BÀI THỰC HÀNH SỐ 1
Môn: MẬT MÃ & AN NINH MẠNG
-o0o-

Họ tên: Trương Anh Khôi
MSSV: 2211701
Nhóm:

Phần 1. Các hệ mã đối xứng truyền thống
Câu 1:

……

Bảng tần số các ký tự của Ciphertext là:

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	2	0	2	0	5	1	0	5	5	3	2	4	5	0	0	1	2	5	2	0	0	5	5	2	0

Ta thử giải mã bằng cách dịch chuyển 1 bước về bên trái (khóa = 1), sau đó kiểm tra xem đoạn văn đã giải mã có phải là một đoạn văn tiếng Anh hợp lệ hay không. Tiếp tục thử giải mã với các khóa khác nhau, cho đến khi tìm ra bản rõ hợp lệ. Với bản mã ciphertext trên, ta sẽ thu được kết quả giải mã là:

JMWLMRKJVIWLAEXIVFIRHWEHQMXWASVJMWLRVGETHZSIJVIPMKEQRDCBCA

Sau khi kiểm tra, ta thấy đây là một đoạn văn tiếng Anh hợp lệ.
Điểm yếu của hệ mã Caesar là khóa mã hóa chỉ có 25 khóa khác nhau, do đó nó rất dễ bị tấn công bằng phương pháp brute force. Ngoài ra, hệ mã Caesar cũng không thay đổi thứ tự của các ký tự trong văn bản gốc, dẫn đến việc thông tin trong văn bản được mã hoá có thể bị dò mã.

Câu 2:

……

Để giải mã được Ciphertext này, ta cần tìm khoá K. Ta sẽ sử dụng phương pháp thử và sai để tìm khoá.

Vì có 26 ký tự trong bảng chữ cái tiếng Anh nên khoá K có thể có giá trị từ 0 đến 25. Ta thử từng giá trị của khoá K để giải mã ciphertext.

Khi K = 4, ta có plaintext là "wonderful".

Do đó, khoá K là 4 và plaintext là "wonderful".

Cách giải mã này dựa trên việc thử từng giá trị của khoá K để giải mã ciphertext. Điểm yếu của hệ mã thay thế theo công thức **C = (M + K) mod 26** là khoá chỉ có 26 giá trị, do đó việc tìm kiếm khoá sẽ rất dễ dàng khi chúng ta đã biết ciphertext và có thể thử các giá trị khoá.

Câu 3:

……

Ký tự xuất hiện nhiều nhất và nhì trong plaintext tương ứng là E: 5 và T: 20 được mã hoá thành 2 ký tự mới là B: 2 và U: 21 trong cipher text. Ta có hệ phương trình:

$$\mathbf{5a + b = 2 + 26k}$$
$$\mathbf{20a + b = 21 + 26h}$$

Với a, b >= 0 và k, h là các số nguyên dương hoặc 0, (a nguyên tố cùng nhau với 26).
Thử với k = 1, h =2. Tính được a = 3, b = 13

Câu 4:

…….

Mật mã One-time Pad là một phương pháp mã hóa được coi là hoàn hảo, tức là không thể bị phá vỡ nếu được thực hiện đúng cách. Tuy nhiên, vẫn tồn tại hai vấn đề đối với mật mã One-time Pad:

- Đòi hỏi phải có khoảng trống bằng nhau giữa khoá và thông điệp: Việc mã hóa và giải mã One-time Pad yêu cầu có một khoảng trống bằng nhau giữa chiều dài của khoá và thông điệp. Điều này có nghĩa là nếu thông điệp không đủ dài, hoặc nếu khoá không đủ dài, thì việc sử dụng One-time Pad sẽ không khả thi.
- Độ dài khoá phải bằng hoặc lớn hơn độ dài của thông điệp: Mật mã One-time Pad yêu cầu một khoá ngẫu nhiên và duy nhất cho mỗi thông điệp được mã hóa. Khoá phải có độ dài bằng hoặc lớn hơn độ dài của thông điệp. Nếu khoá quá ngắn, thì việc mã hóa không thể được thực hiện đúng cách và thông điệp có thể bị phá vỡ.

Câu 5:

…….

MUST SEE YOU OVER CADOGAN WEST. COMING AT ONCE.

