logo1**TRƯỜNG ĐẠI HỌC KỸ THUẬT CÔNG NGHỆ**

**KHOA CÔNG NGHỆ THÔNG TIN**

**Môn: Bảo Mật Thông Tin**

Bài thực hành số 1



**Bài 1: Viết chương trình mã hóa và giãi mã văn bản với thuật toán mã hóa Ceasar. Chương trình có thể thực hiện các chức năng sau:**

**Cho phép nhập văn bản vào hệ thống. Cho phép nhập khóa bảo vệ văn bản.**

**Cho phép ghi File và mở File.**

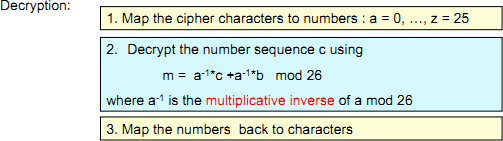
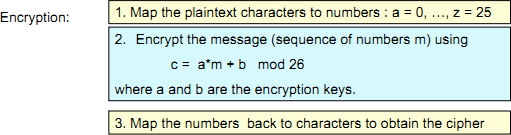
# Hướng dẫn mã dịch chuyển Caesar:

-Ta lần lượt đánh chỉ số cho các chữ cái bắt đầu từ 0.

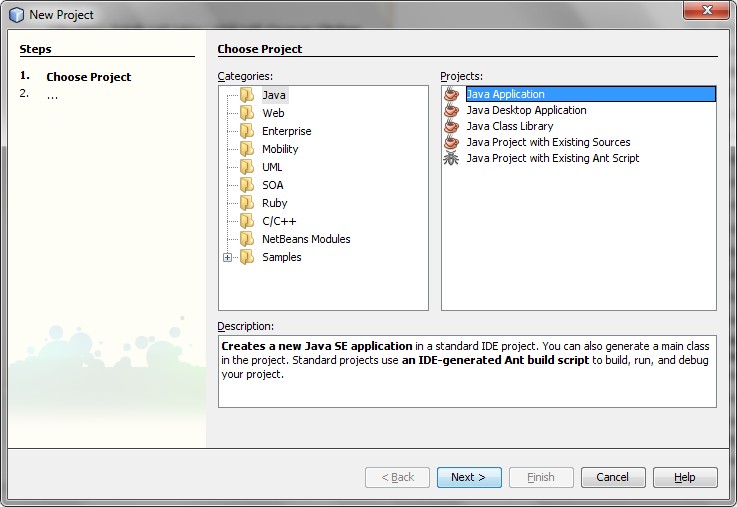
- Gọi k là 1 số nguyên từ 0 ->25 được gọi là khóa.

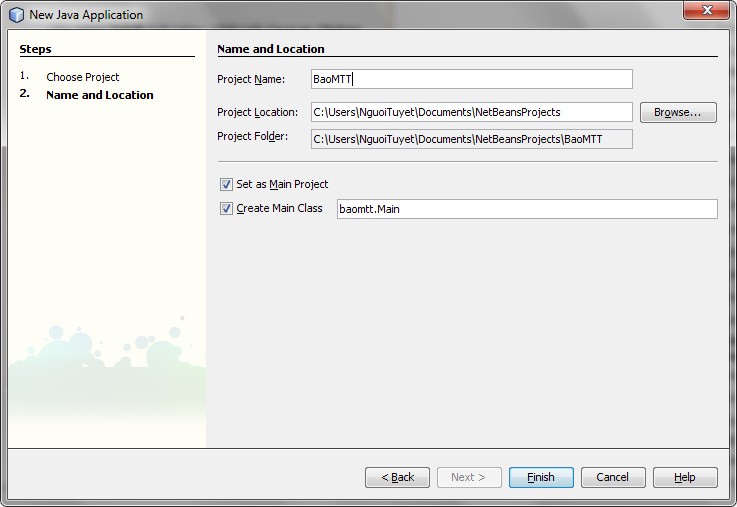
-Hàm mã hóa: E(p,k)=(p+k)mod26 với p là chỉ số của ký tự cần mã hóa.

