóa bằng mã Vigenère: **VECIHXEJZXMA**

Từ khóa mật mã **TCPIP** được sử dụng để mã hóa thông điệp. Cùng từ khóa đó sẽ được sử dụng để giải mã thông điệp.

Một hình vuông hoặc bảng Vigenère chuẩn được sử dụng với từ khóa để giải mã thông điệp.



Giải mã thông điệp bằng cách sử dụng từ khóa và hình vuông Vigenère.

a. Sử dụng bảng bên dưới để giúp bạn giải mã thông điệp. Bắt đầu bằng cách nhập các chữ cái của thông điệp được mã hóa vào hàng thứ hai, từ trái sang phải.

b. Nhập từ khóa TCPIP ở hàng trên cùng, lặp lại các chữ cái cho đến khi mỗi chữ cái của thông điệp được mã hóa đều có một chữ cái từ khóa, ngay cả từ khóa cuối cùng không được khóa hoàn chỉnh.

c. Tham chiếu hình vuông hoặc bảng Vigenère được nêu ở trên và tìm hàng ngang bắt đầu bằng chữ cái đầu tiên của từ khóa (chữ T). Quét qua hàng đó và tìm chữ đầu tiên của thông điệp được mã hóa trong hàng (chữ V). Chữ cái ở đầu cột nơi thông điệp được mã hóa xuất hiện là chữ cái đầu tiên của thông điệp được giải mã (chữ C).

d. Tiếp tục quá trình này cho đến khi bạn đã giải mã toàn bộ thông điệp và nhập nó vào hàng 3 của bảng sau đây.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cipher Keyword** | T | C | P | I | P | T | C | P | I | P | T | C |
| **Encrypted Message** | V | E | C | I | H | X | E | J | Z | X | M | A |
| **Decrypted Message** | C | C | N | A | S | E | C | U | R | I | T | Y |

### Tạo một thông điệp được mã hóa bằng Vigenère Cipher và giải mã nó

Trong Phần 2, hãy làm việc với bạn của mình và thống nhất về mật khẩu bí mật để sử dụng làm khóa chia sẻ trước (pre-shared key). Mỗi bạn trong nhóm tạo một thông điệp bí mật bằng cách sử dụng mật mã Vigenère và khóa. Trao đổi thông điệp cho nhau và giải mã chúng bằng cách sử dụng khóa chia sẻ trước của mình.

**Ghi chú:** Nếu không có bạn làm chung thì hãy tự làm một mình.

#### Xác định từ khóa mật mã.

Cùng với bạn mình, hãy thiết lập một từ khóa mật mã và ghi nó vào đây.

CCNAC

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### Tạo một tin nhắn văn bản đơn giản và mã hóa nó (cả hai bạn).

1. Tạo một tin nhắn văn bản thuần (chưa được mã).

HELLO&THAYNAM \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Bạn có thể sử dụng bảng sau đây để giúp bạn mã hóa thông điệp. Bạn nhập thông điệp chưa mã hóa và từ khóa mật mã vào, nhưng đừng để bạn mình nhìn thấy.
2. Trong bảng Vigenère, xác định hàng bắt đầu bằng chữ cái đầu tiên của từ khóa mật mã. Tiếp theo xác định vị trí chữ cái đầu tiên được mã hóa ở đầu cột trong bảng. Ô mà tại đó hàng (chữ cái khóa) và cột (chữ cái thông điệp) giao nhau là chữ cái đầu tiên của thông điệp được mã hóa. Tiếp tục quá trình này cho đến khi bạn đã mã hóa toàn bộ thông điệp.

**Ghi chú**: Bảng này được giới hạn trong các tin nhắn có 12 ký tự. Bạn có thể tạo các tin nhắn dài hơn nếu muốn. Mã hóa và giải mã thông điệp không phân biệt chữ hoa chữ thường.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cipher Keyword** | C | C | N | A | C |  |  |  |  |  |  |  |
| **Encrypted Message** | J | G | Y | L | Q |  |  |  |  |  |  |  |
| **Decrypted Message** | H | E | L | L | O |  |  |  |  |  |  |  |

#### Giải mã thông điệp từ bạn mình.

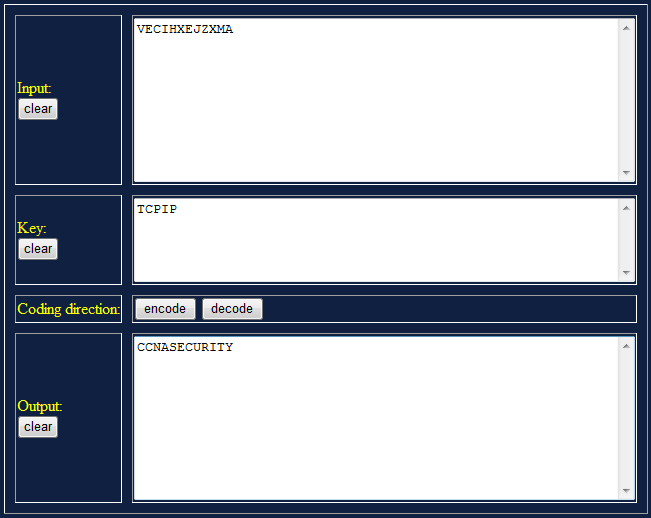
1. Bạn có thể sử dụng bảng sau để giúp bạn giải mã thông điệp được mã hóa của bạn mình. Nhập thông điệp được bạn mình mã hóa và từ khóa mật mã.
2. Sử dụng quy trình tương tự như được mô tả trong Phần 1, Bước 4.

