

# BÁO CÁO THỰC HÀNH

Môn học: CRYPTOGRAPHY – Mật mã học

Tên chủ đề: Classical Cryptography

GVHD: Tô Trọng Nghĩa

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT219.N21.ANTT.1

STT	Họ và tên	MSSV	Email
1	Lê Đoàn Trà My	21521149	21521149@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Nội dung	Tình trạng	Trang
1	Kickoff: Crack the code	100%	2 - 4
2	Caesar cipher	100%	4 - 7
3	Mono-alphabetic substitution cipher and frequency analysis	100%	7-10
4	Playfair cipher	100%	10 - 16
5	Vigenère cipher	100%	17 - 19
6	Other ciphers	100%	19 - 22
Điểm tự đánh giá			9.5 - 10/10

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

---

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

## 1. Kickoff: Crack the code

### a, Tìm mật khẩu của khoá:

- Giả sử, mật khẩu có dạng: ABC.
- Các gợi ý: (1) {6, 8, 2}: 1 số đúng và đúng vị trí.  
(2) {6, 1, 4}: 1 số đúng nhưng sai vị trí.  
(3) {2, 0, 6}: 2 số đúng nhưng sai vị trí.  
(4) {7, 3, 8}: Không số nào đúng.  
(5) {7, 8, 0}: 1 số đúng nhưng sai vị trí.



Figure 4: Crack the code to open the lock

### - Giải mã:

- + Từ các gợi ý, ta có các số có thể là chữ số của mật khẩu là: 0, 1, 2, 3, 4, 5, 6, 7, 8.
- + Từ (4) loại các số: 7, 3, 8.
- + Kết hợp (4), (5) → 0 là 1 chữ số trong mật khẩu nhưng 0 không phải là C. (6)
- + Kết hợp (1), (2) → loại số 6.
- + Kết hợp (1), (4), (6) → C = 2. (7)
- + Kết hợp (3), (6), (7) → A = 0. (8)
- + Kết hợp (2), (7), (8) → B = 4.

### - Kết luận: Mật khẩu của khoá là: **042**.

### b, Tìm mã hoá tương ứng cho mỗi số từ 1 đến 9:

★	★	★	★	?
★	★	★	★	★
?	?	★	★	★
?	★	★	★	★
★	★	★	★	★

Table 1: Find the corresponding encoding for each number

### Giải mã:

- Mỗi ký hiệu mã hoá cho 1 số bất kỳ từ 1 đến 9.
- Có tổng của 4 số bất kỳ luôn  $\leq 36$  (vì tổng lớn nhất có thể có:  $9+9+9+9 = 36$ ).
- Các ô có 2 ký hiệu giống nhau như ★★, ★★ chỉ có thể là: 11 hoặc 22 hoặc 33.
- Xét cột 3, có:  $2\text{ (red star)} + 2\text{ (green star)} = \text{★★} \rightarrow \text{★★} = 22, \text{★} = 2$  (Tổng của 2 số chẵn là 1 số chẵn)

- 🟡🟡 chỉ có thể là 11 hoặc 33:

\* **Trường hợp 1:** 🟡🟡 = 11, 🟡 = 1.

+ Xét hàng 2, có: 3 🟢 + 🟢 = 11.

🟢	1	2	3	4
🟢	8	5	2	-1

Vì 🟡 = 2, 🟡 = 1 nên loại tất cả trường hợp.

\* **Trường hợp 2:** 🟡🟡 = 33, 🟡 = 3.

+ Xét hàng 2, có: 3 🟢 + 🟢 = 33 và xét cột 3: 2 🟡 + 2 🟢 = 22

🟢	1	2	...	7	8	9
🟢	30	27	...	12	9	6
🟡	-	-	...	-	2	5

Vì 🟡 = 2 nên loại trường hợp 🟢 = 8, 🟢 = 9

**Vậy: 🟡 = 3, 🟢 = 9, 🟢 = 6, 🟡 = 5**

+ Xét cột 4, có: 🟡 + 🟡 + 2 🟢 = 🟡🟡 ↔ 🟡 + 🟡 + 2\*9 = 23

🟡	1	2	3	4
🟡	4	3	2	1

Vì 🟡 = 2 nên loại trường hợp { 🟡, 🟡 } = {2, 3} và { 🟡, 🟡 } = {3, 2}

Vậy: { 🟡, 🟡 } có thể là {1, 4} hoặc {4, 1}; { 🟡, 🟡 } chỉ có thể là {7, 8} hoặc {8, 7}

+ Xét trường hợp { 🟡, 🟡 } = {7, 8}:

Cột 2, có: 🟡 + 2\* 🟡 + ?<sub>3,2</sub> = 🟡🟡 ↔ 7 + 2\*9 + ?<sub>3,2</sub> = 33 → ?<sub>3,2</sub> = 8 = 🟡

Hàng 4, có: ?<sub>4,1</sub> + 2\* 🟡 + 🟡 = 🟡🟡 ↔ ?<sub>4,1</sub> + 2\*9 + 6 = 28 → ?<sub>4,1</sub> = 4

Cột 1, có: 🟡 + 🟡 + ?<sub>3,1</sub> + ?<sub>4,1</sub> = 🟡🟡 ↔ 7 + 9 + ?<sub>3,1</sub> + 4 = 29 → ?<sub>3,1</sub> = 9 = 🟡

Hàng 3, có: ?<sub>3,1</sub> + ?<sub>3,2</sub> + 🟡 + 🟡 = 🟡🟡 ↔ 9 + 8 + 5 + 🟡 = 22 → 🟡 = 0

**Vậy loại trường hợp { 🟡, 🟡 } = {7, 8}**

+ Xét trường hợp { 🟡, 🟡 } = {8, 7}:

Cột 2, có: 🟡 + 2\* 🟡 + ?<sub>3,2</sub> = 🟡🟡 ↔ 8 + 2\*9 + ?<sub>3,2</sub> = 33 → ?<sub>3,2</sub> = 7 = 🟡

Hàng 4, có: ?<sub>4,1</sub> + 2\* 🟡 + 🟡 = 🟡🟡 ↔ ?<sub>4,1</sub> + 2\*9 + 6 = 27 → ?<sub>4,1</sub> = 3 = 🟡

Cột 1, có: 🟡 + 🟡 + ?<sub>3,1</sub> + ?<sub>4,1</sub> = 🟡🟡 ↔ 8 + 9 + ?<sub>3,1</sub> + 3 = 29 → ?<sub>3,1</sub> = 9 = 🟡

Hàng 3, có:  $?_{3,1} + ?_{3,2} + \text{★} + \text{★} = \text{★} \text{★} \leftrightarrow 9 + 7 + 5 + \text{★} = 22 \rightarrow \text{★} = 1; \text{★} = 4$

Hàng 1, có:  $2 * \text{★} + \text{★} + \text{★} = ?_{1,4} \leftrightarrow 2 * 8 + 5 + 4 = ?_{1,4} \rightarrow ?_{1,4} = 25 = \text{★} \text{★}$

Kết luận:  $\text{★} = 1, \text{★} = 2, \text{★} = 3, \text{★} = 4, \text{★} = 5, \text{★} = 6, \text{★} = 7, \text{★} = 8, \text{★} = 9.$

## 2. Caesar cipher

- **Mật mã Caesar** là một dạng mật mã thay thế, mỗi ký tự trên văn bản thô sẽ được thay bằng một ký tự khác, có vị trí cách nó một khoảng xác định trong bảng chữ cái.

### - Thuật toán Caesar:

+ Encryption (mã hoá):  $C = E(k, p) = (p + k) \bmod 26$

+ Decryption (giải mã):  $p = D(k, C) = (C - k) \bmod 26$

với: C: bản mã, p: bản rõ, k: khoá (khoảng dịch chuyển)

### - Các đoạn code trong Caesar:

+ Đoạn code Caesar Encryption:

```
void encrypt(string text, int key) //ma hoa voi key
{
    char alphabet[26] = { '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' };
    char alphabet1[26] = { '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' };
    string output = text;
    for (int j = 0; j < text.length(); j++)
    {
        for (int i = 0; i < 26; i++)
        {
            if (text[j] == alphabet[i])
            {
                output[j] = alphabet[(i + key) % 26];
                break;
            }
            else if (text[j] == alphabet1[i])
            {
                output[j] = alphabet1[(i + key) % 26];
                break;
            }
        }
    }
    cout << "\nCiphertext: " << output;
}
```

Hình. Đoạn code Caesar Encryption

+ Đoạn code Caesar Decryption có key và không key:

```
void decrypt(string text, int key) //giai ma voi key
{
    char alphabet[26] = { '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' };
    char alphabet1[26] = { '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' };
    string output = text;
    for (int j = 0; j < text.length(); j++)
    {
        for (int i = 0; i < 26; i++)
        {
            if (text[j] == alphabet[i])
            {
                output[j] = alphabet[(i - key + 26) % 26];
                break;
            }
            else if (text[j] == alphabet1[i])
            {
                output[j] = alphabet1[(i - key + 26) % 26];
                break;
            }
        }
    }
    cout << "\nPlaintext: " << output;
}
```

Hình. Đoạn code Caesar Decryption sử dụng key

```

void decrypt(string text) //giai ma brute-force
{
    char alphabet[26] = { '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' };
    char alphabet1[26] = { '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' };
    string output = text;
    for (int k = 0; k <= 25; k++)
    {
        for (int j = 0; j < text.length(); j++)
        {
            for (int i = 0; i < 26; i++)
            {
                if (text[j] == alphabet[i])
                {
                    output[j] = alphabet[abs(i - k + 26) % 26];
                    break;
                }
                else if (text[j] == alphabet1[i])
                {
                    output[j] = alphabet1[abs(i - k + 26) % 26];
                    break;
                }
            }
        }
        cout << "\nPlaintext with key = " << k << " : " << output<<endl;
    }
}

```

Hình. Đoạn code Caesar Decryption không sử dụng key (brute-force)

### - Tiến hành kiểm tra giải mã đoạn mã:

*Gurer ner gjb xvaqf bs crbcyr va guvf jbeyq: gubfr jub ner ybbxvat sbe n ernfba naq gubfr jub ner svaqvat fhpprrff. Gubfr jub ner ybbxvat sbe n ernfba nyjnlf frrxvat gur ernfbaf jul gur jbex vf abg svavfurq. Naq crbcyr jub svaq fhpprrff ner nyjnlf ybbxvat sbe ernfbaf jul gur jbex pna or pbzcyrgq.*

+ Trong đoạn văn trên, có ký tự 'n' đứng riêng lẻ, trong tiếng Anh các ký tự đơn đứng riêng lẻ có nghĩa thường là I, a tuy nhiên I ít khi đứng giữa câu và không đứng cuối câu → 'n' trong bản mã sẽ là 'a' trong bản rõ → key = 13.