-Hàm giải mã: D(c,k)=|c-k|mod26 với c là chỉ số của ký tự cần giải mã.

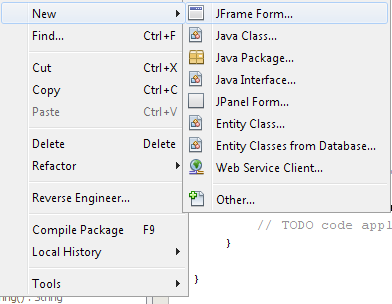


**Bước 1**: Tạo project mới: File  New Project





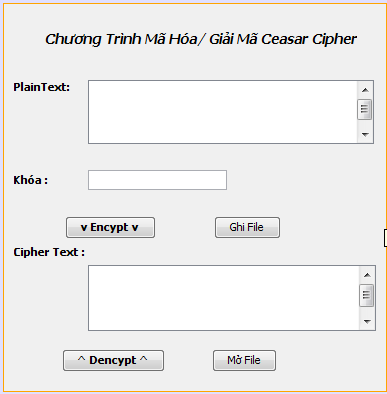
**Bước 2**: Tạo mới jFrame Form thiết kế:



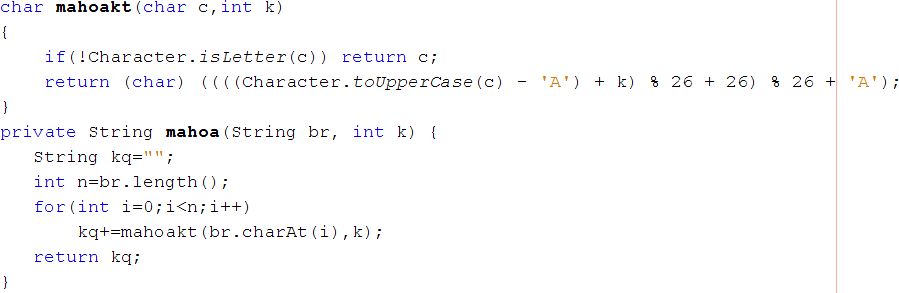
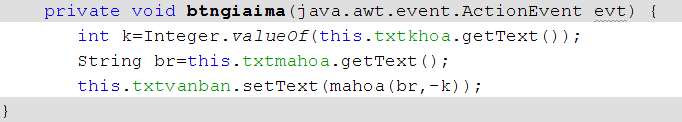
Giao diện thiết kế Frame:

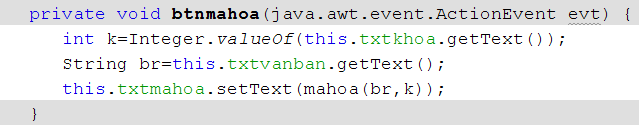


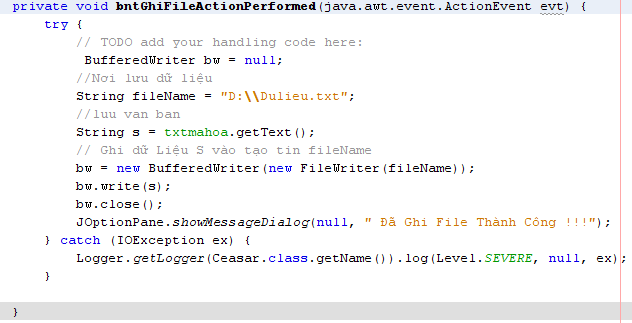
**Bước 3**: Thiết kế Form



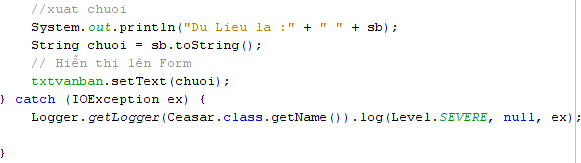
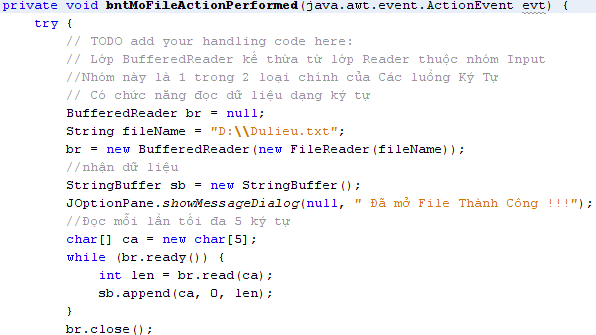
**Bước 4**: Viết hàm xữ lý sự kiện