**Ghi chú**: Bảng này được giới hạn với các thông điệp có 12 ký tự. Bạn có thể tạo các thông điệp dài hơn nếu muốn.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cipher Keyword** | C | C | N | A | C | C | C |  |  |  |  |  |
| **Encrypted Message** | V | J | N | Y | P | C | O |  |  |  |  |  |
| **Decrypted Message** | T | H | A | Y | N | A | M |  |  |  |  |  |

#### Sử dụng công cụ giải mã tương tác để xác nhận giải mã.

1. Tìm kiếm trên Internet về “Vigenère decode” cho thấy có nhiều công cụ mã hóa và giải mã khác nhau. Nhiều trong số này là tương tác (interactive).
2. Một công cụ tương tác được đặt tại trang <http://sharkysoft.com/vigenere/1.0/>. Trong trang này, nhập tin nhắn được bạn mình mã hóa ở phần trên cùng của màn hình và khóa mã hóa ở giữa. Nhấp vào **Decode** để xem bản rõ của thông điệp. Bạn cũng có thể sử dụng công cụ này để mã hóa thông điệp.
3. Ví dụ sau sử dụng công cụ Vigenère Cipher của Sharky để giải mã thông điệp được mã hóa trong Phần 1.



### Nhận xét

1. Mã Vigenère có thể được sử dụng để giải mã các thông điệp mà không có máy tính không?

Có, bạn không chỉ có thể mã hóa một tin nhắn mà còn có thể đặt nó ở bất kỳ kích thước nào bạn muốn. Yêu cầu duy nhất đối với người nhận là các bản sao của hình vuông Vigenère, từ khóa cypher và tin nhắn được mã hóa.

1. Tìm kiếm trên Internet các công cụ bẻ khóa mã Vigenère. Mã Vigenère có được coi là một hệ thống mã hóa mạnh và khó bẻ khóa không?

Không, có một số công cụ bẻ khóa có thể truy cập được. Bạn có thể giải mã mã Vigenere chỉ bằng toán học trong khoảng 20 phút

## Phần 2: Hệ mã DES

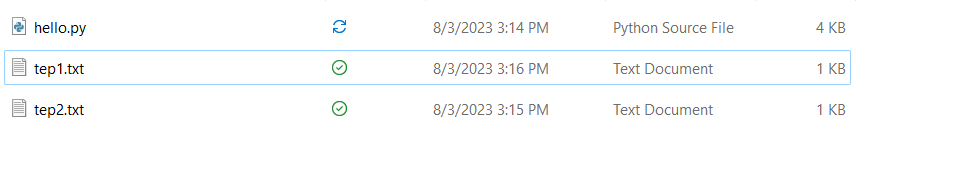
Hãy xây dựng ***1 chương trình*** với ngôn ngữ tự chọn, có thể sử dụng thư viện hỗ trợ, cho phép ***mã hóa*** và ***giải mã file*** (ở mức độ đơn giản) bằng ***giải thuật mã hóa đối xứng*** **DES.** Kích thước khóa: 64 bit (thực chất chỉ dùng 56 bit), kích thước khối: 64 bit

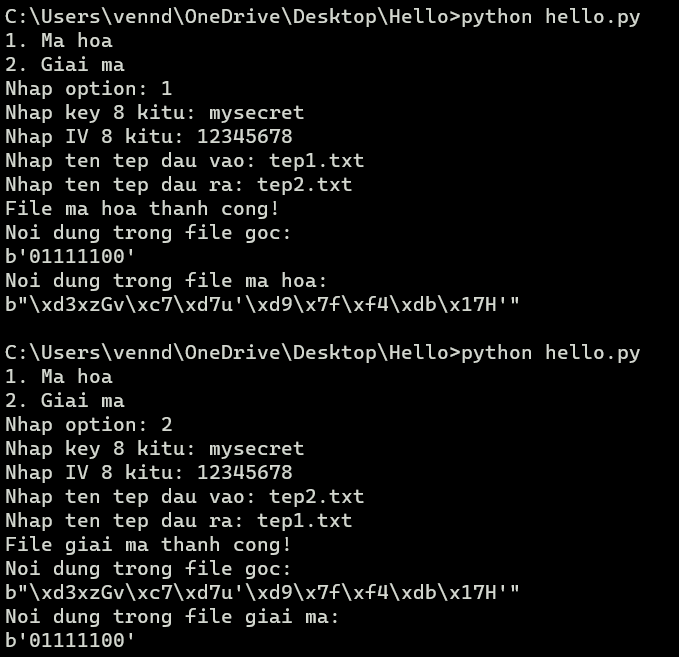
**Nâng cao**: ngoài các kích thước khóa nêu trên, mỗi thuật toán có thể hỗ trợ thêm 1 số độ dài khóa khác.

**Chương trình cho phép chọn chức năng mã hóa hay giải mã file**:

* ***Mật khẩu***: người dùng ***trực tiếp nhập mật khẩu***. Để đơn giản, người sử dụng sẽ nhập mật khẩu có độ dài ***đúng bằng kích thước khóa*** cần dùng (ví dụ: thuật toán sử dụng khóa 64 bit = 8 byte thì mật khẩu gồm 8 ký tự).
* Cho phép ***chọn 1 tập tin bất kỳ***.
* Tiến hành mã hóa/giải mã file sử dụng chế độ padding **PKCS#7** và mode of operation **CBC** với **IV** do người dùng nhập.

**Nâng cao**: cho người dùng chọn thêm các padding scheme và mode of operation khác.





## Tham khảo

CISCO, 7.5.1.2 Lab - Exploring Encryption Methods

Trần Minh Triết, Bài tập thực hành Mã hóa Thông tin và Ứng dụng, ĐHKHTN.