BÀI THỰC HÀNH SỐ 1

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Nguyễn Hữu Bảo**

**MSSV: 1811523**

**Nhóm: L01**

**Phần 1. Các hệ mã đối xứng truyền thống**

**Câu 1:**

Bảng tần số các ký tự của cipher text là:





ở đây 7 ký tự F,I,J,N,S,W,X có tần số xuất hiện cao nhất là 5. Còn ký tự M có tần số xuất hiện là 4 nên coi như nó có tần số xuất hiện là 8, nên có thể giả sử rằng ký tự xuất hiện với tần số cao thứ 8 trong tiếng anh là H đã được mã hoá thành M, do đó khoá k là 5

khi đó, plain text là:

FISHINGFRESHWATERBENDSADMITSWORDFISHRANDOVERHELMINGANYDAY

Text này có nhiều từ có nghĩa nên coi như nó là plain text

**Câu 2:**

Do cipher text ngắn nên chúng ta không thể dùng tần số xuất hiện ký tự để giải mã được, mà phải vùng phương pháp thử khoá k từ 1 đến 25 để xem xem plain text có nghĩa trong tiếng anh không

Các plain text với các giá trị k tương ứng là:

k=1 ZRUOGFXS

k=2 YQTNFEWR

k=3 XPSMEDVQ

k=4 WORLDCUP

k=5 VNQKCBTO

k=6 UMPJBASN

k=7 TLOIAZRM

k=8 SKNHZYQL

k=9 RJMGYXPK

k=10 QILFXWOJ

k=11 PHKEWVNI

k=12 OGJDVUMH

k=13 NFICUTLG

k=14 MEHBTSKF

k=15 LDGASRJE

k=16 KCFZRQID

k=17 JBEYQPHC

k=18 IADXPOGB

k=19 HZCWONFA

k=20 GYBVNMEZ

k=21 FXAUMLDY

k=22 EWZTLKCX

k=23 DVYSKJBW

k=24 CUXRJIAV

k=25 BTWQIHZU

với k=4, ta thấy plain text là world cup là từ có nghĩa

**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 pt:

a\*5 + b = 2 + 26k

a\*20 + b = 21 + 26h

với a,b>=0,k ,h là các số nguyên dương hoặc 0, và a nguyên tố cùng nhau với 26.

thử với k = 1, h =2. Tính được a =3, b= 13

**Câu 4:**

* Pad phải là truly random và phải có độ dài ít nhất bằng với plaintext
* Phía gửi và phía nhận đều phải biết nội dung của pad và phải giữ kín không để lộ cho bên thứ ba

**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=HUU

key2=BAO

* 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 | 2 | 3 |
| **Key** | **H** | **U** | **U** |
|  | S | P | Y |
|  | A | R | R |
|  | I | V | E |
|  | S | O | N |
|  | T | H | U |
|  | R | S | D |
|  | A | Y |  |

* Lấy các ký tự ra theo cột, bắt đầu từ cột có chỉ số thấp nhất, ta được cột 1 đến 3 là SAISTRA, PRVOHSY,YRENUD
* Chọn key2, đánh số cột như key1 và viết nội dung các cột đã tính được lúc trước vào bảng mới theo hàng:

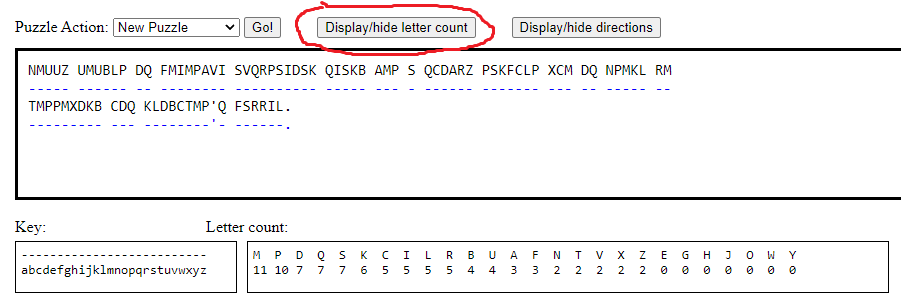
|  |  |  |  |
| --- | --- | --- | --- |
|  | 2 | 1 | 3 |
| **Key** | **B** | **A** | **O** |
|  | S | A | I |
|  | S | T | R |
|  | A | P | R |
|  | V | O | H |
|  | S | Y | Y |
|  | R | E | N |
|  | U | D |  |