1. Hàm xữ lý sự kiện Encypt
2. Hàm xữ lý sự kiện Ghi File



1. Hàm xữ lý sự kiện Dencypt
2. Hàm xữ lý sự kiện Mở File



**Bài 2: Viết chương trình mã hóa và giãi mã văn bản với thuật toán mã hóa Vigenere.**

**Chương trình có thể thực hiện các chức năng sau: Cho phép nhập văn bản vào hệ thống.**

**Cho phép nhập khóa bảo vệ văn bản.**

**Cho phép mở File và Ghi File.**

**Hướng Dẫn:** Mật mã Vigenere còn gọi là mật mã nhiều bảng mã. Ưu điểm của mã này là việc sử dụng 26 bảng mã khác nhau. Do đó mà không bị phá trong một thời gian dài. Ngoài ra mã này còn hỗ trợ việc sử dụng từ khóa vô cùng tiện lợi.

Thuật toán:

* + Khoá K là một bộ gồm nhiều khoá con

o K = (k1, k2, …, km)

# Mã hoá:

o eK(x1, x2, …, xm) = (x1 + k1, x2 + k2, …, xm + km)

# Giải mã:

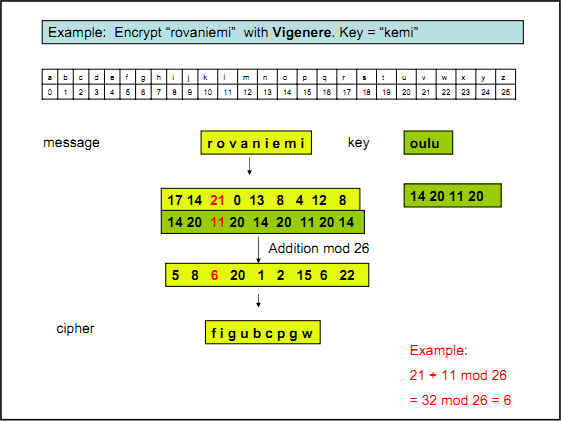
o dK(y1, y2, …, ym) = (y1 – k1, y2 – k2, …, ym – km)

o *(cộng, trừ theo modulo 26)*

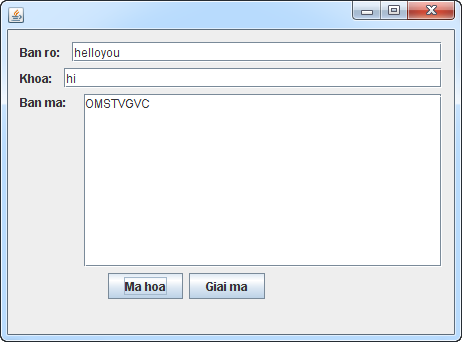
* “MÃ KHỐI” (block cipher)*

*Ví dụ:*

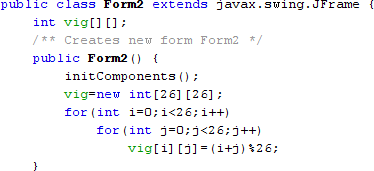
* + {A, B, C, …, X, Y, Z} = **Z**26={0, 1, …, 25}.
  + K = (2, 8, 15, 7, 4, 17) (“CIPHER”).
  + p = “thiscryptosy”.
  + c = “VPXZGIAXIVWP”



**Bước 1**: Thiết Kế Form :

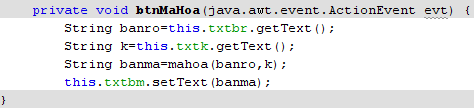


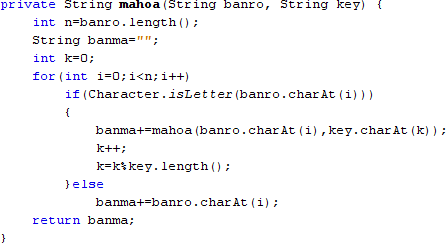
Hàm khởi tạo form:

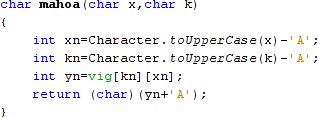


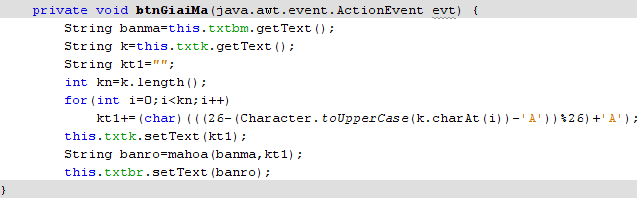
**Bước 2**: Viết hàm xử lý sự kiện

1. Hàm xữ lý sự kiện Encypt







1. Hàm xữ lý sự kiện Dencypt

**Bài Tập Về Nhà:** Yêu cầu viết phần mềm mã hóa và giải mã với 2 thuật toán trên bao gồm:

* Menu mã hóa: Thuật toán Ceasar, Thuật Toán Vigenere
* Menu giãi mã: Thuật toán Ceasar, Thuật Toán Vigenere
* Các chức năng mã hóa và giãi mã đều phải có mục mã hóa và giãi mã theo File( File có thể là .txt, .dat,…)

**Bài 3: Viết chương trình mã hóa và giãi mã văn bản với thuật toán mã hóa Rail Fence.**

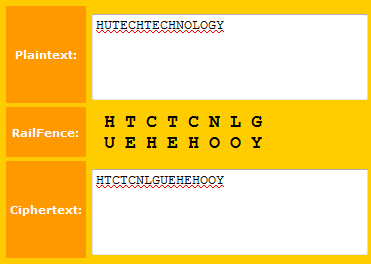
**Chương trình có thể thực hiện các chức năng sau: Cho phép nhập văn bản vào hệ thống.**

**Cho phép nhập khóa bảo vệ văn bản.**

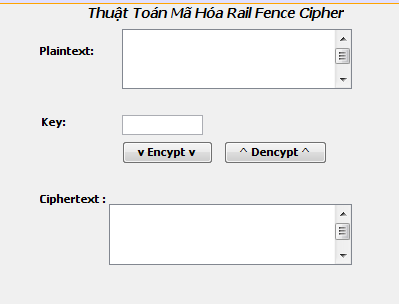
**Cho phép mở File và Ghi File.**

**Hướng Dẫn** :Mã Rail Fence còn được gọi là mã zig zag là một hình thức của mã chuyển vị:

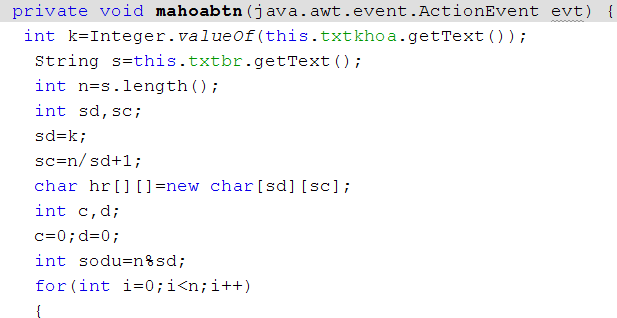
* + Thông điệp được viết lần lượt từ trái qua phải trên các cột (rail) của một hàng dào tưởng tượng theo đường chéo từ trên xuống dưới.
  + Theo đường chéo từ dưới lên khi đạt tới cột thấp nhất.
  + Và khi đạt tới cột cao nhất, lại viết theo đường chéo từ trên xuống. Cứ lặp đi lặp lại như thế nào cho đến khi viết hết toàn bộ nội dung của thông điệp.
  + Ví dụ: mã hóa chuổi HUTECH TECHNOLOGY với khóa là 2.