+ Thu được các kết quả khi chạy chương trình giải mã đoạn bản mã trên:

```

Microsoft Visual Studio Debug Console
Input text: Gurer ner gjb xvaqf bs crbcyr va guvf jbeyq: gubfr jub ner ybbxvat sbe n ernfba naq gubfr jub ner svaqvat fhpprrff. Gubfr jub ner ybbxvat sbe n ernfba nyjnlf frrxvat gur ernfbaf jul gur jbex vf abg svavfurq. Naq crbcyr jub svaq fhpprrff ner nyjnlf ybbxvat sbe ernfbaf jul gur jbex pna or pbzcyrgq

Select (1) encrypt / (2) decrypt
2

Select (1) decrypt with key / (2) decrypt brute-force
1

Input key: 13

Plaintext: There are two kinds of people in this world: those who are looking for a reason and those who are finding success. Those who are looking for a reason always seeking the reasons why the work is not finished. And people who find success are always looking for reasons why the work can be completed
C:\Users\ADMIN\source\repos\21521149_MMH\X64\Debug\Lab01.exe (process 58868) exited with code 0.
Press any key to close this window . . .

```

Hình. Kết quả giải mã đoạn bản mã bằng chương trình vừa viết với key = 13



```

Microsoft Visual Studio Debug Console

Input text: Gurer ner gjb xvaqf bs crbcyr va guvf jbeyq: gubfr jub ner ybbxvat sbe n ernfba naq gubfr jub ner svaqvaf fhpprrff. Gubfr jub ner ybbxvat sbe n ernfba nyjnlf frxrvat gur ernfbaf jul gur jbox
vf abg svavfurq. Naq crbcyr jub svaq fhpprrff ner nyjnlf ybbxvat sbe ernfbaf jul gur jbox pna or pbzcyrgrq

Select (1) encrypt / (2) decrypt
2

Select (1) decrypt with key / (2) decrypt brute-force
2

Plaintext with key = 0 : Gurer ner gjb xvaqf bs crbcyr va guvf jbeyq: gubfr jub ner ybbxvat sbe n ernfba naq gubfr jub ner svaqvaf fhpprrff. Gubfr jub ner ybbxvat sbe n ernfba nyjnlf frxrvat gur ernfbaf
jul gur jbox vf abg svavfurq. Naq crbcyr jub svaq fhpprrff ner nyjnlf ybbxvat sbe ernfbaf jul gur jbox pna or pbzcyrgrq

Plaintext with key = 1 : Ftgds mdq fia wuzpe an bqebxq uz ftue iadxp: ftaeq ita mdq xaawuz rad m dqmeaz mpmke eqquwz ftq dqmeaz
itk ftq iadw uz af ruzetap. Mzp bqabxq ita ruzp egooqee mdq mximke xaawuz rad dqmeaz itk ftq iadw onz nq oaybxqfqp

Plaintext with key = 2 : Espcp lcp ehv vttyd zq apzawp ty estd hzwo: eszdp hsz lcp wzzvtvr qzc 1 cpldzy lyo eszdp hsz lcp qtyotyr dfnnpdd. Eszdp hsz lcp wzzvtvr qzc 1 cpldzy lwhlj dppvtvr esp cpldzyd
hsj esp hzcv td yze qtytdspo. Lyo apzawp hsz qtyo dfnnpdd lcp lwhlj wzzvtvr qzc cpldzyd hsj esp hzcv nly mp nzxawpepo

Plaintext with key = 3 : Drobo kbo dgy usxnc yp zoyzvo sx drsc gybvn: dryco gry kbo vyvuxsq pyb k bokcyx kxn dryco gry kbo psxnsqx cemmoc. Dryco gry kbo vyvuxsq pyb k bokcyx kvkic coosuxq dro bokcyx
gri dro gybu sc xyd psxsron. Kxn zoyzvo gry psxn cemmoc kbo kvkic vyvuxsq pyb bokcyx gri dro gybu mxx lo mnyvodon

Plaintext with key = 4 : Cqan jan cfx trmbx xo ynyxun rw cqb fxaum: cqxbn fax jan uxxtwpx oxa j anjbox jwm cqxbn fax jan ormwpx bdllnbb. Cqxbn fax jan uxxtwpx oxa j anjbox jufjhb bnntwpx cqn anjbox
fqh cqn fxat rb xcc onwrbqnm. Jwm ynyxun fax onw bdllnbb jan jufjhb uxxtwpx oxa anjbox fqh cqn fxat ljj kn lxyvuncnm

Plaintext with key = 5 : Bpmz izm bew sqvla wn mxwmt bp bqpa ewtll: bpmw epw izm twisqvo nzw i zmiaw ivl bpmw epw izm nqlvqo ackmaa. Bpmw epw izm twisqvo nzw i zmiaw iteiga amsqvo bpm zmiawva
epg bpm ewz qa vwb nqvapml. Ivl mxwmt epw nqlv ackmaa izm iteiga twisqvo nzw zmiawva epg bpm ewz kiv jm kwxtwml

Plaintext with key = 6 : Aolyl hyl adv rpuks vm wlvswl pu aopz dyusk: aovl dov hyl svvrpnm myh h ylhvzu huk aovl dov hyl mpukun zbjjlzz. Aovl dov hyl svvrpnm myh h ylhvzu hsdhfz zllrpn aol ylhvzu
dof aol dvyr pz uva mpuzolk. Huk wlvswl dov mpuk zbjjlzz hyl hsdhfz svvrpnm myh ylhvzu dof aol dvyr jhu il jvtwslak

Plaintext with key = 7 : Znkxk gxx zcu qotjy ul vkuvrk ot znoy cuxrj: znuyk cnu gxx ruuqotm lux g xkgvut gtj znuyk cnu gxx lotjotm yaiky. Znuyk cnu gxx ruuqotm lux g xkgvut grcey ykkqotm znk xkgvut
cne znk cuxq oz tuz lotojnkj. Gtj vkuvrk cnu lotj yaiky gxx grcey ruuqotm lux xkgvut cne znk cuxq igt hk iusvzkzj

Plaintext with key = 8 : Ymjwj fwj ybt pnsix kt ujtujz ns ymwx btwqi: ymtxj bmt fwj qttpsnl ktw f wjfxts fsi ymtxj bmt fwj ksnisl xzhjxx. Ymtxj bmt fwj qttpsnl ktw f wjfxts fqbdx xjjpsnl ymj wjfxts
bmd ymj btwp nx sty knsnxmi. Fsi ujtujz bmt knsi xzhjxx fwj fqbdx qttpsnl ktw wjfxts bmd ymj btwp hxx gj htruzjji

Plaintext with key = 9 : Xliyi evi xas omrhv sj tiistpi m xlmw asvph: xlswi als evi psomrk jsv e vjewr erh xlswi als evi jmrhmrk wyggiw. Xlswi als evi psomrk jsv e vjewr epaew wilmrk xli vjewr
alc xli asvo mw rsx jmmwlih. Erh tiistpi als jmrh wyggiw evi epaew psomrk jsv vjewr alc xli asvo gar fi gsgtpixh

Plaintext with key = 10 : Wkwh duh wr nlgvy ri shrosh lq wklv zrugo: wkvrh zkr duh orrnlaq iru d uhvrvq dag wkvrh zkr duh ilaglaq vxffhvv. Wkvrh zkr duh orrnlaq iru d uhvrvq dozbv vhnlaq wkh uhvrvq
v zkb wkh zrwn lv qrw lqlvkhg. Dag shrosh lq wklv vxffhvv duh dozbv orrnlaq iru uhvrvq zkb wkh zrwn fdq eh frpsohwg

Plaintext with key = 11 : Vjgtz ctg vjq mkofu qh rgarng kp vjku yqtnf: vjqwg yjq ctg nqgmki hat c tgcup cof vjqwg yjq ctg hkpkipi uweegu. Vjqwg yjq ctg nqgmki hat c tgcup cnyau ugmkpi vjq tgcup
u yja vjq yqtm kp pav hkpjudgf. Cpf rgarng yjq hkpif uweegu ctg cnyau nqgmki hat tgcup uja vjq yqtm ecp dg eqornvgf

Plaintext with key = 12 : Uuifz bsf uxp ljoet pg qfpmf jo uijt xpsme: uipft xip bsf mpmloj gps b sfbtp boe uipft xip bsf gjoehq tvddftt. Uipft xip bsf mpmloj gps b sfbtp bmbxt tflljoj uif sfbtp
t xiz uif xpsl jt opu gjoetfife. Boe qfpmf xip gjo tvddftt bsf bmbxt mpmloj gps sfbtp xiz uif xpsl dbo cf dpgmfufe

