1. Sử dụng giải thuật Vingenể, m=caothikimcam, k=computer
2. Giải thuật Playfair, m=CAOTHIKIMCAM, k= ANTOANTHONGTIN

Lời giải:

Câu 1.

C= (p+x) mod 26

Từ khoá: CAOTHIKIMCAM

Mã hoá: COMPUTERCOMP

E <- (C+C)%26=4%26=4

O <- (A+O)%26=(26+14)%26=14

A <- (O+M)%26=(14+12)%26=0

I <- (T+P)%26=(19+15)%26=8

B<- (H+U)%26=(7+20)%26=1

B <- (I+T)%26=(8+19)%26=1

O <- (K+E)%26=(10+4)%26=14

Z <- (I+R)%26=(8+17)%26=25

O <- (M+C)%26=(12+2)%26=14

Q <- (C+O)%26=(2+14)%26=16

M <- (A+M)%26=(26+12)%26=12

B <- (M+P)%26=(12+15)%26=1

Kết quả: -> EOA IBB OZO QMB

Câu 2:

* Ma trận khoá: Thêm khoá vào ma trận 5\*5, và thêm lần lượt bảng chữ cái bắt đầu từ A, không trùng khoá vào những ô còn trống. Lưu ý, I và J tính như nhau.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A | N | T | O | H |  |
| G | I | B | C | D |  |
| E | F | K | L | M |  |
| P | Q | R | S | U |  |
| V | W | X | Y | Z |  |
|  |  |  |  |  |  |

* Mã hoá: Từng cặp 2 kí tự liên tiếp

m= CA OT HI KI MC AM

Ví dụ CA không cùng dòng hoặc hàng: CA-> GO

OT cùng dòng: Lấy bên phải OT->HO

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **A** | N | T | O | H |  |
| G | I | B | **C** | D |  |
| E | F | K | L | M |  |
| P | Q | R | S | U |  |
| V | W | X | Y | Z |  |
|  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A | N | **T** | **O** | H |  |
| G | I | B | C | D |  |
| E | F | K | L | M |  |
| P | Q | R | S | U |  |
| V | W | X | Y | Z |  |
|  |  |  |  |  |  |

Tương tự:

Kết quả:

m= CA OT HI KI MC AM

* GO HO ND FB LD HE