Họ và tên: **Nguyễn Minh Thám**
MSSV: **1613166**

Cryptography and Network Security
LAB 1

Exercise 1

Giải mã:

- Ciphertext:
  KNXMNSLKWJXMBFYJWGJSIXFIRNYXBTWIKNXMWFSITAJWMJQRNSLFSDIFD
- Chúng ta đếm thì thấy ký tự f xuất hiện 5 lần, nên chúng ta thử f khi giải mã ra với các chữ cái tần suất sử dụng lớn nhất như e,t,a,...
- Thì chúng ta thấy f giải mã thành a có nghĩa nhất => key =5
- Vậy, plaintext là
  FISHINGFRESHWATERBENDSADMITSWORDFISHRANDOVERHELMINGANYDAY
  FISHING FRESHWATER BENDS ADMITSWORD FISHRAND OVER HELMING ANY DAY

a) Việc giải mã khá đơn giản, vì số key khá nhỏ. Ví dụ ở mật mã Caesar chỉ có 26 key có thể xảy ra.
b) Đúng. Bởi vì Caesar cipher là mã hóa khá đơn giản, những kẻ tấn công có thể dễ dàng bẻ khóa bằng các phương thức như vét cạn, thống kê,..
c)

Exercise 2

Theo đề, chữ cái đầu tiên của:

- Plaintext: W $\Rightarrow M_1 = 23$
- Ciphertext: A $\Rightarrow C_1 = 1$

Do đó, ta có: $1 = (23 + K)\ mod\ 26$

$\Rightarrow K = 4$

Vậy key = 4 và plain text là **WORLD CUP**

Exercise 3

Trong bảng sử dụng tần suất tiếng anh, chữ cái e được sử dụng phổ biến nhất và chữ cái sử dụng phổ biến thứ 2 là t. Do đó, ta có:

- Với e = 5, B = 2: $\Rightarrow$2 = (5*a + b) mod 26
- Với t = 20, U = 21:$\Rightarrow$ 21 = (20*a + b) mod 26

Nên, ta có: 19 = 15*a mod 26 $\Rightarrow$ a = 3
Ta cũng có 2 = (5*3 + b) mod 26 $\Rightarrow$ b = 13
Vậy a = 3 và b = 13

Exercise 4

Hai vấn đề của one time pad là:

- Thứ nhất là việc bảo mật sẽ tốt nhất khi chúng ta dùng mỗi key để mã hóa cho 1 tin nhắn. Chúng ta đảm bảo mỗi key được tạo ra một cách ngẫu nhiên và phải có cùng độ dài với plaintext.
- Thứ hai, Chúng ta làm sao để trao đổi các key đó một cách an toàn nhất ?

Exercise 5

Plain text: MUST SEE YOU OVER CADOGAN WEST. COMING AT ONCE.
MU ST SE EY OU OV ER CA DO GA NW ES TC OM IN GA TO NC EX
Cipher text: UZ TB DL GZ PN NW LG TG TU ER OV LD BD UH FP ER HW QS RZ
UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

Exercise 6

a) Không có bất kỳ giới hạn nào cho giá trị b. Bởi vì việc thay đổi giá trị b chỉ làm thay đổi mối quan hệ giữa plaintext và ciphertext sang trái hay sang phải bao nhiêu mà thôi. Nó vẫn đảm bảo việc ánh xạ one - to - one.
b) Các giá trị a không cho phép là 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24 và tất cả các số lớn hơn 25.
c) Số a và 26 phải là 2 số nguyên tố cùng nhau và lớn hơn 1.
Ta có: $E(a,p) = E(a,q)$
$\Rightarrow (a*p+b)\ mod\ 26 = (a*q+b)\ mod\ 26$
$\Rightarrow a(p-q)\ mod\ 26 = 0$
Giả sử a và 26 là 2 số nguyên tố cùng nhau. Nên ta có:
$a(p-q)\ mod\ 26 \neq 0$ (bởi vì a không chia hết cho 26 và (p-q) luôn nhỏ hơn 26
Vì vậy số và 26 phải là 2 số nguyên tố cùng nhau và lớn hơn 1 mới thỏa.

Exercise 7

- *Key 1* = M I N H
  3 2 4 1
  $\Rightarrow$ AVNRYPRSHDSRETSYIOUA
- *Key 2* = T H A M
  4 2 1 3
  $\Rightarrow$ NRSSUVPDTORSRYAAYHEI
  Vậy cipher text là NRSSUVPDTORSRYAAYHEI

Exercise 8

a) Encryption function: $C_i = (P_{i-1} + P_{i-2}) \; mod \; 26$
b) Decryption function: $P_i = (C_{i+1} - P_{i-1}) \; mod \; 26$
c) D : delay element and E: early element