Plaintext with key = 13 : There are two kinds of people in this world: those who are looking for a reason and those who are finding success. Those who are looking for a reason always seeking the reason
s why the work is not finished. And people who find success are always looking for reasons why the work can be completed

Plaintext with key = 14 : Sgddq zqd svn jhmcr ne odnokd hm sghr vnqk: sgndr vgn zqd knnjhmf enq z qdzrnm zmc sgndr vgn zqd ehnmchf rtbbdrr. Sgndr vgn zqd knnjhmf enq z qdzrnm zkzxr rddjhmf sgd qdzrnm
r vgx sgd vnqj hr mms ehnmhgc. Zmc odnokd vgn ehmc rtbbdrr zqd zkzxr knnjhmf enq qdzrnm vgx sgd vnqj bzm ad bnloksdc

Plaintext with key = 14 : Sgddq zqd svn jhmcr ne odnokd hm sghr vnqk: sgndr vgn zqd knnjhmf enq z qdzrnm zmc sgndr vgn zqd ehnmchf rtbbdrr. Sgndr vgn zqd knnjhmf enq z qdzrnm zkzxr rddjhmf sgd qdzrnm
r vgx sgd vnqj hr mms ehnmhgc. Zmc odnokd vgn ehmc rtbbdrr zqd zkzxr knnjhmf enq qdzrnm vgx sgd vnqj bzm ad bnloksdc

Plaintext with key = 15 : Rfcpc ypc rum iglba md ncmjic gl rfaq umpjb: rfmcq ufm ypc jmmigle dmp y pcyqnl ylb rfmcq ufm ypc dglbgle qsaacq. Rfmq ufm ypc jmmigle dmp y pcyqnl yjuyw qccigle rfc pcyqnl
q ufw rfc umpi gl lmr dglbqfcb. Ylb ncmjic ufm dglb qsaacq ypc yjuyw jmmigle dmp pcyqnl ufw rfc umpi ayl z amknjrcrb

Plaintext with key = 16 : Qebob xob qtl hfkap lc mblimb fk qefp tloia: qelpb tel xob illhfdk clo x obxplk xka qelpb tel xob cfkafkd przzbpb. Qelpb tel xob illhfdk clo x obxplk xitxw pbbhfdk qeb obxplk
p tev qeb tloh fp kfl cfkfeba. Xka mblimb tel cfka przzbpb xob xitxw illhfdk clo obxplk tev qeb tloh zkk yb zljmbqba

Plaintext with key = 17 : Pdana wna psk gejoz kb lakla ej pdeo slrhv: pdkoa sdk wna hkggejc bkn w nawokj wjz pdkoa sdk wna bejzejc oqyao. Pdkoa sdk wna hkggejc bkn w nawokj whswu oaagejc pda nawokj
o sdu pda skng eo jkp bejeadaz. Wjz lakla sdk bejz oqyao wna whswu hkggejc bkn nawokj sdu pda skng ywaj xa ykilhapaz

Plaintext with key = 18 : Ocznz vmz orj fdiyn ja kzjkgz di ocnd rjmgv: ocjnz rcj vmz gjjfdib ajm v mznvji viy ocjnz rcj vmz adiydib npxznn. Ocjnz rcj vmz gjjfdib ajm v mznvji vgrvtn nzzfdib ocr mznvji
n rct ocr rjmf dn ijo adidnczy. Viy kzjkgz rcj adiy npxznn vmz vgrvtn gjjfdib ajm mznvjin rct ocr rjmf xvi wz xjhkgzozy

Plaintext with key = 19 : Nbyly ulv nqi echxm iz jyjify ch nbcm qilfx: nbmy qbi ulv fiiecha zil u lyumih uhx nbmy qbi ulv zchxcha mowymm. Nbmy qbi ulv fiiecha zil u lyumih ufqum myyecha nby lyumih
m qbs nby qile cm hin zchcnbx. Uhx jyjify qbi zchx mowymm ulv ufqum fiiecha zil lyumih qbs nby qile wuh vy wigjfyx

Plaintext with key = 20 : Maxlx tkx mph dgbul hy ixhiex bg mabl phkw: mahlx pah tkx ehhdgzy yhk t kxtlgh tgw mahlx pah tkx ybgdgyz lnvxl. Mahlx pah tkx ehhdgzy yhk t kxtlgh teptrl lxxdgyz max kxtlgh
l par max phkd bl ghm ybgw lnvxl tkx teptrl ehhdgzy yhk kxtlgh par max phkd vtg ux vhfexmxw

Plaintext with key = 21 : Lzjwg sjw log cufvk gx hughdw af lzak ogjdv: lzgkw ozg sjw dggcayf xgj s jwskgf svf lzgkw ozg sjw xafvafy kmuukk. Lzgkw ozg sjw dggcayf xgj s jwskgf sdosqk kwcafyz lzw jwskgf
k ozg lzw ogjc ak fgl xafakzvw. Sfv hughdw ozg xafv kmuukk sjw sdosqk dggcayf xgj jwskgf ozg lzw ogjc usf tw ueghdlwv

Plaintext with key = 22 : Kyfjv riv knf bzeuf fw gvfvcv ze kyvjz nfcu: kyfjv nyf riv cffbzex wfi r ivrjfe reu kyfjv nyf riv wzeuzex jlttvjj. Kyfjv nyf riv cffbzex wfi r ivrjfe rcnnpj jvzbzex kyv ivrjfe
j nyp kyv nfbz zj efk wzezyjv. Reu gvfvcv nyf wzeu jlttvjj riv rcnnpj cffbzex wfi ivrjfe nyp kyv nfbz tre sv trdgcvkvu

Plaintext with key = 23 : Jxuhu qhu jme aydti ev fuefbu yd jxyi meht: jxeiu mxe qhu beaaydw veh q huqied qdt jxeiu mxe qhu vydytdw ikssui. Jxeiu mxe qhu beaaydw veh q huqied qbmqoi iuuaydw jxu huqied
i mxo jxu meha yi dej vydyixut. Qdt fuefbu mxe ydt ikssui qhu qbmqoi beaaydw veh huqied mxo jxu meha sqd ru secfbujut

Plaintext with key = 24 : Iwtgt pgt ild zxcsh du etdeat xc ixwh ldgas: iwdht lwd pgt addzxcv udg p gthpdc pcs iwdht lwd pgt uxcsxv hjrrthh. Iwdht lwd pgt addzxcv udg p gthpdc palpnh httxxcv iwt gthpdc
h lwn iwt ldgz xh cdi uxchxwts. Pcs etdeat lwd uxcs hjrrthh pgt palpnh addzxcv udg gthpdc lwn iwt ldgz rqc rpt rdbeatits

Plaintext with key = 25 : Hvsfs ofs hkc ywbrg ct dscdzb wb hwvg kcfzr: hvcsz kvc ofs zccyubu tcf o fsogcb obr hvcsz kvc ofs twrbwbu giqqsqg. Hvcsz kvc ofs zccyubu tcf o fsogcb ozkomg gssyubu hvs fsogcb
g kmv hvs kcfy wg bch twbwgvsr. Obr dscdzb kvc twbr giqqsqg ofs ozkomg zccyubu tcf fsogcb kmv hvs kcfy qob ps qcadzshz

C:\Users\ADMIN\source\repos\21521149_MWH\Lab01\Debug\Lab01.exe (process 58876) exited with code 0.
Press any key to close this window . . .

```

Hình. Kết quả giải mã đoạn bản mã bằng chương trình vừa viết bằng brute-force

+ Kiểm tra, so sánh lại với bản rõ được giải mã bằng dcode:

**Results**

Brute-Force mode: the 25 shifts (for the alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ) are tested and sorted from most probable to least probable.

↑↓	↑↓
→13 (←13)	There are two kinds of people in this world: those who are looking for a reason and those who are finding success. Those who are looking for a reason always seeking the reasons why the work is not finished. And people who find success are always looking for reasons why the work can be completed.

**CAESAR CIPHER DECODER**

★ CAESAR SHIFTED CIPHERTEXT (?)

Gurer ner gjb xvagf bs crbcyr va guvf jbeyq: gubfr jub ner ybbxvat sbe n ernfba naq gubfr jub ner svagvat fhpprrff. Gubfr jub ner ybbxvat sbe n ernfba nyjnlf frxxvat gur ernfba jul gur jbex vf abg svavfurq. Naq crbcyr jub svag fhpprrff ner nyjnlf ybbxvat sbe ernfba jul gur jbex pna or pbzcyrgqr.

