**Mã cổ điển**

1, Mật mã Caesar

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

Input: M = SAVEFORARAINYDAY

Key: K = 25

C = ?

M = S A V E F O R A R A

C = R Z U D E N Q Z Q Z

2, Vigenere

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

A, Lặp khóa

Input: M = WHENINROMEDO Key:

K = THETRU

Bài làm

M = WHENINROMEDO

K = THETRUTHETRUT

C = ?

* C = Q P H

B, Autokey

Input: M = BARKINGDOGSS

Key: K = LIKEFA

Tìm Output: C = ?

Bài làm

M = BARKINGDOGSS

K = LIKEFABARKING

C = N J

3, Play fair

Input: M = STILLWATERSR

Key: K = SAVEFORA

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

Key: K = MONEYIS

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

Ta có :

M = STILLWATERSR

=> ST IL LW AT ER SR

Đo với bảng trên ta có

FM KG HZ FN AC AO

C = FMKGHZFNACAO

4, Mã hoán vị

(Trên mạng)

Input: M = TIMEISMONEYTIMEISM

Key: K = 5

Tìm Output: C =

Vì k = 5 nên ta có 5 cột

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| T | I | M | E | I |
| S | M | O | N | E |
| Y | T | I | M | E |
| I | S | M | X | X |

* Viết theo cột ta được C

C = TSYI IMTS MOIM ENMX IEEX

(Của cô) 