* Lại lấy các ký tự ra theo cột, bắt đầu từ cột có chỉ số thấp nhất, chia thành nhóm 5 chữ cái, ta được: ATPOY EDSSA VSRUI RRHYN

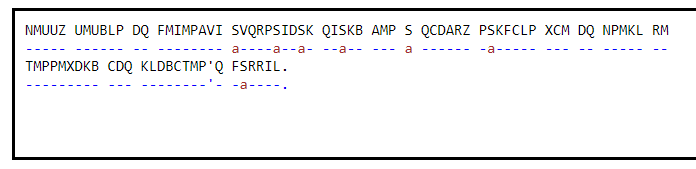
Vậy cipher text là: ATPOY EDSSA VSRUI RRHYN

**Câu 7:**

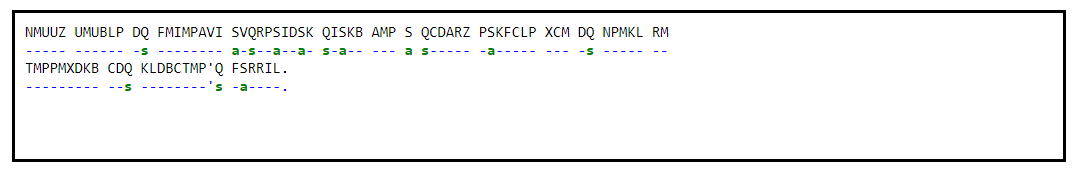
* Nhấn vào display/hide letter count để hiện ra bảng tần số các ký tự trong cipher text:



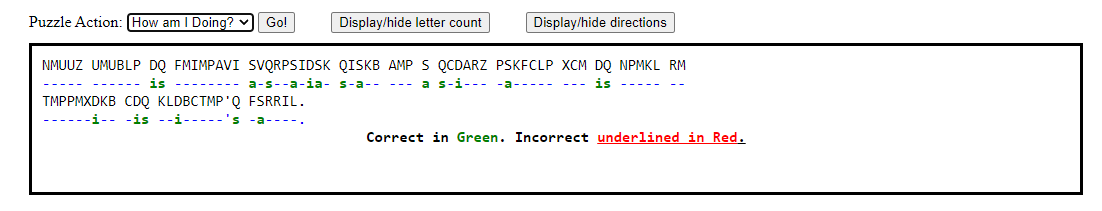
* Xét từ thứ 8 là từ S, trong tiếng anh chỉ có 2 từ có 1 ký tự là A và I, do đó ta giả sử 2 trường hợp là bản rõ là A và I, biến đổi thành bản mã là S
  + Giả sử bản rõ là A, khi đó ta bấm chữ S trên Cipher letter và chữ a trên Goes to plain letter để biến S thành a:



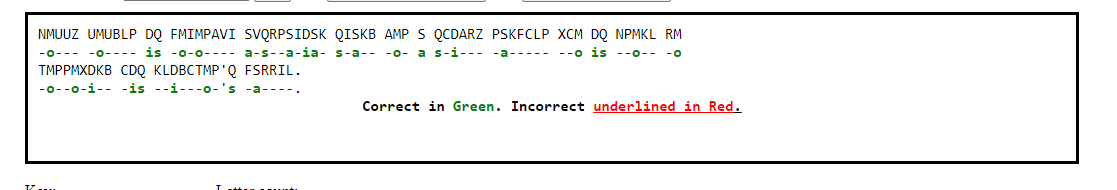
* + Ký tự Q xuất hiện với số lần xem như xếp thứ 3 đến 5 (7 lần bằng với D và S), và trước nó là 1 dấu nháy đơn nên bản rõ của nó có thể là S,T,D,M theo thứ tự phổ biến, nên ta giả sử bản rõ của Q là s:



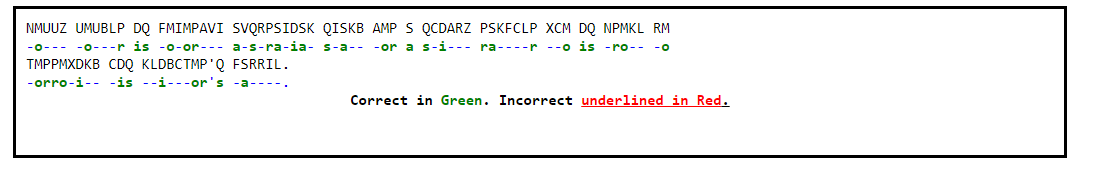
* + Xét chữ D có độ phổ biến là từ 3 đến 5, ta lần lượt thay nó bằng các ký tự E,T,A,O,N,I rồi chọn mục How am I Doing? Để check đúng sai:



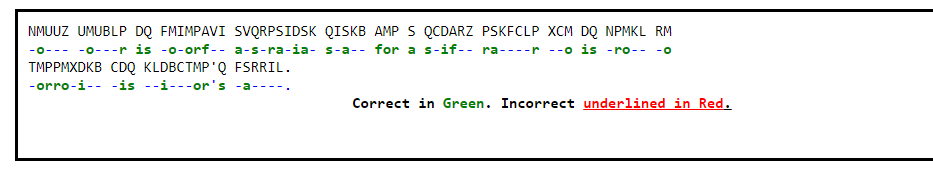
* + Xét ký tự M có độ phổ biến cao nhất, tương tự ta lần lượt thay nó bằng các ký tự E,T,A,O,N,I,S,R rồi bấm Go! Để check:



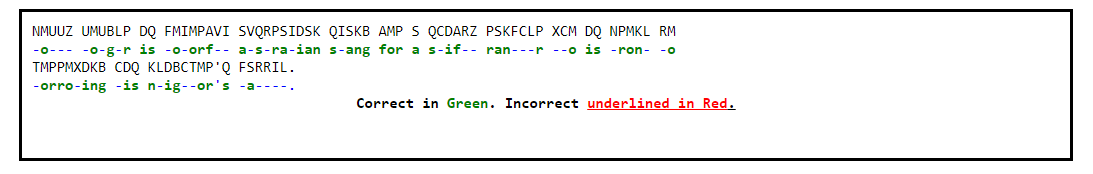
* + Đến ký tự P



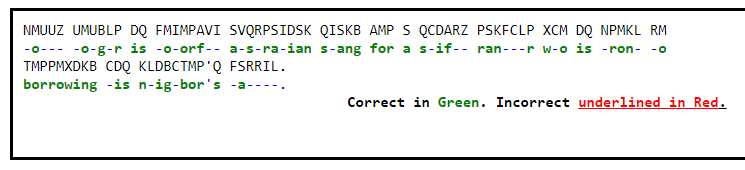
* + Thử đoán AMP thành for:



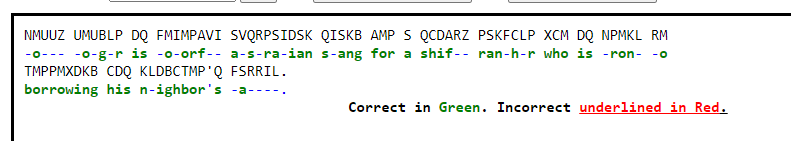
* + Xét từ TMPPMXDKB nó có đuôi là i-- nên ta có thể đoán nó có thể là ing hoặc ion:



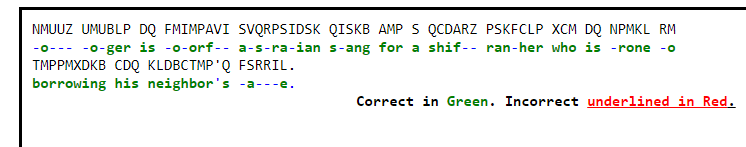
* + Xét từ TMPPMXDKB có dạng -orro-ing, chúng ta đoán nó là borrowing:



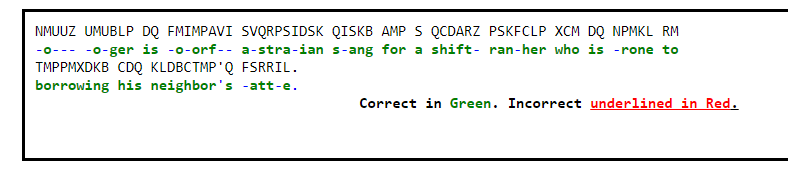
* + Xét từ CDQ có dạng -is, chúng ta đoán nó là his:



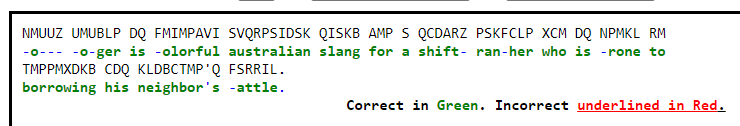
* + Xét từ KLDBCTMP'Q có dạng n-ighbor's , chúng ta đoán nó là neighbor's:



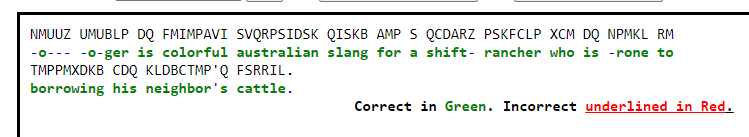
* + Xét từ RM có dạng -o, chúng ta thử thay các phụ âm vào chỗ -, được kết quả:



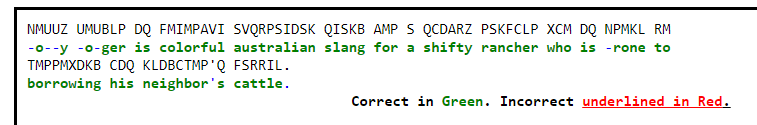
* + Xét từ SVQRPSIDSK có dạng a-stra-ian, chúng ta đoán từ này là australian:



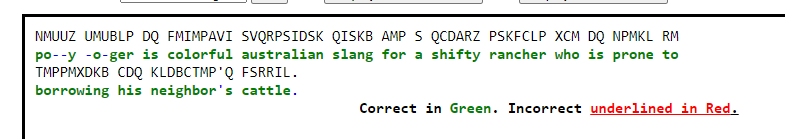
* + Xét từ FMIMPAVI có dạng -olorful, đoán nó là colorful:



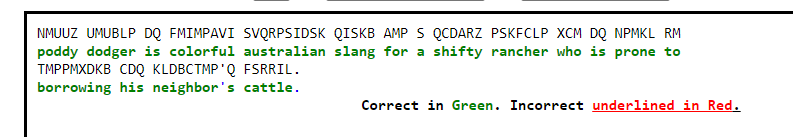
* + Đoán QCDARZ là shifty:



* + Đoán NPMKL là prone:



* + Đoán U là d:



**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 5 2 3

a.

M = 0000000100100011010001010110011110001001101010111100110111101111

K = 0000000100100011010001010110011110001001101010110001010100100011

K+ = 00110000000011001010101001001010101001001100001100000000

C0 = 0011000000001100101010100100

D0 = 1010101001001100001100000000

C1 = 0110000000011001010101001000

D1 = 0101010010011000011000000001

C1D1 = 01100000000110010101010010000101010010011000011000000001

K1 = 000000100000001000100111100110110000000110100001

b.

IP = 1100110000000000110011001111111111110000101010101111000010101010

L0 = 11001100000000001100110011111111

R0 = 11110000101010101111000010101010

c.

E[R0] = 011110100001010101010101011110100001010101010101

d.

A = 011110000001011101110010111000010001010011110100

e.

B1 = 011110

B2 = 000001

B3 = 011101

B4 = 110010

B5 = 111000

B6 = 010001

B7 = 010011

B8 = 110100

S1(B1) = 0111

S2(B2) = 0011

S3(B3) = 1111

S4(B4) = 0001

S5(B5) = 0110

S6(B6) = 0110

S7(B7) = 0011

S8(B8) = 1010

f.

B = 01110011111100010110011000111010

g.

f = P(B) = 11001110001001111100011110001110

h.

R1 = 00000010001001110000101101110001

i.

L1 = R0

R1L1 = 0000001000100111000010110111000111110000101010101111000010101010

Ciphertext sau vòng thứ 1:

00010101011101100001000000100110100010011011101110001001101010102

Đổi sang hex là:

1576102689BB89AA16