Test all possible shifts (26-letter alphabet A-Z)

► DECRYPT (BRUTEFORCE)

**MANUAL DECRYPTION AND PARAMETERS**

★ SHIFT/KEY (NUMBER): 13

☒ USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)

☐ USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9

☐ USE THE LATIN ALPHABET IN THE TIME OF CAESAR (23 LETTERS, NO J, U OR W)

Hình. Kết quả giải mã đoạn bản mã bằng <https://www.dcode.fr/caesar-cipher>

### 3. Mono-alphabetic substitution cipher and frequency analysis

- Sử dụng <https://www.cryptool.org/en/cto/n-gram-analysis> để tiến hành phân tích đoạn bản mã, dựa vào kết quả phân tích có:

- + Trong các ký tự, 'n' xuất hiện nhiều nhất với tần suất 12,16% → 'n' khả năng cao là 'e'.
- + Trong các từ có 3 ký tự, 'ytn' xuất hiện nhiều nhất và thường ở đầu đoạn văn bản → 'ytn' khả năng cao là 'the' → y = t, t = h, n = e.
- + 'v' đứng một mình và xuất hiện tại đầu và giữa câu → khả năng cao v = a
- + 'y[x]' ↔ 't[x]' → khả năng cao là 'to' → x = o
- + 'v[q] a' ↔ 'a[q] a' → q = s (q ≠ n vì không thể là an a)
- + 'x[u]n', 'x[u]', '[u]x' ↔ 'o[u]e', 'o[u]', '[u]o' → u = n
- + '[m]u' ↔ '[m]n' và đứng trước mạo từ the → có thể là giới từ in → m = i
- + 'x[b]' ↔ 'o[b]' và đứng trước mạo từ the → có thể là giới từ of → b = f
- + '[l]myt' ↔ '[l]ith' và đứng trước mạo từ the → có thể là giới từ with → l = w
- + 'yx [g]n' ↔ 'to [g]e' → có thể là to be, g = b
- + 'vu[p]' ↔ 'an[p]' với tần suất xuất hiện đứng thứ 2 trong các chữ có 3 ký tự → có thể là and → p = d
- + 'dnv[h]', 'ln[h]n' ↔ 'pea[h]', 'we[h]e' → có thể là pear, were → h = r
- + 'xu[a]n' ↔ 'on[a]e' → có thể là once → a = c
- + 'v[ii]', 'av[ii]', 'av[ii]np' ↔ 'a[ii]', 'ca[ii]', 'ca[ii]ed' → ii = ll, i = l
- + 'hmvii[d]' ↔ 'reall[d]' → có thể là really → d = y

- + 'ym[c]n', 'lx[c]nu' ↔ 'ti[c]e', 'wo[c]en' → c = m
- + 'gv[rr]nh', 'ixu[r]', 'hm[r]ty', 'gm[r]' ↔ 'ba[rr]er', 'lon[r]', 'ri[r]ht', 'bi[r]' → r = g
- + '[e]vd', '[e]xlnh', 'td[e]n', 'tni[e]' ↔ '[e]ay', '[e]ower', 'hy[e]e', 'hel[e]' → e = p
- + '[z]e', 'x[z]y' ↔ '[z]p', 'o[z]t' → z = u
- + 'bn[f]nh', 'cx[f]np', 'v[f]xmp', 'un[f]nh' ↔ 'fe[f]er', 'mo[f]ed', 'a[f]oid', 'ne[f]er' → f = v
- + '[o]zqy', '[o]zpp', '[o]zgmivuy' ↔ '[o]ust', '[o]udd', '[o]ubilant' → o = j
- + 'n[k]yvh', 'qn[k]mqy', 'n[k]enhyq' ↔ 'e[k]tra', 'se[k]ist', 'e[k]perts' → k = x
- + 'cv[s]n', 'im[s]n', 'giva[s]' ↔ 'ma[s]e', 'li[s]e', 'blac[s]' → s = k
- + '[j]zmy' ↔ '[j]uit', vì chỉ còn z và q → j = q
- + 'ehm[w]n' ↔ 'pri[w]e' → w = z

Key mã hoá:

	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
key	v	g	a	p	n	b	r	t	m	o	s	i	c	u	x	e	j	h	q	y	z	f	l	k	d	w

Key giải mã:

	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
key	c	f	m	y	p	v	b	r	l	q	x	w	i	e	j	d	s	g	k	h	n	a	z	o	t	u

- Kiểm tra lại kết quả (dùng <https://www.dcode.fr/monoalphabetic-substitution>):

**Results**

dCode tried to find the correct alphabet and its substitution automatically.  
The result is a draft that should allow you to perform the decryption manually by indicating letters in each cell.

THE OSCARS TURN ON SUNDAY WHICH SEEMS ABOUT RIGHT AFTER THIS LONG STRANGE AWARDS TRIP THE BAGGER FEELS LIKE A NONAGENARIAN TOO THE AWARDS RACE WAS BOOKENDED BY THE DEMISE OF HARVEY WEINSTEIN AT ITS OUTSET AND THE APPARENT IMPLOSION OF HIS FILM COMPANY AT THE END AND IT WAS SHAPED BY THE EMERGENCE OF METOO TIMES UP BLACKGOWN POLITICS ARMCANDY ACTIVISM AND A NATIONAL CONVERSATION AS BRIEF AND MAD AS A FEVER DREAM ABOUT WHETHER THERE OUGHT TO BE A PRESIDENT WINFREY THE SEASON DIDNT JUST SEEM EXTRA LONG IT WAS EXTRA LONG BECAUSE THE OSCARS WERE MOVED TO THE FIRST WEEKEND IN MARCH TO AVOID CONFLICTING WITH THE CLOSING CEREMONY OF THE WINTER OLYMPICS THANKS PYEONGCHANG ONE BIG QUESTION SURROUNDING THIS YEARS ACADEMY AWARDS IS HOW OR IF THE CEREMONY WILL ADDRESS METOO ESPECIALLY AFTER THE GOLDEN GLOBES WHICH BECAME A JUBILANT COMINGOUT PARTY FOR TIMES UP THE MOVEMENT SPEARHEADED BY POWERFUL

**MONOALPHABETIC SUBSTITUTION DECODER**

★ ALPHABETIC SUBSTITUTION CIPHERTEXT

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

⇒ VGAPNBRTMOSICUXEJHQYZFLKDW (Original Encryption Alphabet)  
⇒ CFMYPVBRLLQXWIEJDSGKHNAZOTU (Reciprocal Decryption Alphabet)

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

Hình. Kết quả giải mã đoạn text bằng dcode

- Bản rõ hoàn chỉnh được gửi cùng báo cáo Lab 01 với tên **task3\_Decrypt.txt**.



\* **Bài nâng cao:** Giải mã đoạn bản mã trong cuốn sách của Edgar Allan Poe – Con bọ hung vàng

53#++305))6\*;4826)4#.)4#);806\*;48+8¶60))85;1#(:#\*8+83(88)  
 5\*+;46(;88\*96\*?;8)\*#(:485);5\*+2:\*#(:4956\*2(5\*-4)8¶8\*;40692  
 85);)6+8)4##;1(#+9;48081;8:8#1;48+85;4)485+528806\*81(#+9;48  
 ;(88;4(#+34;48)4#;161;:188;#?;

- Sử dụng <https://www.cryptool.org/en/cto/n-gram-analysis> để tiến hành phân tích đoạn bản mã, dựa vào kết quả phân tích có:

- + 3 ký tự có tần suất cao nhất: '8', ';', '4' → khả năng cao là 'e'.
- + 'ee' là cụm chữ thường gặp trong tiếng anh, xét tần suất xuất hiện các cặp 2 ký tự '88', ';;', '44' có tần suất của '88' là cao nhất → '8' = e
- + 'the' là một từ 3 chữ thường xuất hiện nhiều nhất trong tiếng anh, xét bảng tần suất thấy '[;4]8' ↔ '[;4]e' xuất hiện 7 lần → ';' = t, '4' = h
- + Dựa vào tần số, thấy ')', '¶', '\*', '5', '6' có khả năng là thay thế của 'a', 'o', 'i', 'n', 's', 'r'
- + Các từ 2 ký tự thường gặp trong tiếng anh còn có 'an', 'in', và chúng đều kết thúc bằng 'n' và 'oo', 'ss' thường hay gặp
- xét các tần suất của các chữ 2 ký tự được tạo bởi ')', '¶', '\*', '5', '6' thấy '6\*' (5 lần), '5\*' (3 lần), '5)' (3 lần), '¶¶' (2 lần), '))' (2 lần)
- khả năng cao '\*' = n, '5' = a, '6' = i
- + Giả sử '5' ↔ 'a' đầu tiên là một mạo từ → 'a 3¶ ¶' → '¶' = o, ')' = s
- + 'an[¶]' → khả năng cao là 'an[d]' → ¶ = d
- + 'thi[()]teen', 'no[()]theast' ↔ 'thi[r]teen', 'no[r]theast' → '(' = r
- + '[3]ood', 'de[3]ree' ↔ '[g]ood', 'de[g]ree' → '3' = g
- + 'thro[?]gh' ↔ 'thro[u]gh' → '?' = u
- + '[9]inutes' ↔ '[m]inutes' → '9' = m
- + 'g[0]ass' ↔ 'g[l]ass' → '0' = l
- + 'de[¶]ils' ↔ 'de[v]ils' → '¶' = v
- + '[1]rom', 'le[1]t' ↔ '[f]rom', 'le[f]t' → '1' = f
- + 'fort[:]', 'e[:]e', 'fift[:]' ↔ 'fort[y]', 'e[y]e', 'fift[y]' → ':' = y
- + '[2]y' ↔ '[b]y' → '2' = b

+ 'bran[-]h'  $\leftrightarrow$  'bran[c]h'  $\rightarrow$  '-' = c

+ 'bisho[.]'  $\leftrightarrow$  'bisho[p]'  $\rightarrow$  '.' = p

	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
key	5	2	-	†	8	1	3	4	6			0	9	*	‡		.	(	)	;	?	¶			:	

- Bản rõ:

***A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb eastside shoot from the left eye of the death's head a beeline from the tree through the shot fifty feet out***

*(A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb eastside shoot from the left eye of the death's head a beeline from the tree through the shot fifty feet out)*

#### 4. Playfair cipher

- **Mật mã Playfair** là một hệ mã hóa nhiều chữ.