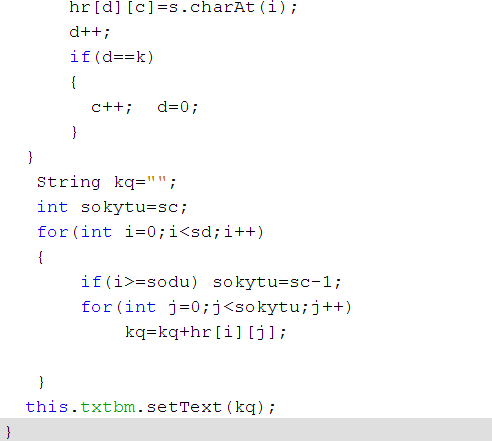


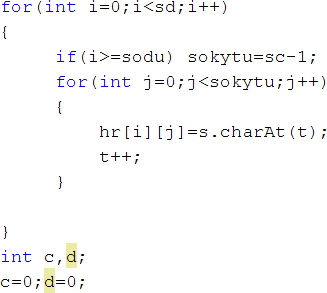
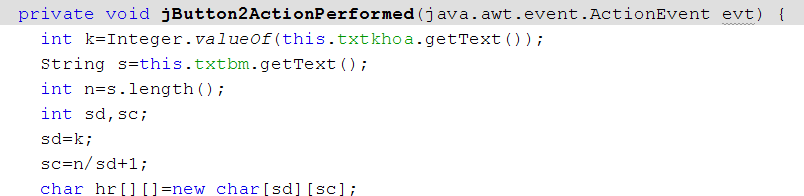
**Bước 1**: Thiết Kế Form :

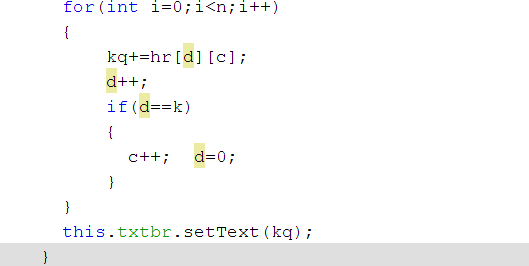


**Bước 2**: Viết hàm xử lý sự kiện

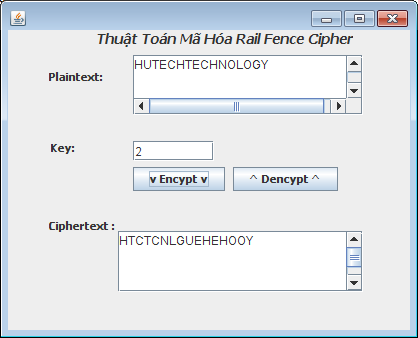
1. Hàm xữ lý sự kiện Encypt



1. Hàm xữ lý sự kiện Dencypt: ( Bài tập về nhà Sinh viên )



# Bước 3: Kiểm Tra



**Bài 4: Viết chương trình mã hóa và giãi mã văn bản với thuật toán mã hóa PLayFail.**

**Chương trình có thể thực hiện các chức năng sau: Cho phép nhập văn bản vào hệ thống.**

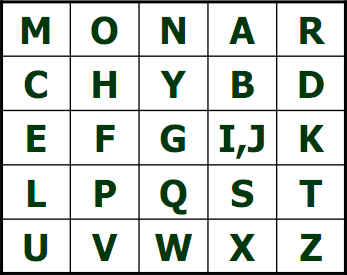
**Cho phép nhập khóa bảo vệ văn bản.**

**Cho phép mở File và Ghi File.**

**Hướng dẫn:**

* **Phương pháp** là lập ma trận 5x5 dựa trên từ khóa cho trước và các ký tự trên bảng chữ cái :

