**KIỂM TRA BUỔI 6**

**Msv: 18109001**

**Họ tên: Hứa Lăng Mạnh Quang**

**Lớp: TH24.38**

**Câu 2:**  Tìm bản mã của chuỗi sau:

"CONG NGHE THONG TIN"

1. Dùng hệ Ceasar với K=3

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 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 |
| 1 | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | C | O | N | G | N | G | H | E | T | H | O | N | G | T | I | N |  |  |  |  |  |  |  |  |  |  |
| L | Z | L | K | D | K | D | E | B | Q | E | L | K | D | Q | F | K |  |  |  |  |  |  |  |  |  |  |
| R | F | R | Q | J | Q | J | K | H | W | K | R | Q | J | W | L | Q |  |  |  |  |  |  |  |  |  |  |

0: bản gốc

1: bản thay thế

L: left – dịch sang trái k đơn vị

R: dịch sang phải k đơn vị

1. Dùng hệ Playfair với K=”TIN HOC”

Ma trận :

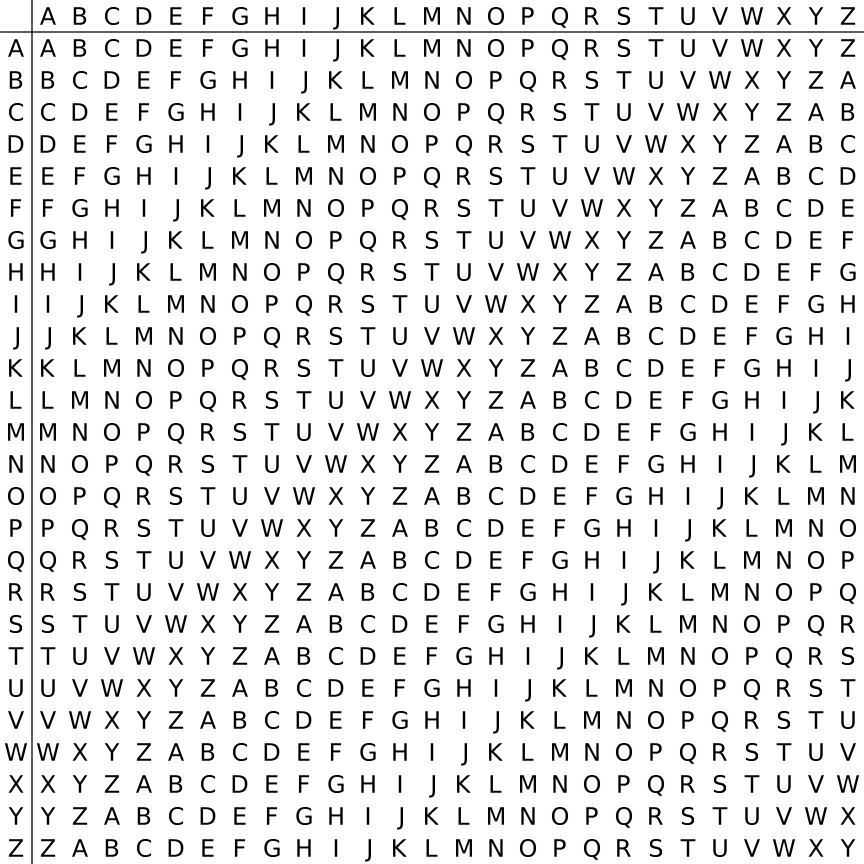
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **T** | **I** | **N** | **H** | **O** |
| **C** | **A** | **B** | **D** | **E** |
| **F** | **G** | **K** | **L** | **M** |
| **P** | **Q** | **R** | **S** | **U** |
| **V** | **W** | **X** | **Y** | **Z** |

**Bản đã mã hóa:**

ETIKIKODIOTHFINH

**Bài 1. *Hệ mã Vigenere***

Cho hệ mã Vigenere có M = 6. Giải mã xâu C = “RANJLV” người ta thu được bản rõ là “CIPHER”.



1. Tìm khóa đã sử dụng của hệ mã trên.

TỪ BẢNG TRÊN TÌM ĐƯỢC MÃ LÀ: LICYTW

1. Dùng khóa tìm được ở phần trên hãy hãy giải mã xâu M = “PLDKCI DUJQJO“.

GIẢI MÃ: atfive oclock

**Bài 3: *Cho hệ mã RSA***

Cho hệ mã RSA có p = 17, q = 19. Chọn số mũ để mã hóa là e = 7.

1. Hãy tìm khóa công khai Kp

N= p\*q = 323

Phi(323)= 288

D = e^-1 mod 288 = 247

* Kp = (e,n) = (7,323)

1. Hãy tìm khóa bí mật Ks

* Ks = (d,n) = (247,323)

1. Cho bản rõ x=22, hãy tìm bản mã y sử dụng định lý phần dư Trung Hoa

Y = x^e mod n = 22^7 mod 323 = 78

1. Cho bản mã y=31, hãy tìm bản rõ x sử dụng thuật toán nhân và bình phương có lặp

X = y^d mod n = 31^247 mod 323 = 164