- **Cơ chế hoạt động:** sử dụng một ma trận chữ cái 5x5 trên cơ sở một từ khóa, điền các chữ cái của từ khóa (bỏ các chữ trùng), điền những vị trí còn lại của ma trận với các chữ cái khác của bảng chữ cái; I, J có thể ở trên cùng một ô của ma trận (hoặc thường bỏ đi J, nếu trong bản rõ chứa J thì nó được thay bằng I).

- **Thuật toán mã hoá:**

+ Bản rõ được chia thành các cặp gồm 2 chữ cái, nếu số chữ cái lẻ thì thêm một chữ cái không có thật vào cuối. *(Em sử dụng một chữ cái không có thật là chữ 'X')*

+ Không được có cặp chữ giống nhau, nếu có thì chia ra và ghép với một chữ cái không có thật vào chữ cái trước. *(Em sử dụng một chữ cái không có thật là chữ 'X')*

+ Cả 2 chữ cái trong cặp nằm trong cùng một cột: lấy chữ cái bên dưới mỗi chữ (quay trở lại đầu nếu ở dưới cùng).

+ Cả 2 chữ cái trong cặp nằm trong cùng một hàng: lấy chữ cái bên phải mỗi chữ (quay trở lại ngoài cùng bên trái nếu ở vị trí ngoài cùng bên phải).

+ 2 chữ cái không cùng hàng/cột: Tạo một hình chữ nhật với hai chữ cái và lấy các chữ cái ở góc đối diện nằm ngang của hình chữ nhật.

**- Các đoạn code trong Playfair:**

+ Đoạn code xử lý đoạn text đưa vào: chuyển tất cả các ký tự về chữ in hoa, xoá các ký tự không là chữ cái (các ký tự đặc biệt, khoảng trắng,...).

```
char keyMatrix[5][5]; //tạo ma trận khoá

void changeText(string& text)
{
    for (int i = 0; i < text.length(); i++)
    {
        text[i] = toupper(text[i]); //chuyển tất cả kí tự trong text về chữ in hoa
    }
    int i, count = 0;
    for (i = 0; i < text.length(); i++)
    {
        if ((text[i] >= 'A') && (text[i] <= 'Z'))
        {
            text[count++] = text[i];
            count;
        }
        else //xoá các ký tự không là chữ
        {
            text.erase(text.begin() + i);
            i--;
        }
    }
}
```

Hình. Đoạn code xử lý chuyển các ký tự sang chữ in hoa, xoá các ký tự không là chữ

+ Đoạn code tạo ma trận khoá 5x5 dựa trên key và bảng chữ cái (tiếng anh):

```
void createKeyMatrix(string key, char keyMatrix[5][5])
{
    int flag[26] = {}; //tạo mảng để đánh dấu sự xuất hiện của ký tự, mặc định = 0
    int row = 0, col = 0;
    for (int i = 0; i < key.length(); i++) //thêm các chữ trong key vào ma trận trước
    {
        if (key[i] == 'J') //vì lược bỏ J, I/J ở cùng 1 ô nên các vị trí có j sẽ được thay bằng i
            key[i] = 'I';
        if (flag[key[i] - 'A'] == 0) //thêm kí tự chưa có vào ma trận và bật cờ của chữ cái đó
        {
            flag[key[i] - 'A'] = 1;
            keyMatrix[row][col++] = key[i];
        }
        if (col == 5) //hết hàng xuống hàng mới
        {
            row++;
            col = 0;
        }
    }
    for (char c = 'A'; c <= 'Z'; c++) //thêm các chữ cái trong bảng chữ cái vào ma trận
    {
        if (c == 'J') //vì lược bỏ J
            continue;
        if (flag[c - 'A'] == 0) //thêm kí tự chưa có vào ma trận và bật cờ của chữ cái đó
        {
            flag[c - 'A'] = 1;
            keyMatrix[row][col++] = c;
        }
        if (col == 5) //hết hàng xuống hàng mới
        {
            row++;
            col = 0;
        }
    }
}
```

Hình. Đoạn code tạo ma trận khoá 5x5

+ Đoạn code khai báo cấu trúc của chữ cái và hàm trả về vị trí (hàng, cột) của chữ cái:

```
typedef struct //khai bao cau truc vi tri (hang, cot) cua chu cai
{
    int row;
    int column;
} pos;

pos getPosition(char c)
{
    for (int i = 0; i < 5; i++)
    {
        for (int j = 0; j < 5; j++)
        {
            if (c == keyMatrix[i][j])
            {
                pos position = { i, j };
                return position;
            }
        }
    }
}
```

Hình. Đoạn code khai báo cấu trúc và hàm trả về vị trí của chữ cái

+ Đoạn code xử lý chuỗi đưa vào theo thuật toán Playfair:

```
void handleText(string& text)
{
    for (int i = 0; i < text.length(); i++) // thay J bằng I
    {
        if (text[i] == 'J')
            text[i] = 'I';
    }
    for (int j = 1; j < text.length(); j = j + 2) // biến đổi text theo 2 ý đầu của thuật toán mã hoá
    {
        if (text[j] == text[j - 1])
            text.insert(text.begin() + j, 'X');
    }
    if (text.length() % 2 == 1) //nếu chuỗi lẻ, thêm ký tự X
        text = text + 'X';
}
```

Hình. Đoạn code xử lý đoạn text theo thuật toán Playfair

+ Đoạn code Playfair Encryption:

```

void encrypt(string text)
{
    string output = "";
    for (int i = 0; i < text.length(); i += 2)
    {
        //lấy vị trí của 2 ký tự kế nhau
        pos p1 = getPosition(text[i]);
        pos p2 = getPosition(text[i + 1]);
        int x1 = p1.row; int y1 = p1.column;
        int x2 = p2.row; int y2 = p2.column;

        if (x1 == x2) // cùng hàng dịch phải 1, mod 5 nếu quá vòng
        {
            output = output + keyMatrix[x1][(y1 + 1) % 5];
            output = output + keyMatrix[x2][(y2 + 1) % 5];
        }
        else if (y1 == y2) // cùng cột dịch xuống 1, mod 5 nếu quá vòng
        {
            output = output + keyMatrix[(x1 + 1) % 5][y1];
            output = output + keyMatrix[(x2 + 1) % 5][y2];
        }
        else //khác, đổi cột
        {
            output = output + keyMatrix[x1][y2];
            output = output + keyMatrix[x2][y1];
        }
    }
    cout << "\nCiphertext: " << output;
}

```

Hình. Đoạn code Playfair Encryption

+ Đoạn code Playfair Decryption:

```

void decrypt(string text)
{
    string output = "";
    for (int i = 0; i < text.length(); i += 2)
    {
        //lấy vị trí của 2 ký tự kế nhau
        pos p1 = getPosition(text[i]);
        pos p2 = getPosition(text[i + 1]);
        int x1 = p1.row; int y1 = p1.column;
        int x2 = p2.row; int y2 = p2.column;

        if (x1 == x2) // cùng hàng dịch phải 1, mod 5 nếu quá vòng
        {
            output = output + keyMatrix[x1][abs(y1 - 1 + 5) % 5];
            output = output + keyMatrix[x2][abs(y2 - 1 + 5) % 5];
        }
        else if (y1 == y2) // cùng cột dịch xuống 1, mod 5 nếu quá vòng
        {
            output = output + keyMatrix[abs(x1 - 1 + 5) % 5][y1];
            output = output + keyMatrix[abs(x2 - 1 + 5) % 5][y2];
        }
        else //khác, đổi cột
        {
            output = output + keyMatrix[x1][y2];
            output = output + keyMatrix[x2][y1];
        }
    }
    cout << "\nPlaintext: " << output;
}

```

Hình. Đoạn code Playfair Encryption



**a, Kiểm tra lại chương trình vừa viết:**

- Text: *The karst seascape of Ha Long Bay is one of the world's most spellbinding sea views and is a UNESCO World Heritage Site. With the bay's scenery best seen by boat, this is prime cruising territory. You should opt for at least an overnight tour to see Ha Long Bay's iconic views as a day trip doesn't do it justice. There are plenty of caves in the bay that can be entered including the Hang Sung Sot, with three mammoth caverns, and the Hang Dao Go, with superbly weird stalagmites and stalactites. For most people though, the highlight is simply cruising amid the karsts and soaking up the changing scenery of pinnacles as you pass by.*

- Key: *cryptophyuit*

- Các kết quả thu được khi chạy chương trình:

```

Microsoft Visual Studio Debug Console
Input text: The karst seascape of Ha Long Bay is one of the world's most spellbinding sea views and is a UNESCO World Heritage Site. With the bay's scenery best seen by boat, this is prime cruising territory. You should opt for at least an overnight tour to see Ha Long Bay's iconic views as a day trip doesn't do it justice. There are plenty of caves in the bay that can be entered including the Hang Sung Sot, with three mammoth caverns, and the Hang Dao Go, with superbly weird stalagmites and stalactites. For most people though, the highlight is simply cruising amid the karsts and soaking up the changing scenery of pinnacles as you pass by.

Key: cryptophyuit

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

Select (1) encrypt / (2) decrypt
1

Ciphertext: PUINGYZCXIOWYOHNUIUHKGLHDGDCIXNUIPUDXGCMBWKICCCZHNNVVLEKEBLHXIGWBFXVHMEBWOHQIXOISAGVEABPFCHAIXFCDXFCUPENDG
CWCONXBPRDIXCZNPXDRIGUYPUKCKCTYDKIPTGKCEKURBPCBCUYPCAOZUGGQIATCIUYGRQDHZCHMGSBPKEAUPZCUGTCUXINEGMHKBOLDACKOIKERSBFXVOW
DMDACYECIAIXQPIAFCFZCKOFFENPBGYNHNBQPCAITGWIXEKPUFDDAPUUYOLENPNXPFPBEBKPQGEBLHPUNEHMOVHQOVUCSDPUPUPBDNDWKAPUYOXBPLWO
MEPUNEHMBABGAGSDPUZOHNGLMRXDBCIWYUMGALFCIXHMIWYUMGRFCIXIUYLICCTIHRNFPUGOAUPENOEAKBAUCFVZCKNYMRRYOFCKLHDWBEPUIINGYZCWO
MECIOMEKAOTCENPOHMOBLHCONXBPCAETEMHRKIXOWCAHTOWVIPW
C:\Users\ADMIN\source\repos\21521149_MMH\x64\Debug\Lab01_playfair.exe (process 30696) exited with code 0.
Press any key to close this window . . .

