Thành viên 1: Thái Hoàng Nhân

ID: 18520326

Thành viên 2: Nguyễn Đức Phú

ID: 18520333

**Bài thực hành Lab1- Nhóm 7**

**Task 1.1.1:**

* :

+ Số 0 là đáp án và đứng sai vị trí (ở hình là vị trí 3)

* Số 0 đứng ở 1 hoặc 2.

+ Không có số 7, 3, 8

* :

Số 0 là đáp án nhưng sai vị trí (ở hình là vị trí thứ 2)

* Số 0 đứng ở 1.
* :
* Số 2 là đáp án và đứng ở 3
* :

Do số 0 đứng ở 1 và số 2 đứng ở 3

* Không có số 6
* :

Nếu số 1 là đáp án => số 1 đứng ở 1 hoặc 3 (là vị trí của số 0 và 2)

* Không có số 1
* Số 4 đứng ở giữa.

Vậy đáp án là 042.

**Task 1.1.2:**

* ♥ ♠ ♦ ♣    
* Với 4 số tự nhiên bất kì (từ 0 đến 9): tổng của nó luôn <= 36

Từ cột 3, 4 và hàng 2 => • và ♦ = 1 hoặc ♦ = 2 hoặc ♦ = 3 (1)

* Từ cột 3: 2 + 2♠ = •• => •• phải là số chẵn (2)

(1) + (2) => • = 2

=> ♦ = 1 hoặc ♦ = 3

+) Xét ♦ = 1:

Hàng 2: 3♥ + ♠ = 11

=> ♥ = (11 - ♠) / 3 => ♥ là số chia hết cho 3

=> ♠ = 2 hoặc ♠ = 5 hoặc ♠ = 8

Nếu ♠ = 2 => loại (vì • = 2)

Nếu ♠ = 5 => loại (vì ♥ = 2 mà • = 2)

Nếu ♠ = 8 => loại (vì ♥ = 1 mà đang xét trường hợp ♦ = 1)

🡺 ♦ = 3

=> Hàng 2: 3♥ + ♠ = 33

=> ♥ = (33 - ♠) / 3 => ♥ là số chia hết cho 3

=> ♠ = 3 hoặc ♠ = 6 hoặc ♠ = 9

Nếu ♠ = 3 => loại (vì ♥ = 10)

Nếu ♠ = 9 => loại (vì ở cột 3:  = 2 mà • = 2)

🡺 ♠ = 6

🡺 ♥ = 9

* Từ cột 3: 2 + 2♠ = 22

🡺  = 5

Lúc này ta đã có giá trị của • = 2, ♦ = 3,  = 5, ♠ = 6, ♥ = 9

* Từ cột 4:  + 2♥ + ♣ = •♦

⬄  + 18 + ♣ = 23

⬄  + ♣ = 5

=> Có 2 trường hợp xảy ra đối với  và ♣: 1/  = 1 và ♣ = 4 (\*)

2/  = 1 và ♣ = 4

=> Có 2 trường hợp xảy ra đối với  và : 1/  = 7 và  = 8

2/  = 8 và  = 7 (\*\*)

Ta xét cột 1, cột 2, hàng 3, hàng 4 có hệ phương trình sau:

+ ?1 + ?2 = 20

+ ?3 = 15

?1+ ?3 + ♣ = 17

?2 -  = -4

Xét trường hợp (\*\*), khi đó:

?1 = 9

?3 = 7

♣ = 1 =>  = 4 (Thỏa (\*))

?2 = 3

🡺 Vậy kết quả của bài toán là:

♣ = 1, • = 2, ♦ = 3,  = 4,  = 5, ♠ = 6,  = 7,  = 8, ♥ = 9

**Task 1.2: (source code được đính kèm trong file .zip)**



**Task 1.3:**

**Ciphertext:**

Crbcyr jub fhpprrq unir zbzraghz. Gur zber gurl fhpprrq, gur zber gurl jnag gb fhpprrq naq gur zber gurl svaq n jnl gb fhpprrq. Fvzvyneyl, jura fbzrbar vf snvyvat, gur graqrapl vf gb trg ba n qbjajneq fcveny gung pna rira orpbzr n frysshysvyyvat cebcurpl.