MU = UZ
ST = TB
SE = DL
EY = GZ
OU = PN
OV = NW
ER = LG
CA = TG
DO = TU
GA = ER
NW = OV
ES = LD
TC = BD
OM = UH
IN = FP
GA = ER
TO = HW
NC = QS
E = EX = RZ

`Must see you over Cadogan West. Coming at once.`

Được mã hoá thành: **UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ**

Câu 6:

……..……..…….

key1 = ANH
key2 = KHOI

- Đầu tiên chọn key1 và viết nội dung bản rõ dưới key1 theo hàng và đánh số key1 theo thứ tự bảng chữ cái tiếng anh, chữ nào trùng thì đánh số nhỏ hơn với chữ đứng trước:

	1	3	2
Key1	**A**	**N**	**H**
	S	P	Y
	A	R	R
	I	V	E
	S	O	N
	T	H	U
	R	S	D
	A	Y	X

- Lấy các ký tự ra theo cột, bắt đầu từ cột có chỉ số thấp nhất, ta được cột 1 đến 3 là:

SAISTRA YRNEUDX PRVOHSY

- Chọn key2, đánh số cột như key1 và viết nội dung các cột đã tính được lúc trước vào bảng mới theo hàng:

	3	1	4	2
Key2	**K**	**H**	**O**	**I**
	S	A	I	S
	T	R	A	Y
	R	N	E	U
	D	X	P	R
	V	O	H	S
	Y	X	X	X

- Lại lấy các ký tự ra theo cột, bắt đầu từ cột có chỉ số thấp nhất, chia thành nhóm 4 chữ cái, ta được:

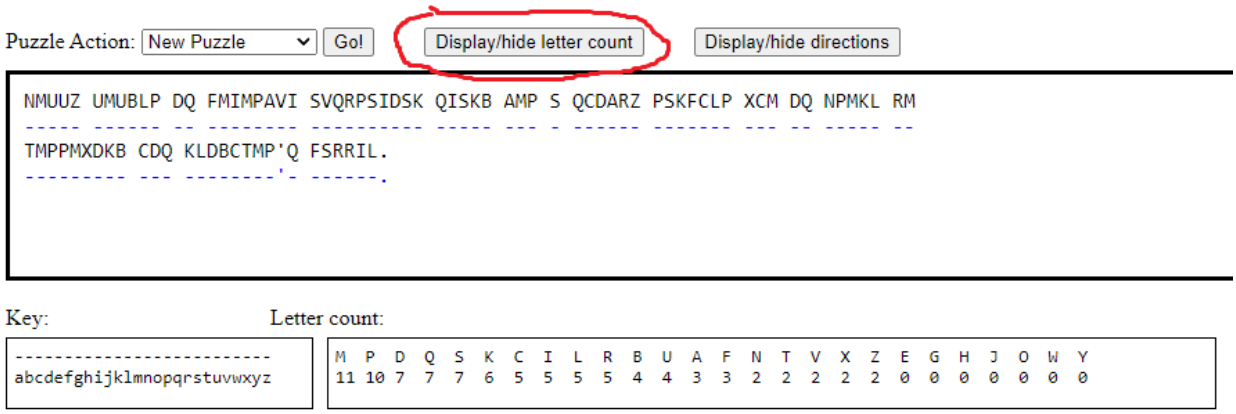
saistrayrneudXprvohsyXXX

Vậy cipher text là: **arnXoXsyursXstrdvyiaephX**

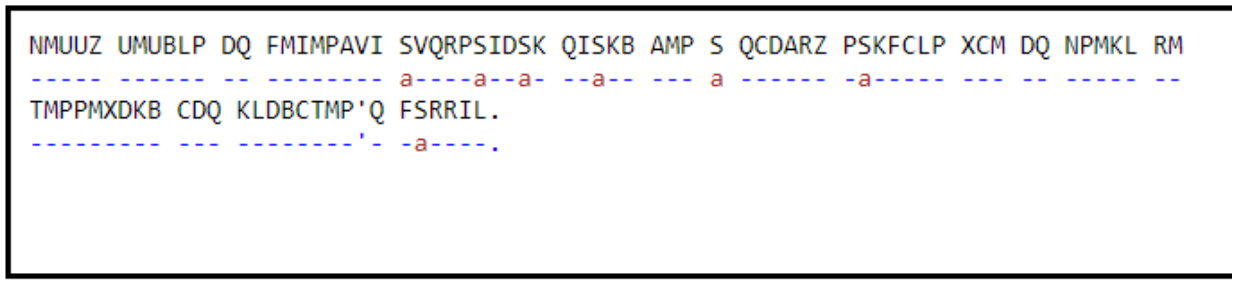
Câu 7:

……..……..…….