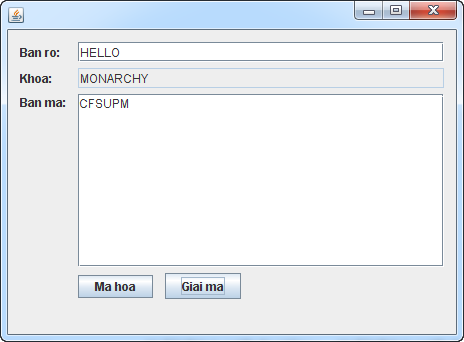
* Trước hết viết các chữ của từ khoá vào các hàng của ma trận bắt từ hàng thứ nhất.
* Nếu ma trận còn trống, viết các chữ khác trên bảng chữ cái chưa được sử dụng vào các ô còn lại. Có thể viết theo một trình tự qui ước trước, chẳng hạn từ đầu bảng chữ cái cho đến cuối.
* Vì có 26 chữ cái tiếng Anh, nên thiếu một ô. Thông thuờng ta dồn hai chữ nào đó vào một ô chung, chẳng hạn I và J.
* Giả sử sử dụng từ khoá MORNACHY. Lập ma trận khoá Playfair tương ứng như sau:



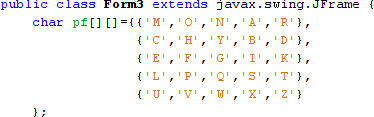
* **Quy tắc mã hóa và giải mã**

* + Chia bản rõ thành từng cặp chữ. Nếu một cặp nào đó có hai chữ như nhau, thì ta chèn thêm một chữ lọc chẳng hạn X. Ví dụ, trước khi mã **“balloon”** biến đổi thành **“ba lx lo on”.**
  + Nếu cả hai chữ trong cặp đều rơi vào cùng một hàng, thì mã mỗi chữ bằng chữ ở phía bên phải nó trong cùng hàng của ma trận khóa (cuộn vòng quanh từ cuối về đầu), chẳng hạn “**ar”** biến đổi thành “RM” .
  + Nếu cả hai chữ trong cặp đều rơi vào cùng một cột, thì mã mỗi chữ bằng chữ ở phía bên dưới nó trong cùng cột của ma trận khóa (cuộn vòng quanh từ cuối về đầu), chẳng hạn “**mu”** biến đổi thành “CM”.
  + Trong các trường hợp khác, mỗi chữ trong cặp được mã bởi chữ cùng hàng với nó và cùng cột với chữ cùng cặp với nó trong ma trận khóa. Chẳng hạn, **“hs”** mã thành **“BP”**, và **“ea”** mã thành **“IM”** hoặc **“JM”** .

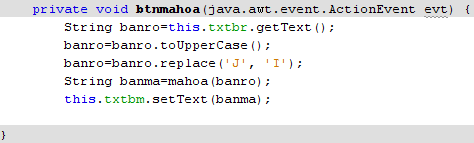
**Bước 1**: Thiết Kế Form :



Khai báo bảng khóa playfair ứng với khóa MONARCH khóa form:



**Bước 2**: Viết hàm xử lý sự kiện

1. Hàm xữ lý sự kiện nút mã hóa

String mahoa String banro) { n=banro.length ):

i=O:

String banma=””:

a,b:

it i==n-1)

a=banro.charAt i):

b= :

lelse{

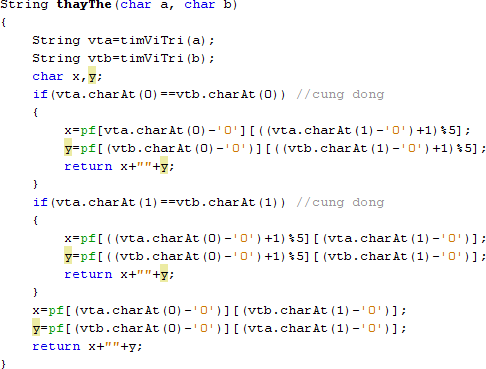
a=banro.charAt i): b=banro.charAt i+1):

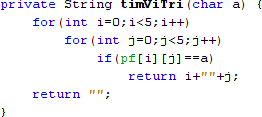
it a==b)

b= :