**Plain text:**

People who succeed have momentum. The more they succeed, the more they want to succeed and the more they find a way to succeed. Similarly, when someone is failing, the tendency is to get on a downward spiral that can even become a self-fulfilling prophecy.

**\*\*\* Điểm đặc biệt \*\*\***  
Đây là đoạn thông điệp được mã hóa bằng phương pháp mã hóa Caesar với key = 13 (hay còn được gọi với tên gọi ROT13). Loại mã hóa này đặc biệt ở chỗ sau khi plaintext được mã hóa tạo thành ciphertext, thì có thể dùng chính ciphertext vừa được mã hóa tiếp tục sử dụng thuật toán mã hóa với key = 13 sẽ trở lại thành plaintext ban đầu.

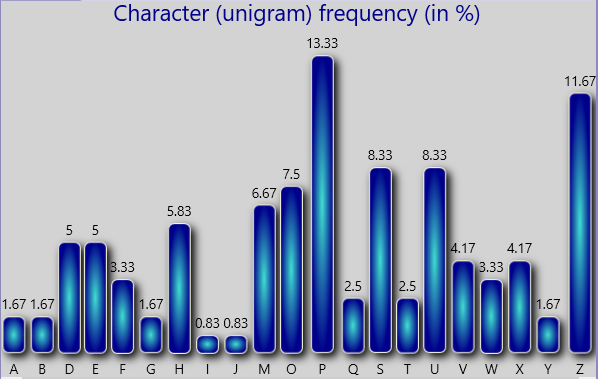
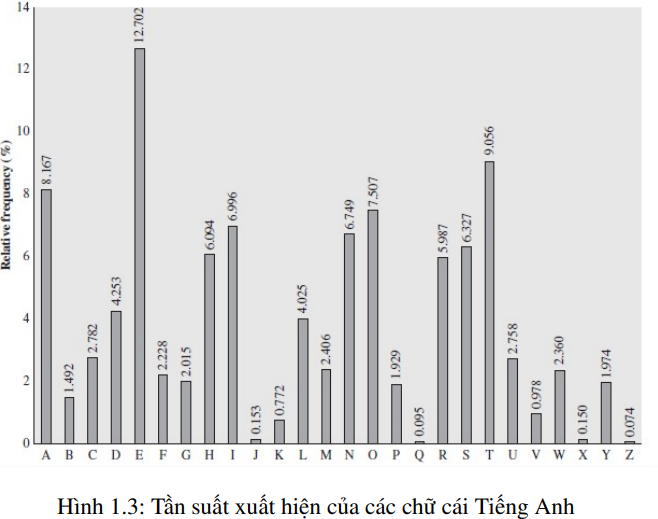
**Task 1.4:**

**Ciphertext:**

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZVUEP HZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFP OMBZWPFUPZHMDJUDTMOHMQ

**Plaintext:**

IT WAS DISCLOSED YESTERDAY THAT SEVERAL INFORMAL BUT DIRECT CONTACTS HAVE BEEN MADE WITH POLITICAL REPRESENTATIVES OF THE VIETCONG IN MOSCOW



Dựa vào tần suất xuất hiện của các ký tự trong ciphertext và tần suất xuất hiện phổ biến của các chữ cái trong bảng chữ cái Tiếng Anh, ta có thể đoán P là mã hóa của E, Z là mã hóa của T. Cứ tiếp tục với cái cụm từ có 2, 3 kí tự ta sẽ có được bản giải mã.