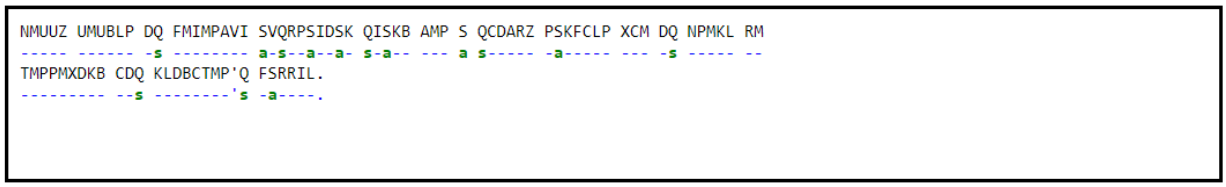
Nhấn vào display/hide letter count để hiện ra bảng tần số các ký tự trong cipher text:



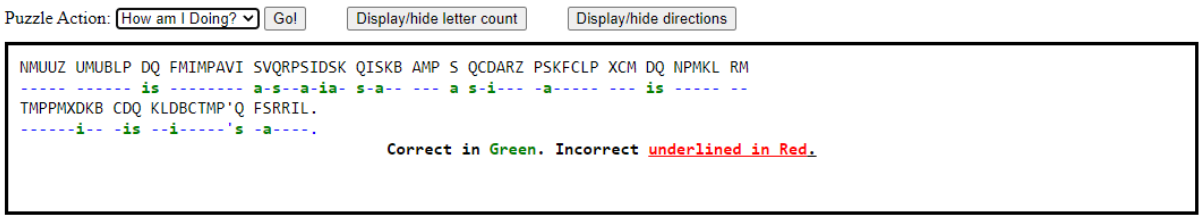
- Xét từ thứ 8 là từ S, trong tiếng anh chỉ có 2 từ có 1 ký tự là A và I, do đó ta giả sử 2 trường hợp là bản rõ là A và I, biến đổi thành bản mã là S:
  - Giả sử bản rõ là A, khi đó ta bấm chữ S trên Cipher letter và chữ a trên Goes to plain letter để biến S thành a:



  - Ký tự Q xuất hiện với số lần xem như xếp thứ 3 đến 5 (7 lần bằng với D và S), và trước nó là 1 dấu nháy đơn nên bản rõ của nó có thể là **S, T, D, M** theo thứ tự phổ biến, nên ta giả sử bản rõ của Q là s:



  - Xét chữ D có độ phổ biến là từ 3 đến 5, ta lần lượt thay nó bằng các ký tự: **E, T, A, O, N, I** rồi chọn mục How am I Doing?
    Để check đúng sai:



  - Xét ký tự M có độ phổ biến cao nhất, tương tự ta lần lượt thay nó bằng các ký tự:

E, T, A, O, N, I, S, R rồi bấm Go! Để check:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--- -o---- is -o-o---- a-s--a-ia- s-a-- -o- a s-i--- -a----- --o is --o-- -o
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
-o--o-i-- -is --i---o-'s -a----.
                                    Correct in Green. Incorrect underlined in Red.
```

- Đến ký tự P

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--- -o---r is -o-or--- a-s-ra-ia- s-a-- -or a s-i--- ra----r --o is -ro-- -o
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
-orro-i-- -is --i---or's -a----.
                                    Correct in Green. Incorrect underlined in Red.
```

- Thử đoán AMP thành for:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--- -o---r is -o-orf-- a-s-ra-ia- s-a-- for a s-if-- ra----r --o is -ro-- -o
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
-orro-i-- -is --i---or's -a----.
                                    Correct in Green. Incorrect underlined in Red.
```

- Xét từ **TMPPMXDKB** nó có đuôi là i-- nên ta có thể đoán nó có thể là ing hoặc ion:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--- -o-g-r is -o-orf-- a-s-ra-ian s-ang for a s-if-- ran---r --o is -ron- -o
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
-orro-ing -is n-ig--or's -a----.
                                    Correct in Green. Incorrect underlined in Red.
```