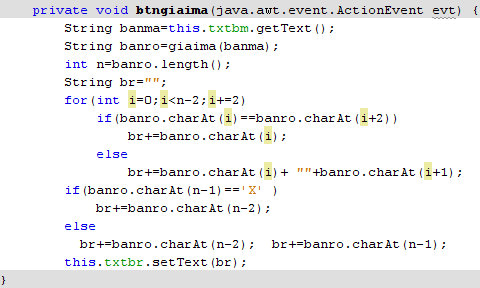


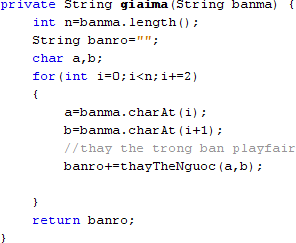
banma+=thagThe a,b): return banma:

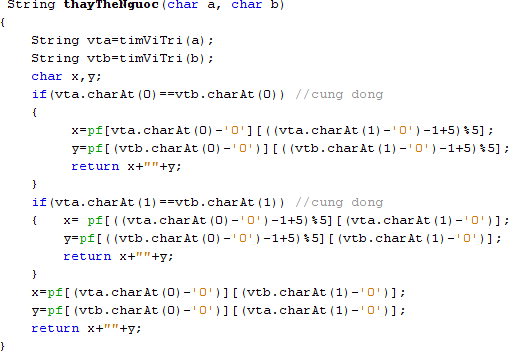




1. Hàm xữ lý sự kiện nút giải mã







**Bài 5: Viết chương trình mã hóa và giãi mã văn bản với thuật toán mã hóa Transposition cipher.**

**Chương trình có thể thực hiện các chức năng sau: Cho phép nhập văn bản vào hệ thống.**

**Cho phép nhập khóa bảo vệ văn bản.**

**Cho phép mở File và Ghi File.**

# Hướng dẫn :Hệ mã hóa đổi chỗ ( Transposition Cipher)

Là hệ mã hóa trong đó các kí tự của bản gốc được giữ nguyên, nhưng vị trí bị thay đổi.

***Đảo ngược toàn bộ plaintex*** : nghĩa là bản gốc được viết theo thứ tự ngược lại từ sau ra trước.

Ví dụ Plaintext: SECURE EMAIL Bản mã: LIAMEERUCES

***Mã hóa theo mẫu hình học***: bản gốc được sắp xếp lại theo một mẫu hình học nào đó, thường là một mảng hoặc ma trận hai chiều.

Ví dụ: bản gốc ban đầu là BAO MAT

# Ví dụ mã hoá theo mẫu hình học.

|  |  |  |
| --- | --- | --- |
| Cột 1 | Cột 2 | Cột 3 |
| B | A | O |
| M | A | T |

Nếu lấy các cột theo thứ tự 2, 3, 1. Bản mã sẽ là AAOTBM

***Đổi chỗ cột:*** đổi chỗ các kí tự trong plaintext thành dạng hình chữ nhật theo cột. Ví dụ : Bản gốc BAO MAT THU DIEN TU

Bản gốc được chuyển thành ma trận 3x5 như sau:

# Bảng ví dụ mã hóa bằng phương pháp đổi chỗ cột

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cột 1 | Cột 2 | Cột 3 | Cột 4 | Cột 5 |
| B | M | T | D | N |
| A | A | H | I | T |
| O | T | U | E | U |

Vì có 5 cột nên chúng có thể được sắp lại theo 5! = 120 cách khác nhau

Nếu ta chuyển vị các cột theo thứ tự 3, 5, 2, 4, 1 rồi lấy các kí tự theo hàng ngang ta sẽ thu được bản mã: TNMDBHTAIAUUTEO.

***Hoán vị các kí tự của bản gốc theo chu kỳ cố định d*:** Nếu hàm f là hoán vị của một khối gồm d kí tự thì khóa mã hóa được biểu diễn bởi K(d, f)

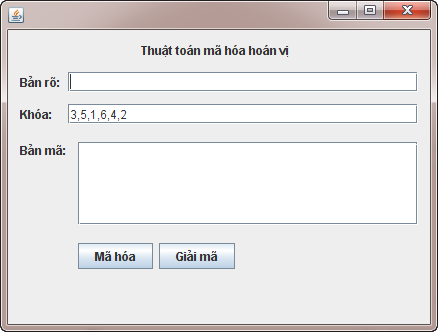
Ví dụ: với d = 5, f hoán vị của dãy 12345 thành 35142