```

Hình. Kết quả mã hoá đoạn text bằng chương trình vừa viết

```

Microsoft Visual Studio Debug Console

Input text: PUINGYZCXIOWYOHNIUHKGLHDGDCIXNUIPUDXGCMWIKICZHNWVLEKEBLHXIGWBFVHMEBWOHQIXOISAGVEABPFCXAIFCDXFCUPENDGC
WCONXBPRDIXCZNPXNDRIUGYPUKCKCTYDKIPTGKCEKURBPCBCUYPYCAOZUGGQIATCIUYGRQDHZCHMGSPKEAUPZCUGTCUXINEGMHKBLDACKOIKERSBFXVOWDM
DACYECIAIXQPIAFCDZCKOFENPBGYNNHNBQCAITGWIXEKPUDFADPUUYOLENPNXFPFBEBKQGEHLHPUNEHMOVHQOUCSDPUPUPBDNDWKAPUYOXBPLWOMEPE
UNEHMABHGAGSDPUZOHNGLMRXDBCIWYUMGALFCIXHMIWYUMGRFCIXIUYLICCTIHRNFPUGOAUPENOEAKUBAUCFVZCKNYMRRYOFCKLHDWBEPUINGYZCWOMECEI
OMEKAOCTCENPOHMOBLHCONXBPCAEATEKMRKIXOWCAHTOWVIPW

Key: cryptographyuit

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

Select (1) encrypt / (2) decrypt
2

Plaintext: THEKARSTSEASCAPEOFHALONGBAYISONEOFTHETWORLDSPLEASINGVIEWSSANDISAUNESCOWORLDERITAGESITWITHTHEBAYS
SCENERYBESTSEENBYBOATTHISISPRIMECRUISINGTERRITORYYOU SHOULD OPT FOR AT LEAST AN OVERNIGHT TOUR TO SEE HALONGBAY'S ICONIC VIEWS AS A
YTRIP DOESN'T DO IT JUSTICE. THERE ARE PLenty OF CAVES IN THE BAY THAT CAN BE ENTERED INCLUDING THE HANG SUNG SOT WITH THREE MAMMOTH CAVERNS AND TH
EHANGDAO GOWITH SUPERBLY WEIRD STALAGMITES AND STALACTITES FORMOST PEOPLE THOUGH THE HIGHLIGHT IS SIMPLY CRUISING AMID THE KARST SANDS OF A
KINGDOM THE CHANGING SCENERY OF PINNACLES AS YOU PASS BYX
C:\Users\ADMIN\source\repos\21521149_MMH\X64\Debug\Lab01_playfair.exe (process 25568) exited with code 0.
Press any key to close this window . . .

```

Hình. Kết quả giải mã đoạn text bằng chương trình vừa viết

- Kiểm tra lại kết quả (dùng <https://www.dcode.fr/vigenere-cipher>):

PUINGYZCXIOWYOHNIUHKGLHDGDCIXNUIPUDXGCMWIKICZHNWVLEKEBLHXIGWBFVHMEBWOHQIXOISAGVEABPFCXAIFCDXFCUPENDGCWCONXBPRDIXCZNPXNDRIUGYPUKCKCTYDKIPTGKCEKURBPCBCUYPYCAOZUGGQIATCIUYGRQDHZCHMGSPKEAUPZCUGTCUXINEGMHKBLDACKOIKERSBFXVOWDM

MDACYECIAIXQPIAFCDZCKOFENPBGYNNHNBQCAITGWIXEKPUDFADPUUYOLENPNXFPFBEBKQGEHLHPUNEHMOVHQOUCSDPUPUPBDNDWKAPUYOXBPLWOMEPEUNEHMABHGAGSDPUZOHNGLMRXDBCIWYUMGALFCIXHMIWYUMGRFCIXIUYLICCTIHRNFPUGOAUPENOEAKUBAUCFVZCKNYMRRYOFCKLHDWBEPUINGYZCWOMECEIOMEKAOCTCENPOHMOBLHCONXBPCAEATEKMRKIXOWCAHTOWVIPW

Twitter going all in on Jetpack Compose for feature development

Learn More

PlayFair Cipher - dCode

Tag(s) : Polygrammic Cipher, GRID\_CIPHER

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to

O G A H U

I B D E F

K L M N Q

S V W X Z

CRYPTOGAHUIBDEFKLMNQSVWXZ

SHIFT IF SAME ROW Cell on the left ← (Encryption with right cell →)

SHIFT IF SAME COLUMN Cell above ↑ (Encryption with below cell ↓)

ORDER OF LETTER ELSEWHERE Same row as letter 1 first

▶ DECRYPT PLAYFAIR

▶ BRUTEFORCE DECRYPTION ATTACK WITH THE GRID

WITHOUT KNOWING KEY

KNOWN PLAINTEXT

▶ KNOWN PLAINTEXT ATTACK

PLAYFAIR ENCODER

PLAYFAIR PLAIN TEXT

The karst seascape of Ha Long Bay is one of the world's most spellbinding sea views, and is a UNESCO World Heritage Site. With the bay's scenery best seen by boat, this is prime cruising territory. You should opt for at least an overnight tour to see Ha Long Bay's iconic views as a day trip doesn't do it justice. There are plenty of caves in the bay that can be entered including the Hang Sung Sot, with three mammoth caverns, and the Hang Dao

PLAYFAIR GRID

C R Y P T

O G A H U

I B D E F

K L M N Q

S V W X Z

CRYPTOGAHUIBDEFKLMNQSVWXZ

How to decrypt a PlayFair cipher?

How to recognize PlayFair ciphertext?

How to decipher PlayFair without the grid/key?

Multiple grids can fit a PlayFair cipher?

What are the variants of the PlayFair cipher?

When PlayFair was invented?

Similar pages

Two-square Cipher

Slidefair Cipher

Collon Cipher

Three Squares Cipher

Bifid Cipher

Four Square Cipher

Letters Bars

DCODE'S TOOLS LIST

Support

Paypal

Patreon

More

Forum/Help

DISCORD

Keywords

playfair, play, fair, lord, game, key, wheatstone, grid

Hình. Kết quả mã hoá đoạn text bằng dcode

PHÒNG THÍ NGHIỆM  
AN TOÀN THÔNG TIN

Báo cáo Mật mã học  
HỌC KỲ 2 – NĂM HỌC 2022-2023



Hình. Kết quả giải mã đoạn text bằng dcode

### b, Mã hoá bản rõ dựa trên ma trận khoá cho trước

- Đoạn text: LEDOANTRAMYATTTUITCOBONLACAMTUCAUTUDANGDAQYBINGAN

- Ma trận khoá:

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

Figure 5: Playfair matrix for task

- Mã hoá:

+ Tiến hành xử lý đoạn text trên, tách thành các cặp 2 ký tự và xử lý chuỗi lặp, lẻ nếu có  
LE | DO | AN | TR | AM | YA | TX | TX | TU | IT | CO | BO | NL | AC | AM | TU | CA | UT | UD  
| AN | GD | AQ | UY | BI | NG | AN

+ Xử lý mã hoá theo từng cặp, thu được các cặp chữ tương ứng:

GD | FL | IV | BL | OI | VO | HW | HW | BP | TH | FA | MR | PA | IN | OI | BP | NI | PB | PK |  
IV | LE | GN | SZ | IT | QA | IV

+ Kết quả: GD FL IV B LO I V O H W H W B P T H F A M R P A I N O I B P N I P B P K I V L E G N S Z I T Q A I V

## 5. Polyalphabetic cipher – Vigenère

- **Mật mã Vigenère** là phương pháp mã hoá thay thế đa bảng chữ cái bằng cách sử dụng xen kẽ một số phép mã hóa Caesar khác nhau dựa trên các chữ cái của từ khóa.

