**Bài tập ngày 17/9 – An toàn mạng máy tính (NT101.P11)**

1. ***Mã hoá Vigènere***

Plaintext: **THANH PHO HO CHI MINH**

Key: **TANGDUNGCAM**

Theo phương pháp ta tra bảng lần lượt từng kí tự của plaintext theo kí tự tương xứng với vị trí ở key

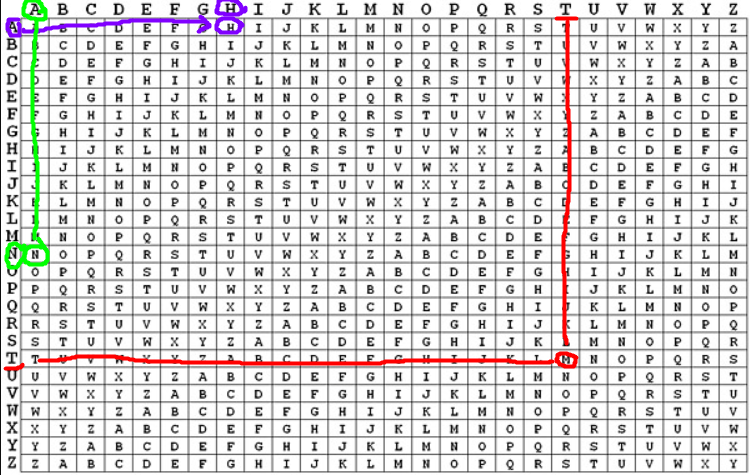
+ Dò tìm kí tự T theo T thì được chữ **M**

+ Dò tìm kí tự H theo A thì được chữ **H**

+ Dò tìm kí tự A theo N thì được chữ **N**

+ Tương tự với các kí tự còn lại

Cuối cùng ta được kết quả ciphertext là “**MHNTK JUU JO OAI ZOQB**”



1. ***Mã hoá Playflair***

M: “NAM HOC 2024”

K: TANGDUNGCAM

* **Tách chuỗi Plaintext:**

+ Đối với mã hoá Playflair ta cần tách chuỗi M thành các cặp gồm 2 kí tự.

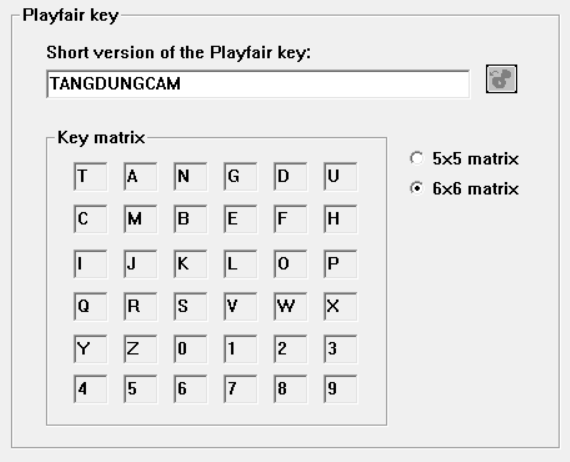
+ Như vậy ta được **NA MH OC 20 24**

* **Lập bảng:**

+ Tiếp theo xét từng cặp kí tự để dò ra cặp mã hoá tương ứng theo bảng

+ Bảng sẽ là ma trận 6x6 vì Plaintext có chứ chữ số

+ Thêm từ trái sang phải từ trên xuống dưới từng kí tự của key vào, nếu kí tự bị lặp lại thì bỏ qua kí tự đó. Khi đến Z tiếp tục thêm các số vào từ 0 đến 9 vào.



* **Dò bảng tìm mã:**

+ Với cặp đầu tiên NA ta sẽ tìm vị trí N và A trên bảng sau đó tiến hành xét. Vì nằm cùng dòng nên sẽ thay bằng 2 kí tự nằm bên phải. Ở đây kế N là G và kế A là N. Nên thay cho cặp NA sẽ là cặp **GN**.

+ Cặp MH rơi vào trường hợp nằm cùng dòng như cặp NA nên nó sẽ tương tự. Bên phải M là B, H nằm cuối hàng nên bên phải của H sẽ trở về đầu hàng là C. Cặp kết quả là **BC**.

+ Cặp OC nằm không cùng hàng cũng không cùng dòng. Ta tiến hành tìm vị trí có chung hàng với chữ O và chung cột với chữ C, vị trí đó là chữ I. Tương tự nhưng ngược lại, tìm vị trí có chung hàng với chữ C và chung cột với chữ O, đó là chữ F. Cặp kết quả là **IF**.

+ Cặp 31 và Y8 có trường hợp như trên nên ta thực hiện tương tự

* Ciphertext cuối cùng: **GN BC IF 31 Y8**

1. ***Mã hoá Hill***

n = 2

M= “**BAO MAT INTERNET**”

K = …

* Tiến hành lập bảng có kích thước 2x2 (vì n =2) và cho vào đó các kí tự ngẫu nhiên. Bảng tương tự sẽ chứa giá trị của kí tự đó theo dạng số thứ tự của nó trong bảng Alphabet.

A white square with black text

Description automatically generated

* Với n bằng 2 ta lấy từng cặp 2 kí tự từ M để tìm và dùng giá trị thứ tự của chúng để tính toán theo công thức. Sau đó đổi tiếp theo bảng thứ tự chữ cái Alphabet để ra kí tự mã hoá.
* BA = [ 02 01 ]

+ Tính ( 2 \* 19 + 1 \* 16 ) mod 26 = 2 🡺 Kí tự B

+ Tính ( 2 \* 5 + 1 \* 7 ) mod 26 = 17 🡺 Kí tự Q

* Tính tương tự với các cặp kí tự còn lại:
* OM = [ 15 13 ]

+ ( 15 \* 19 + 13 \* 16 ) mod 26 = 25 🡺 Kí tự Y

+ ( 15 \* 05 + 13 \* 07 ) mod 26 = 10 🡺 Kí tự J

* AT = [ 01 20 ]

+ ( 01 \* 19 + 20 \* 16 ) mod 26 = 01 🡺 Kí tự A

+ ( 01 \* 05 + 20 \* 07 ) mod 26 = 15 🡺 Kí tự O

…

* Sắp xếp các kí tự tìm được và giữ nguyên vị trí dấu cách thì ciphertext cuối cùng là “**BQY JAO EMRETFYI**”.