**Task 1.5:**

**Ciphertext:**

GSVFMREVIHRGBLURMULINZGRLMGVXSMLOLTBRHZNVNYVILUE RVGMZNMZGRLMZOFMREVIHRGBSLXSRNRMSXRGBEMFSXNZMW RHGSVLMOBFMREVIHRGBLUERVGMZNGSZGFMWVIGZPVHRMULI NZGRLMZMWXLNNFMRXZGRLMGVXSMLOLTBIVHVZIXSZMWULX FHVWRMWVKGSGIZRMRMTGSVFMREVIHRGBSZHGSVBLFMTVHG NZMZTVNVMGIVHVZIXSZMWGVZXSRMTHGZUULUZMBEMFSXNN VNYVIYIRMTRMTTIVZGVMGSFHRZHNZOLMTDRGSWBMZNRXZM WXIVZGREVZWEZMGZTVH

**Plaintext:**

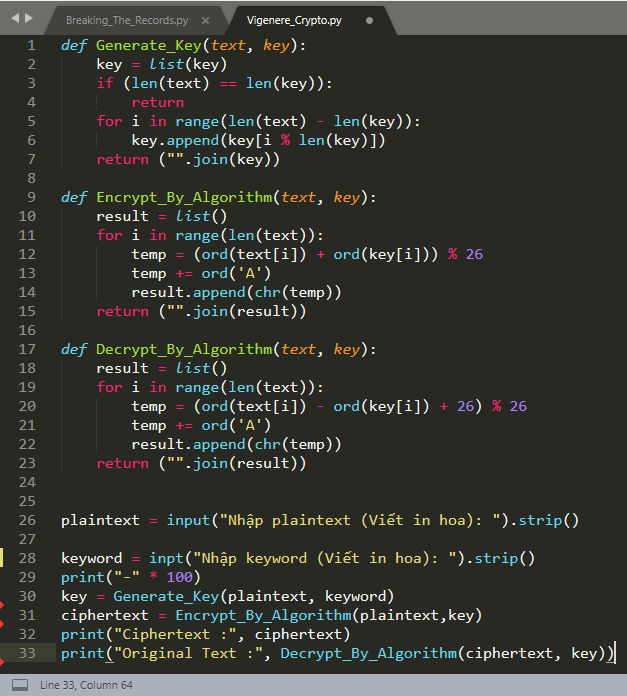
THE UNIVERSITY OF INFORMATION TECHNOLOGY IS A MEMBER OF VIETNAM NATIONAL UNIVERSITY HOCHIMINH CITY (VNU-HCM) AND IS THE ONLY UNIVERSITY OF VIETNAM THAT UNDERTAKES INFORMATION AND COMMUNICATION TECHNOLOGY RESEARCH AND FOCUSED IN DEPTH TRAINING. THE UNIVERSITY HAS THE YOUNGEST MANAGEMENT RESEARCH AND TEACHING STAFF OF ANY VNU-HCM MEMBER BRINGING GREAT ENTHUSIASM ALONG WITH DYNAMIC AND CREATIVE ADVANTAGES.

**\*\*\* Điểm đặc biệt \*\*\***

Phương pháp Monoalphabetic tổng quát hóa phương pháp Caesar. Tuy nhiên, không phải là dịch chuyển k vị trí các chữ cái A, B,C, … mà là một hoán vị của 26 chữ cái này.

Điểm đặc biệt là bảng kí tự được sử dụng làm khóa cho đoạn cipher text gần nhưng tương tự với bảng anphabet đảo ngược (vẫn có vài vị trí không đúng).

**Task 1.6: (source code được đính kèm trong file .zip)**

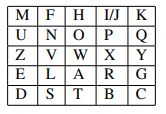


**Task 1.7:**

**Plain text:**

Must see you over Cadogan West. Coming at once.