### - Thuật toán Vigenère:

+ Encryption:  $E_i = (P_i + K_i) \bmod 26$

+ Decryption:  $P_i = (E_i - K_i + 26) \bmod 26$

### - Các đoạn code trong Vigenère:

+ Khi tiến hành giải mã/mã hoá cần tạo một key mới có chiều dài bằng với đoạn text đã cho bằng cách lặp lại key trong chuỗi key mới:

```
void createNewKey(string text, string key, string& newkey) //tạo key mới có độ dài bằng độ dài text bằng cách lặp lại key
{
    int i, j;
    for (i = 0, j = 0; i < text.length(); i++, j++)
    {
        if (((text[i] >= 'A' && (text[i] <= 'Z')) || ((text[i] >= 'a' && (text[i] <= 'z')))) //nếu ký tự là chữ thì lặp lại trong key mới, còn không giữ nguyên
        {
            if (j == key.length())
                j = 0; //khi j = độ dài chuỗi key, lặp lại key trong chuỗi mới
            newkey[i] = key[j];
        }
        else
        {
            j--;
        }
    }
}
```

Hình. Đoạn code tạo key mới

+ Đoạn code Vigenère Encrypt:

```
void encrypt(string text, string key)
{
    char alphabet[26] = { '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' };
    string output = text;

    for (int j = 0; j < text.length(); j++)
    {
        for (int i = 0; i < 26; i++)
        {
            if (text[j] == alphabet[i])
            {
                output[j] = alphabet[(abs(text[j] + key[j]) % 26)];
                break;
            }
        }
    }
    cout << "\nCiphertext: " << output;
}
```

Hình. Đoạn code Vigenère Encrypt

+ Đoạn code Vigenère Decrypt:

```
void decrypt(string text, string key)
{
    char alphabet[26] = { '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' };
    string output = text;

    for (int j = 0; j < text.length(); j++)
    {
        for (int i = 0; i < 26; i++)
        {
            if (text[j] == alphabet[i])
            {
                output[j] = alphabet[(abs(text[j] - key[j] + 26) % 26)];
                break;
            }
        }
    }
    cout << "\nPlaintext: " << output;
}
```

Hình. Đoạn code Vigenère Decrypt

**- Tiến hành kiểm tra chương trình vừa viết:**

+ Text: *The karst seascape of Ha Long Bay is one of the world's most spellbinding sea views and is a UNESCO World Heritage Site. With the bay's scenery best seen by boat, this is prime cruising territory. You should opt for at least an overnight tour to see Ha Long Bay's iconic views as a day trip doesn't do it justice. There are plenty of caves in the bay that can be entered including the Hang Sung Sot, with three mammoth caverns, and the Hang Dao Go, with superbly weird stalagmites and stalactites. For most people though, the highlight is simply cruising amid the karsts and soaking up the changing scenery of pinnacles as you pass by.*

+ Key: *cryptographyuit*

+ Kết quả thu được khi chạy chương trình:

```

Microsoft Visual Studio Debug Console

Input text: The karst seascape of Ha Long Bay is one of the world's most spellbinding sea views and is a UNESCO World Heritage Site
. With the bay's scenery best seen by boat, this is prime cruising territory. You should opt for at least an overnight tour to see
Ha Long Bay's iconic views as a day trip doesn't do it justice. There are plenty of caves in the bay that can be entered including
the Hang Sung Sot, with three mammoth caverns, and the Hang Dao Go, with superbly weird stalagmites and stalactites. For most peopl
e though, the highlight is simply cruising amid the karsts and soaking up the changing scenery of pinnacles as you pass by.

Key: cryptographyuit

New key: CRY PTOGR APHYUITC RY PT OGRA PHY UI TCR YP TOG RAPHY'U ITCR YPTOGRAPHYUI TCR YPTOG RAP HY U ITCRYP TOGRA PHYUITCR YPTO. G
RAP HYU ITC'R YPTOGRAPHYUI TCR YP TOGR, APHY UI TCRYP TOGRAPHYUITCRYPTO. GRA PHYUIT CRY PTO GR APHYU IT CRYPTOGRAPHYUI IT CRY PT
OGRA PHY'U ITCRYP TOGRA PH Y UIT CRYPT TOGRA'P HY UI TCRYPTO. GRAPH YUI TCRYPT OG RAPHY UI TCR YPT OGRA PHY UI TCRYPTO GRAPHYUIT CRY
PTOG RAPH YUI, TCRY PTOGR APHYUIT CRYPTOGR, RAP HYU ITCR YPT OG, RAPH YUITCRYP TOGRA PHYUITCRYPT OGR APHYUITCRYP. TOG RAPH YUITCR Y
PTOGR, APH YUITCRYPT OG RAPHYU ITCRYPTO GRAP HYU ITCRYP TOG RAPHYUI TC RYP TOGRAPHYUITCRYP TO GRAPHYUIT CR YPT OGRA PH.

Select (1) encrypt / (2) decrypt
1

Ciphertext: VYC ZTFYK STHQWIIIG FD WT ZUEG QHW CA HPV MU MVK NOGSB'M UHUK QEXZRSICKGHO LGR TXXKY RNS PQ U CGGJAD PCXCD WLPBCTIV QXMS
. CZTW AFY JTA'J QRXBKIY QLQN AXGE ZN UCGK, TWPQ CA ITZKT VFAZSXUE NMKTZRDKM. EFU HOMOTW QGR UHF GK LTHQN IG QMGGMWYT IVSL BH UVC
WT ZUEG QHW'M QVQEGR OMKNS PZ Y XIR VIGE WCKJN'I KM CB CWRXVS. ZYEG L YLM INVLIR CL TAKLQ CV MJV ZPR HNRT RHL VM XPXCGXR OECABBCVZ
VYC WTBM JUCN QIB, PKKF IAFKV MPTKIBA ERTTKBY, RNS AFY PTPX BPH UU, NIIO QOXXTSJN PSOID HAYFIZOZRTL OTU SIHJUKMKKCH. YCX DOHA NYWIN
V RWHIMY, TWL FCOANZEMW WY JIBWJS KKWZQXGU GDIS AFY STTJRH TBJ JOPRGHO NR KFT VVGEGXUE MKXPVNP HT VZNCHAFML CJ WDN DGJS QF.
C:\Users\ADMIN\source\repos\21521149_MMH\64\Debug\Lab01_vigenere.exe (process 25336) exited with code 0.
Press any key to close this window . . .
  
```

Hình. Kết quả mã hoá đoạn text bằng chương trình vừa viết

+ Giải mã ngược lại đoạn kết quả trên:

```

Microsoft Visual Studio Debug Console

Input text: VYC ZTFYK STHQWIIIG FD WT ZUEG QHW CA HPV MU MVK NOGSB'M UHUK QEXZRSICKGHO LGR TXXKY RNS PQ U CGGJAD PCXCD WLPBCTIV QXMS
. CZTW AFY JTA'J QRXBKIY QLQN AXGE ZN UCGK, TWPQ CA ITZKT VFAZSXUE NMKTZRDKM. EFU HOMOTW QGR UHF GK LTHQN IG QMGGMWYT IVSL BH UVC
WT ZUEG QHW'M QVQEGR OMKNS PZ Y XIR VIGE WCKJN'I KM CB CWRXVS. ZYEG L YLM INVLIR CL TAKLQ CV MJV ZPR HNRT RHL VM XPXCGXR OECABBCVZ
VYC WTBM JUCN QIB, PKKF IAFKV MPTKIBA ERTTKBY, RNS AFY PTPX BPH UU, NIIO QOXXTSJN PSOID HAYFIZOZRTL OTU SIHJUKMKKCH. YCX DOHA NYWIN
V RWHIMY, TWL FCOANZEMW WY JIBWJS KKWZQXGU GDIS AFY STTJRH TBJ JOPRGHO NR KFT VVGEGXUE MKXPVNP HT VZNCHAFML CJ WDN DGJS QF.

Key: cryptographyuit

New key: CRY PTOGR APHYUITC RY PT OGRA PHY UI TCR YP TOG RAPHY'U ITCR YPTOGRAPHYUI TCR YPTOG RAP HY U ITCRYP TOGRA PHYUITCR YPTO. GR
AP HYU ITC'R YPTOGRAPHYUI TCR YP TOGR, APHY UI TCRYP TOGRAPHYUITCRYPTO. GRA PHYUIT CRY PTO GR APHYU IT CRYPTOGRAPHYUI IT CRY PT
OGRA PHY'U ITCRYP TOGRA PH Y UIT CRYPT TOGRA'P HY UI TCRYPTO. GRAPH YUI TCRYPT OG RAPHY UI TCR YPT OGRA PHY UI TCRYPTO GRAPHYUIT CRY PT
OG RAPH YUI, TCRY PTOGR APHYUIT CRYPTOGR, RAP HYU ITCR YPT OG, RAPH YUITCRYP TOGRA PHYUITCRYPT OGR APHYUITCRYP. TOG RAPH YUITCR YPTO
GR, APH YUITCRYPT OG RAPHYU ITCRYPTO GRAP HYU ITCRYP TOG RAPHYUI TC RYP TOGRAPHYUITCRYP TO GRAPHYUIT CR YPT OGRA PH.

Select (1) encrypt / (2) decrypt
2

Plaintext: THE KARST SEASCAPE OF HA LONG BAY IS ONE OF THE WORLD'S MOST SPELLBINDING SEA VIEWS AND IS A UNESCO WORLD HERITAGE SITE.
WITH THE BAY'S SCENERY BEST SEEN BY BOAT, THIS IS PRIME CRUISING TERRITORY. YOU SHOULD OPT FOR AT LEAST AN OVERNIGHT TOUR TO SEE HA
LONG BAY'S ICONIC VIEWS AS A DAY TRIP DOESN'T DO IT JUSTICE. THERE ARE PLenty OF CAVES IN THE BAY THAT CAN BE ENTERED INCLUDING THE
HANG SUNG SOT, WITH THREE MAMMOTH CAVERNS, AND THE HANG DAO GO, WITH SUPERBLY WEIRD STALAGMITES AND STALACTITES. FOR MOST PEOPLE THO
UGH, THE HIGHLIGHT IS SIMPLY CRUISING AMID THE KARSTS AND SOAKING UP THE CHANGING SCENERY OF PINNACLES AS YOU PASS BY.
C:\Users\ADMIN\source\repos\21521149_MMH\64\Debug\Lab01_vigenere.exe (process 52884) exited with code 0.
Press any key to close this window . . .
  
