Lê Ngọc Kiều Anh - 22520047

**Bài 1.**

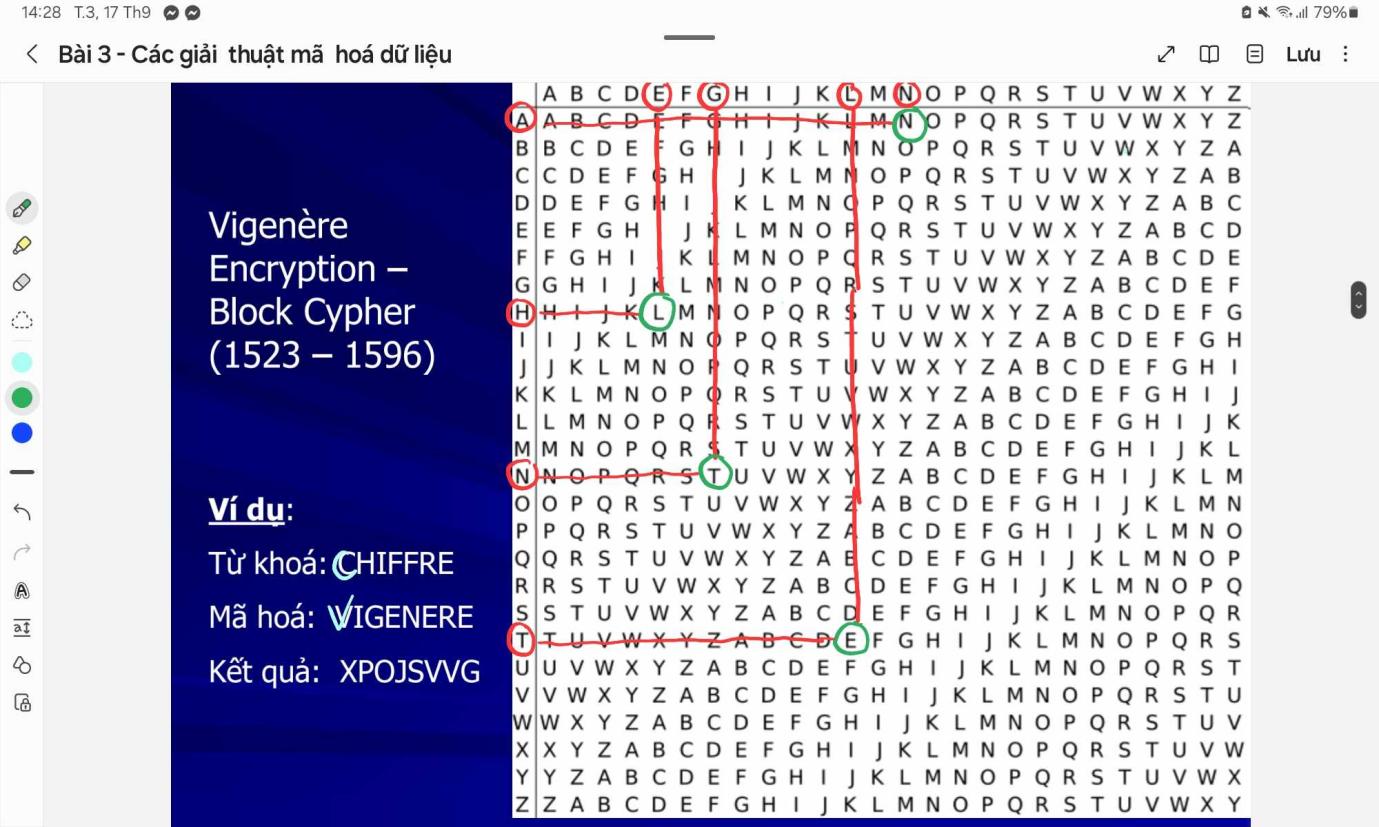
**Mã hóa Vingenere**

**Plaintext = THANH PHO HO CHI MINH**

**Key = LE NGOC KIEU ANH**

**T H A N H P H O H O C H I M I N H**

**L E N G O C K I E U A N H L E N G**

****

T được dịch L lần --> E

H được dịch E lần --> L

A được dịch N lần --> N

N được dịch G lần --> T

H được dịch O lần --> V

P được dịch C lần --> R

H được dịch K lần --> R

O được dịch I lần --> W

H được dịch E lần --> L

O được dịch U lần --> I

C được dịch A lần --> C

H được dịch N lần --> U

I được dịch H lần --> P

M được dịch L lần --> X

I được dịch E lần --> M

N được dịch N lần --> A

H được dịch G lần --> N

Ghép các chữ cái lại ta được: **C = ELNTV RRW LI CUP XMAN**

**Bài 2.**

**M = “NAM HOC 2024”**

**K = LENGOCKIEUANH**

K = "LENGOCKIEUANH" và loại bỏ các ký tự trùng lặp. Sau đó, bổ sung các chữ cái còn lại trong bảng chữ cái và các số từ 0 đến 9 vào bảng.

Bảng Playfair 6x6:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| L | E | N | G | O | C |
| K | I | U | A | H | B |
| D | F | J | M | P | Q |
| R | S | T | V | W | X |
| Y | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

M = "NAM HOC 2024":

Loại bỏ khoảng trắng và giữ lại các chữ cái cùng với số: NAMHOC2024.

Chia văn bản thành các cặp ký tự: NA, MH, OC, 20, 24.

NA → GU

MH → PA

OC → CL.

20 → 31.

24 → Y8.

"NAM HOC 2024" sau khi mã hóa Playfair với khóa "LENGOCKIEUANH" và sử dụng ma trận 6x6 là:

**C = GU PA CL 31 Y8**

**Bài 3.**

Mã hóa Hill (n =2)

M = “BAO MAT INTERNET”

K = CDZI

**C = JISMEXEVBSFVQX**

**Ta có: K =**

|  |  |
| --- | --- |
| **C 03** | **D 04** |
| **Z 26** | **I 09** |

**BA = [02, 01]**

02 \* 03 + 01 \* 04 (mod 26) = 10 --> J

02 \* 26 + 01 \* 09 (mod 26) = 9 --> I

**OM = [15, 13]**

15 \* 03 + 13 \* 04 (mod 26) = 19 --> S

15 \* 26 + 13 \* 09 (mod 26) = 13 --> M

**AT = [01, 20]**

01 \* 03 + 20 \* 04 (mod 26) = 5 --> E

01 \* 26 + 20 \* 09 (mod 26) = 24 --> X

**IN = [09,14]**

09 \* 03 + 14 \* 04 (mod 26) = 5 --> E

09 \* 26 + 14 \* 09 (mod 26) = 22 --> V

**TE = [20, 05]**

20 \* 03 + 05 \* 04 (mod 26) = 2 --> B

20 \* 26 + 05 \* 09 (mod 26) = 19 --> S

**RN = [18, 14]**

18 \* 03 + 14 \* 04 (mod 26) = 6 --> F

18 \* 26 + 14 \* 09 (mod 26) = 22 --> V

**ET = [05, 20]**

05 \* 03 + 20 \* 04 (mod 26) = 17 --> Q

05 \* 26 + 20 \* 09 (mod 26) = 24 --> X

Ghép các chữ cái lại ta được mã **C = JISMEXEVBSFVQX**