**Bảng Playfair:**

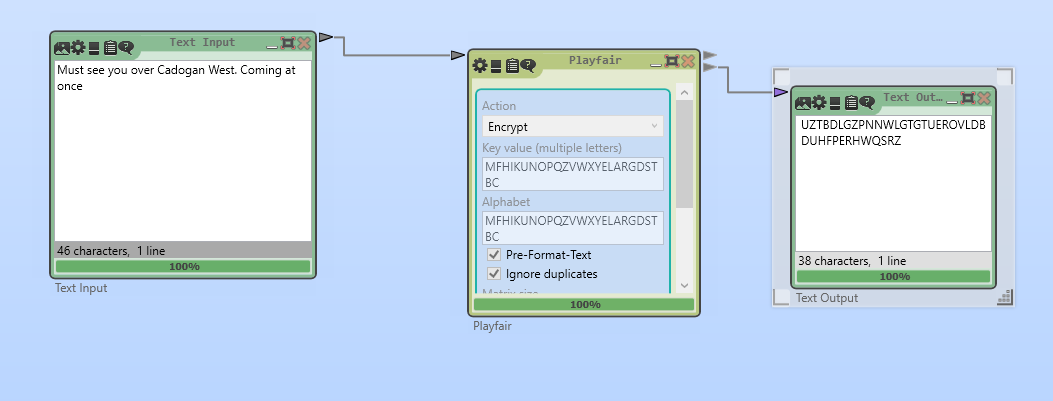


**Quy tắc mã hoá:**

Xử lý từng cặp 2 ký tự liên tiếp kế bên nhau. Nếu dư 1 ký tự, thêm **"x"** vào cuối. Trường hợp 2 ký tự nằm cùng dòng, thay thế bằng 2 ký tự tương ứng bên phải của từng ký tự. Trường hợp ký tự nằm ở cột cuối cùng thì thay bằng ký tự ở cột đầu tiên. Trường hợp 2 ký tự nằm cùng cột, thay thế bằng 2 ký tự bên dưới của từng ký tự. Trường hợp ký tự ở hàng cuối cùng thì thay bằng ký tự ở hàng trên cùng. Nếu 2 ký tự chéo nhau lập thành hình chữ nhật thì thay bằng 2 ký tự tương ứng ở hai đỉnh còn lại.

**Ciphertext:**

UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ



**Task 1.8:**

**Key:**

royal new Zealand navy

**Bảng Playfair:**

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

**Plaintext:** PTBOATONEOWENINELOSTINACTIONINBLACKESUSUSTRAITTWOMILESSWMERESUCOVEXCREWOFTWELVEXREQUESTANYINFORMATIONX

**Message:**

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION.

**Task 1.9:**

**Ciphertext:**

4C6520666C6167206465206365206368616C6C656E6765206573743A2 03261633337363438316165353436636436383964356239313237356433323465

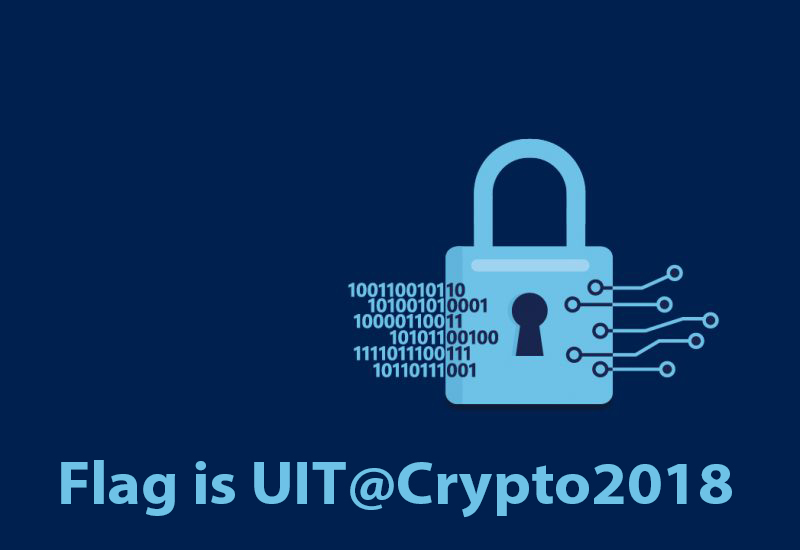
**Plaintext:**

Le flag de ce challenge est: 2ac376481ae546cd689d5b91275d324e

**Flag: 2ac376481ae546cd689d5b91275d324e**

**Task 1.10:**

**Flag: UIT@Crypto2018**

****

**Hướng giải quyết:**

Nhận thấy file ảnh bị lỗi nhưng có đuôi .jpg suy ra sẽ có signature là ff d8 ff, hexdump file thấy 3 bytes đầu là 8a b1 8b. Xor 2 đoạn với nhau sẽ ra 75, 69, 74, convert ra decimal là 117, 105, 116 và tra mã ASCII sẽ ra phần đầu key là uit.