# Bảng Hoán vị các kí tự của bản gốc theo chu kỳ cố định d

|  |  |  |  |
| --- | --- | --- | --- |
| Vị trí ban đầu | Vị trí hoán vị | Nội dung mã hóa | Mã hóa |
| 1 | 3 | G | O |
| 2 | 5 | R | P |
| 3 | 1 | O | G |
| 4 | 4 | U | U |
| 5 | 2 | P | R |

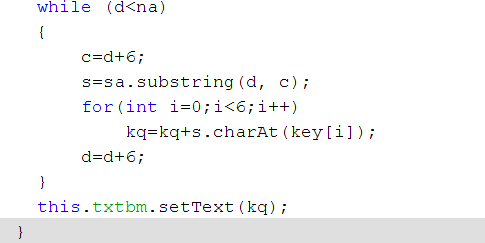
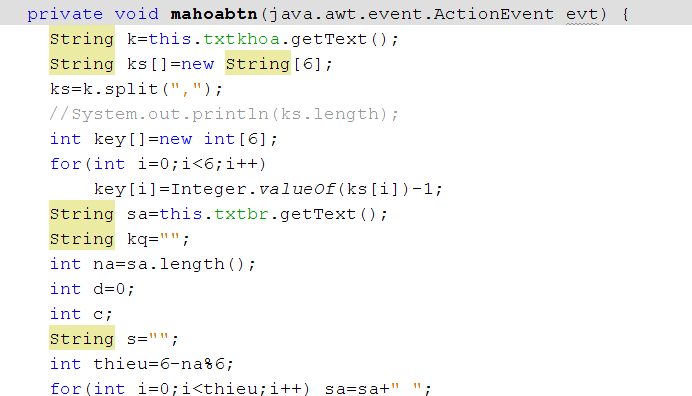
Theo bảng trên bản gốc ban đầu được mã hóa thành OPGUP.

**Bước 1**: Thiết Kế Form :

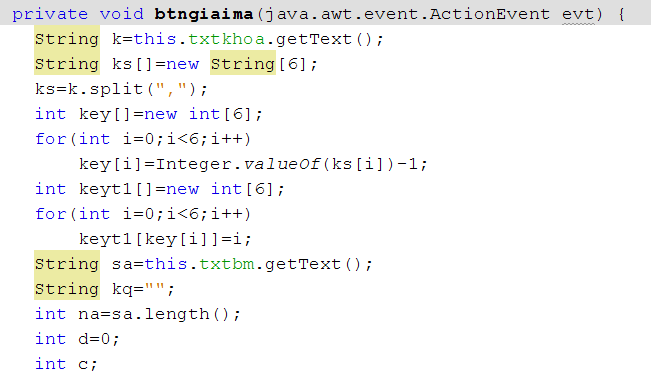
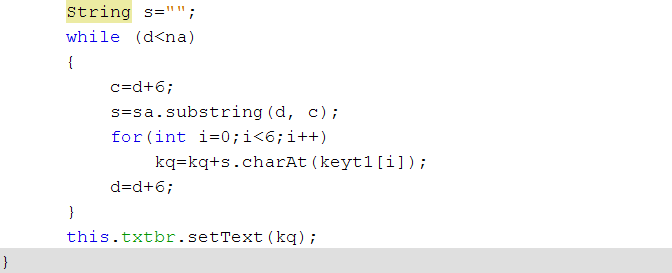


**Bước 2**: Viết hàm xử lý sự kiện

1. Hàm xử lý sự kiện Encypt



1. Hàm xử lý sự kiện Dencypt



**Bài Tập: Viết phần mềm mã hóa văn bãn với các thuật toán mã hóa trên. Chương trình có thể thực hiện các chức năng sau:**

**Cho phép nhập văn bản vào hệ thống. Cho phép nhập khóa bảo vệ văn bản. Cho phép mở File và Ghi File.**

**Cho phép bên gữi mã hóa dữ liệu và bên nhận mã hóa dữ liệu với khóa K.**