NHÓM 3

BÀI TẬP : MÃ HOÁ CỔ ĐIỂN

1. MẬT MÃ CAESAR

M = NOROSEWITHOUTATH

K = 8

TH 1: C = E(p) = (p+k) mod 26

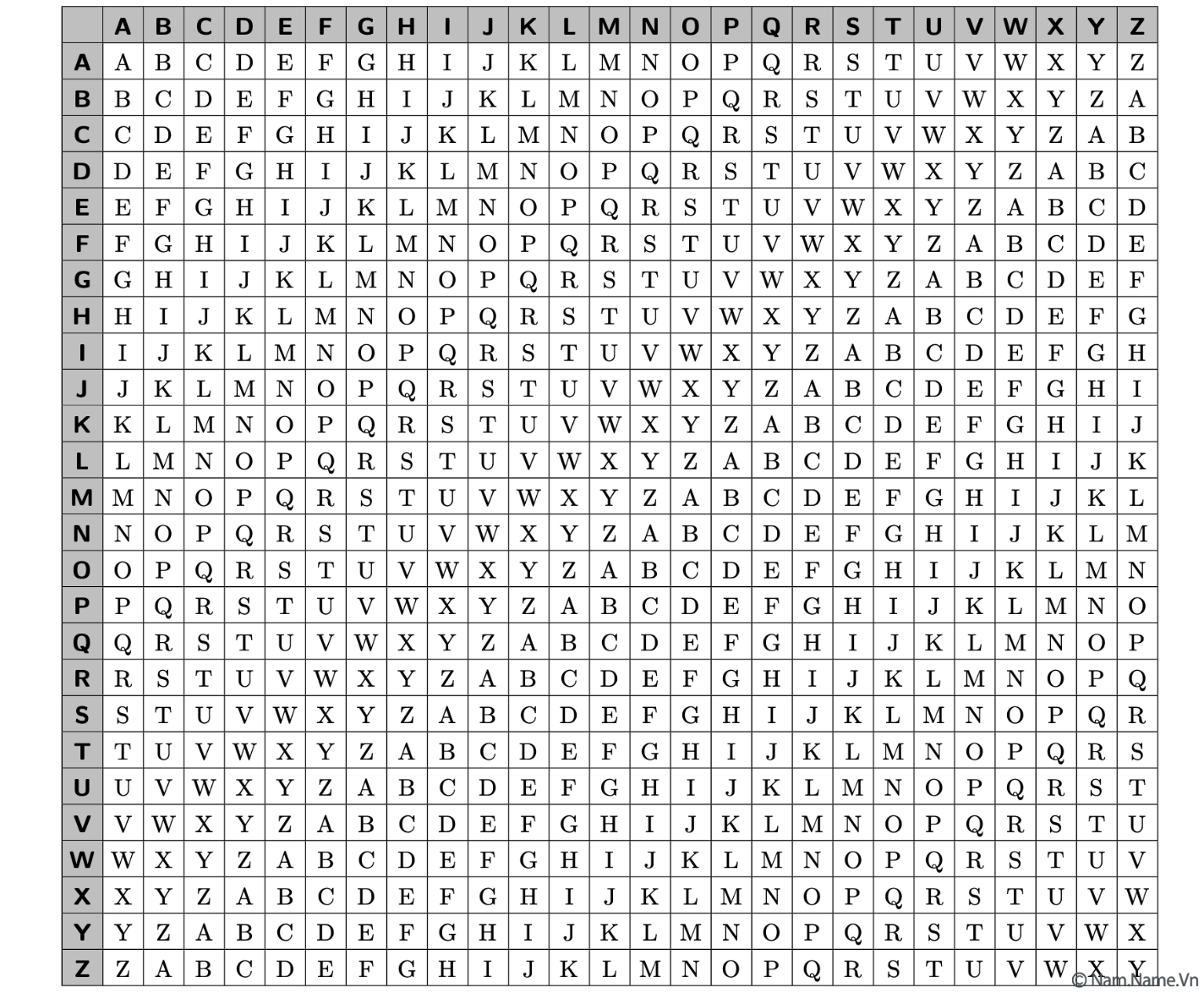
= VWZWAMEQBPWCBIBP

1. MẬT MÃ VIGENERE- LẶP KHOÁ

M = MONEYMAKESTHE

K = YOUREON

* YOUREONYOUREO



* C: KCHVCANISMKLS

1. MẬT MÃ VIGENERE- AUTO KEY (từ khoá nối tiếp bằng chính bản rõ để tạo thanh khoá)

M = MONEYMAKESTHE

K = YOUREON

* YOUREONMONEYM
* C = KCHVCANWSFXFQ

1. MÃ HOÁ CHỮ ĐƠN (sắp xếp khoá K theo bảng chữ cái abc rồi dọc theo thứ tự để tìm C theo M)

M = AWOMANGIVESANDFO

K = THLEYNPSXADWKFUBOGMQVJRCIZ

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

* C = TRUKTFPXJYMTFENU

1. MẬT MÃ MA TRẬN KHOÁ PLAYFAIR

Input: M = THETRUTHWILLOU

Key: K = THEDIEIS

Tìm Output: C =

Bài làm

B1: Tạo ma trận 5x5 với khoá K: THEDIEIS

(I, J chung 1 vị trí)

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

Tách: M = TH ET RU TH WI LL OU

Biến đổi M: M = TH ET RU TH WI LX LO UX (có cặp trùng thêm X giữa và có lẻ thì thêm X cuối)

Mã hoá: TH 🡺 HE

ET 🡺 DH

RU 🡺 UO

TH 🡺 HE

WI 🡺 ZH

LX 🡺 QE

LO 🡺 GQ.

UX 🡺 QZ

Output C = HE DH UO HE ZH QE GQ QZ

1. MẬT MÃ HOÁN VỊ

Input: M = ABADBEGINNINGMAKES

Key: K = 9

Tìm Output: C =

Bài làm

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | E |  |
|  | B |  |  |  |  |  |  |  |  |  |  |  |  |  | K |  | S |
|  |  | A |  |  |  |  |  |  |  |  |  |  |  | A |  |  |  |
|  |  |  | D |  |  |  |  |  |  |  |  |  | M |  |  |  |  |
|  |  |  |  | B |  |  |  |  |  |  |  | G |  |  |  |  |  |
|  |  |  |  |  | E |  |  |  |  |  | N |  |  |  |  |  |  |
|  |  |  |  |  |  | G |  |  |  | I |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | I |  | N |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | N |  |  |  |  |  |  |  |  |  |

C = AE BKS AA DM BG EN GI IN N