Phần key còn lại đọc file ở dạng binary thấy “UITHCM” xuất hiện nhiều.

* Có key là “uithcm” và dùng script Python (source code kèm theo) để viết ra file ảnh đúng.

**Task mở rộng 1.1:**

**Ciphertext:**

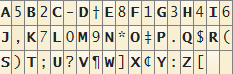
53‡‡†305))6\*;4826)4‡.)4‡);806\*;48†8¶60))85;;]8\*;:‡\*8†83(88)5\*†;46(;88\*96 \*?;8)\*‡(;485);5\*†2:\*‡(;4956\*2(5\*—4)8¶8\*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡ 1;48†85;4)485†528806\*81(‡9;48;(88;4 (‡?34;48)4‡;161;:188;‡?;

**Plaintext:**

A GOOD GLASS IN THE BISHOPS HOSTEL IN THE DEVILS SEAT TWENTY-ONE DEGREES AND THIRTEEN MINUTES NORTHEAST AND BY NORTH MAIN BRANCH SEVENTH LIMB EAST SIDE SHOOT FROM THE LEFT EYE OF THE DEATH'S-HEAD A BEE LINE FROM THE TREE THROUGH THE SHOT FIFTY FEET OUT

**Hướng giải quyết:**

Dựa vào bảng kí tự dưới đây để giải mã

****

**Task mở rộng 1.2:**

**Ciphertext:**

cv vvobobxy uocmgjg, olgiaqsliioa dynxyu fi axjwdy qgmqdgimpqz uvw jqygcgpemnqhu vqwpgpsgya wltupmw mtag utajqgimpemf khueqjbl hpp u axa qr lcel-dmmmw jcxwcehvuivl jcxfmw hnsizbajym bh atmhayvty gmlzcsya bu ymsa mocf uzx ocdx bh kgocxalt. fbmll fqnmktkzcampe mfohykfbul htq oaxk hal kkfrfiokhrtck dla syvxycfcwg hpp xqzpvmf abnpuho tuf hyzbmkoubbvp fi xkvvqwb whvm jzbccos, exi ddielpps iv mog uhbxypqn igk eahnbkgznqts eagunukoubbvpe mcvo ce wzxkkf wikk vduvlhefcwgz czx mfhkx

**Plaintext:**

in computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher. these deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email

**Hướng giải quyết:**

Thống kê sự lặp lại của các cụm từ để phỏng đoán chiều dài của khóa, ví dụ key trong bản mã lặp lại cách nhau 6 vị trí nên có thể đoán chiều dài của khóa là 6. Và từ đó có thể tách bản mã thành nhiều phần, phần thứ nhất gồm các chữ 1, 7, 13, 19, … phần thứ hai gồm các chữ 2, 8, 14, 20….. Mỗi phần coi như được mã hóa bằng phương pháp mã hóa đơn bảng. Từ đó áp dụng phương pháp phá mã dựa trên tần suất chữ cái cho từng phần một. Cuối cùng ráp lại sẽ tìm ra được bản rõ.

**Task mở rộng 1.4:**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Rail-fence cipher\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Quy tắc mã hoá:**

Cho key là một số lớn hơn 1, Rail fence sẽ tách plaintext thành các dòng với số dòng tương ứng với số key theo đường zig zag từ trên xuống và trái qua phải. Sau đó gộp các ký tự cùng dòng lại và gộp các hàng lại sau cùng.

Vd:

**Plaintext:**

“meet me at the toga party”

**Key:** 2

m e m a t e o a a t

e t e t h t g p r y

**Ciphertext:**

Memateoaatetethtgpry

Nguồn tham khảo:

<https://www.geeksforgeeks.org/>

<https://www.dcode.fr/>