- Xét từ **TMPPMXDKB** có dạng -orro-ing, chúng ta đoán nó là borrowing:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--- -o-g-r is -o-orf-- a-s-ra-ian s-ang for a s-if-- ran---r w-o is -ron- -o
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
borrowing -is n-ig-bor's -a----.
                                    Correct in Green. Incorrect underlined in Red.
```

- Xét từ CDQ có dạng -is, chúng ta đoán nó là his:

- Xét từ **KLDBCTMP'Q** có dạng n-ighbor's , chúng ta đoán nó là neighbor's:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--- -o-ger is -o-orf-- a-s-ra-ian s-ang for a shif-- ran-her who is -rone -o
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
borrowing his neighbor's -a---e.
                                    Correct in Green. Incorrect underlined in Red.
```

- Xét từ RM có dạng -o, chúng ta thử thay các phụ âm vào chỗ -, được kết quả:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--- -o-g-r is -o-orf-- a-s-ra-ian s-ang for a shif-- ran-h-r who is -ron- -o
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
borrowing his n-ighbor's -a----.
                                    Correct in Green. Incorrect underlined in Red.
```

- Xét từ SVQRPSIDSK có dạng a-stra-ian, chúng ta đoán từ này là australian:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--- -o-ger is -o-orf-- a-stra-ian s-ang for a shift- ran-her who is -rone to
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
borrowing his neighbor's -att-e.
                                    Correct in Green. Incorrect underlined in Red.
```

- Xét từ FMIMPAVI có dạng -olorful, đoán nó là colorful:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--- -o-ger is colorful australian slang for a shift- rancher who is -rone to
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
borrowing his neighbor's cattle.
                                    Correct in Green. Incorrect underlined in Red.
```

- Đoán QCDARZ là shifty:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--- -o-ger is -olorful australian slang for a shift- ran-her who is -rone to
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
borrowing his neighbor's -attle.
                                    Correct in Green. Incorrect underlined in Red.
```

- Đoán NPMKL là prone:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
-o--y -o-ger is colorful australian slang for a shifty rancher who is -rone to
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
borrowing his neighbor's cattle.
                                    Correct in Green. Incorrect underlined in Red.
```

- Đoán U là d:

```
NMUUZ UMUBLP DQ FMIMPAVI SVQRPSIDSK QISKB AMP S QCDARZ PSKFCLP XCM DQ NPMKL RM
poddy dodger is colorful australian slang for a shifty rancher who is prone to
TMPPMXDKB CDQ KLDBCTMP'Q FSRRIL.
borrowing his neighbor's cattle.
                                    Correct in Green. Incorrect underlined in Red.
```

Phần 2. Chuẩn mã hoá dữ liệu DES

Câu 1:

……

Sự khác biệt chính giữa mã hoá khối và mã hoá dòng là mã hoá khối mã hóa và giải mã một khối văn bản tại một thời điểm, mã hóa dòng mã hóa và giải mã văn bản bằng cách lấy một byte của văn bản tại một thời điểm.

Câu 2:

Thông điệp: **0 1 2 3 4 5 6 7 8 9 A B C D E F**

Khoá: **0 1 2 3 4 5 6 7 8 9 A B 1 7 0 1**

a) Tính khoá con K1 được sử dụng cho vòng mã hoá đầu tiên

1. Chuyển Key (K) sang 64-bit Binary:

K = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 0001 0111 0000 0001

2. Áp dụng Hoán vị PC-1 (56-bit): Thực hiện chọn các bit 57, 49, 41,... từ K, ta được khóa 56-bit K^+ :

K^+ = 0011000 0000010 0001100 1100011 0101111 1011011 1000100 0001001

3. Chia thành C_0 và D_0 (mỗi bên 28-bit):

C0 = 0011000 0000010 0001100 1100011

D0 = 0101111 1011011 1000100 0001001

4. Dịch trái 1 bit (Vòng 1):

C1 = 0110000 0000100 0011001 1000110

D1 = 1011111 0110111 0001000 0010010

5. Nối C1D1 và áp dụng Hoán vị PC-2 (48-bit): Thực hiện chọn các bit 14, 17, 11,... từ C1D1, ta được khóa con K1:

K1 = 000000 100000 110010 001101 101100 110100 101010 000001

b) Plaintext (M) (Binary):

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

1. Áp dụng Hoán vị ban đầu (IP):

IP = 1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 1010 1010 1111 0000 1010 1010 11

2. Chia L0 và R0 (mỗi bên 32-bit):

L0 = 1100 1100 0000 0000 1100 1100 1111 1111

R0 = 1111 0000 1010 1010 1111 0000 1010 1010

c) Áp dụng Bảng chọn bit E (E Bit-Selection Table) 17 để mở rộng R0 từ 32-bit lên 48-bit:

E[R0] = 011110 100001 010101 010101 011110 100001 010101 010101

d) Thực hiện phép toán XOR bit-với-bit:

E[R0] = 011110 100001 010101 010101 011110 100001 010101 010101

K1 = 000000 100000 110010 001101 101100 110100 101010 000001

XOR A = 011110 000001 100111 011000 110010 010101 111111 010100

e) Chia 48-bit kết quả ở câu d và chia thành các nhóm 6 bit, thực hiện tính toán trên từng nhóm 6 bit thông qua S-box, ghi lại kết quả.

Ta chia A thành 8 khối 6-bit (B_1 đến B_8) và tra bảng S-box:

$B_1 = 011110 \rightarrow$ (S-Box 1) $\rightarrow$ Hàng (00) Cột (1111) $\rightarrow$ 7 $\rightarrow$ `0111`

$B_2 = 000001 \rightarrow$ (S-Box 2) $\rightarrow$ Hàng (01) Cột (0000) $\rightarrow$ 13 $\rightarrow$ `1101`

$B_3 = 100111 \rightarrow$ (S-Box 3) $\rightarrow$ Hàng (11) Cột (0011) $\rightarrow$ 13 $\rightarrow$ `1101`

$B_4 = 011000 \rightarrow$ (S-Box 4) $\rightarrow$ Hàng (00) Cột (1100) $\rightarrow$ 12 $\rightarrow$ `1100`

$B_5 = 110010 \rightarrow$ (S-Box 5) $\rightarrow$ Hàng (10) Cột (1001) $\rightarrow$ 15 $\rightarrow$ `1111`

$B_6 = 010101 \rightarrow$ (S-Box 6) $\rightarrow$ Hàng (01) Cột (1010) $\rightarrow$ 0 $\rightarrow$ `0000`

$B_7 = 111111 \rightarrow$ (S-Box 7) $\rightarrow$ Hàng (11) Cột (1111) $\rightarrow$ 3 $\rightarrow$ `0011`

$B_8 = 010100 \rightarrow$ (S-Box 8) $\rightarrow$ Hàng (00) Cột (1010) $\rightarrow$ 5 $\rightarrow$ `0101`

Kết quả sau S-box: 0111 1101 1101 1100 1111 0000 0011 0101

f) Nối các kết quả tính được ở câu e thành chuỗi kết quả 32-bit, ghi lại kết quả dưới dạng binary (B)

B = 0111 1101 1101 1100 1111 0000 0011 0101

g) Áp dụng hoán vị P 24 (chọn bit 16, 7, 20,...) cho chuỗi B:

P(B) = 0000 0111 0000 1111 1101 1011 1101 0010

h) Thực hiện phép toán XOR:

P(B) = 0000 0111 0000 1111 1101 1011 1101 0010

L0 = 1100 1100 0000 0000 1100 1100 1111 1111

XOR R1 = 1100 1011 0000 1111 0001 0111 0010 1101

i) Kết quả của vòng 1 là L1R1 trong đó L1 = R0

- L1 = R0 = 1111 0000 1010 1010 1111 0000 1010 1010
- R1 = 1100 1011 0000 1111 0001 0111 0010 1101

Kết quả vòng 1 (Binary):1111 0000 1010 1010 1111 0000 1010 1010 1100 1011 0000 1111 0001 0111 0010 1101

Kết quả vòng 1 (Hex): F0AA F0AA CB0F 172D