```

Hình. Kết quả giải mã đoạn text bằng chương trình vừa viết



- Kiểm tra lại kết quả (dùng <https://www.dcode.fr/vigenere-cipher>):

Vigenere CRYPTOGRAPHYUIT  
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

Vyc ztfyk sthqwieg fd wt Zueg Qhw ca hvp mu mvk nogsb'm uhuk qexzrsickgho lgr txxky rns pq u CGGJAD Pxcd Wlpcbtiv Qxms. Cztw afy jta'j qrxbkiiy qlqn axge zn ucgk, twpq ca itzkt vfazsxue nmktzrdkm. Efu homotw qgr uhf gk lthqn ig qmcggwmyt ivsl bh uvc Wt Zueg Qhw'm qvqegr owkns pz y xir vige wckjn'i km cb cwjrxvs. Zyeql ylm invlir cl taklq cv mjb zpr hnrh rh1 vm xpkcgr oecabbcvz vyc Wtbn Jucn Qib, pkkf iafkv mptkiba erttkby, rns afy Ptpx Bph Uu, niio qoxxtsjn psoid hayfizozrtl otu sihjukmkch. Ycx doha nywinv rwhimy, twl fcoanzewm wy jibwjs kkwzqxgu gdis afy sttjrh tbj joprgho nr kft vvgexue mkxpvpn ht vznchafm1 cj wdn dgjs qf.

**Lắp Bảng Trắng Toàn Quốc**  
bangtot.vn chuyên sản xuất, lắp đặt  
bảng từ trắng giá rẻ, chất lượng tiêu

**VIGENERE CIPHERTEXT (?)**

**PARAMETERS**

★ PLAINTEXT LANGUAGE English

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

**DECRYPTION METHOD**

☒ KNOWING THE KEY/PASSWORD: CYLAB

☐ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

☐ KNOWING ONLY A PARTIAL KEY: KE?

☐ KNOWING A PLAINTEXT WORD:

☐ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

▶ DECRYPT

See also: Beaufort Cipher – Caesar Cipher

**VIGENERE ENCODER**

★ VIGENERE PLAIN TEXT (?)

The karst seascape of Ha Long Bay is one of the world's most spellbinding sea views and is a UNESCO world Heritage Site. With the bay's scenery best seen by boat, this is prime cruising territory. You should opt for at least an overnight tour to see Ha Long Bay's iconic views as a day trip doesn't do it justice. There are plenty of caves in the bay that can be entered including the Hang Sung Sot, with three mammoth caverns, and the Hang Dao

★ CIPHER KEY CRYPTOGRAPHYUIT

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

Hình. Kết quả giải mã đoạn text bằng dcode

## 6. Other ciphers:

### a, Tìm flag của thông điệp

- Thông điệp:

TXpNek5ETXpNek16TXpNMU16TXpNak16TXpVek16TTVNek16TIRNek16QXpNek0xTXp  
Nek5ETXpNelF6TkRNMk16TXpORE16TXpjek16TTFNek16TWpNek16UXpNek14TXpNek  
5UTXpNekF6TXpNME16TXpPRE16TXpVek16TTU=

- Giải mã:

+ Nhận thấy dấu '=' ở cuối thông điệp, ta giải mã thông điệp sang Base64 (sử dụng <https://www.base64decode.org/>), thu được thông điệp mới:

MzMzNDMzMzMzMzM1MzMzMjMzMzUzMzM5MzMzNTMzMzMzMzM1MzMzNDMzMzMzQz  
NDM2MzMzNDMzMzczMzM1MzMzMjMzMzQzMzMzMzMzMzNTMzMzMzMzM0MzMzODMz  
MzUzMzM5

+ Tiếp tục giải mã thông điệp mới trên sang Base64 (sử dụng <https://www.base64decode.org/>), thu được thông điệp mới:

333433333335333233353339333533303335333433343436333433373335333233343331333533303334333833353339

+ Thông điệp mới thu được ở trên là mã Thập lục phân (hexadecimal), ta chuyển thông điệp đó sang chữ - mã ASCII (sử dụng <https://anytexteditor.com/vi/hex-to-ascii>), thu được thông điệp mới: 343335323539353035343446343735323431353034383539

+ Tiếp tục chuyển thông điệp trên sang chữ - mã ASCII (sử dụng <https://anytexteditor.com/vi/hex-to-ascii>), thu được thông điệp mới:

43525950544F475241504859

+ Tiếp tục chuyển thông điệp trên sang chữ - mã ASCII (sử dụng <https://anytexteditor.com/vi/hex-to-ascii>), thu được thông điệp mới: CRYPTOGRAPHY

- **Kết luận:** Vậy flag của thông điệp là **CRYPTOGRAPHY**.

## b, Mật mã cổ điển khác – Affine:

- **Mật mã Affine** là một loại mật mã thay thế một chữ cái, trong đó mỗi chữ cái trong bảng chữ cái được ánh xạ thành số tương đương của nó, được mã hóa bằng một hàm toán học đơn giản và được chuyển đổi trở lại thành một chữ cái.

### - Thuật toán Affine:

+ Encryption:  $E(p, k) = (a \cdot p + b) \bmod 26$

+ Decryption:  $P(c, k) = (a^{-1}(c - b)) \bmod 26$

Với:  $k$  là một bộ gồm 2 thành phần  $k = (a, b)$ ,  $a^{-1}$  là module nghịch đảo của  $a$ .

- Các đoạn code trong Affine:

+ Đoạn code Affine Encrypt:

```
void encrypt(string text, int a, int b)
{
    char alphabet[26] = { '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' };
    char alphabet1[26] = { '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' };
    string output = text;
    for (int j = 0; j < text.length(); j++)
    {
        for (int i = 0; i < 26; i++)
        {
            if (text[j] == alphabet[i])
            {
                output[j] = alphabet[abs(a * i + b) % 26];
                break;
            }
            else if (text[j] == alphabet1[i])
            {
                output[j] = alphabet1[abs(a * i + b) % 26];
                break;
            }
        }
    }
    cout << "\nCiphertext: " << output;
}
```

Hình. Đoạn code Affine Encrypt

## + Đoạn code Affine Decrypt:

```

void decrypt(string text, int a, int b)
{
    char alphabet[26] = { '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' };
    char alphabet1[26] = { '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' };
    int moduLDN = 0, check = 0;
    string output = text;

    for (int i = 0; i <= 25; i++)//tim modul đảo nghịch của a
    {
        check = (a * i) % 26;
        if (check == 1)
        {
            moduLDN = i;
        }
    }

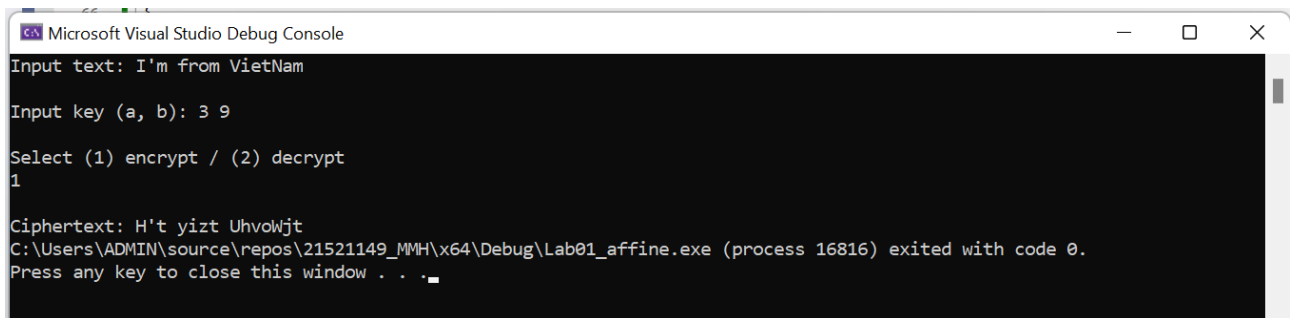
    for (int j = 0; j < text.length(); j++)
    {
        for (int i = 0; i < 26; i++)
        {
            if (text[j] == alphabet[i])
            {
                output[j] = alphabet[abs(moduLDN * (i - b + 26)) % 26];
                break;
            }
            else if (text[j] == alphabet1[i])
            {
                output[j] = alphabet1[abs(moduLDN * (i - b + 26)) % 26];
                break;
            }
        }
    }
    cout << "\nPlaintext: " << output;
}

```

Hình. Đoạn code Affine Decrypt

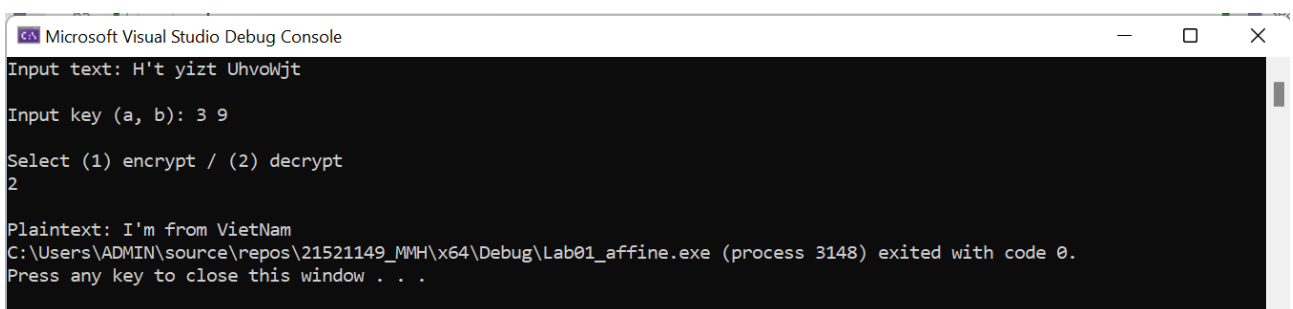
**- Tiến hành kiểm tra chương trình vừa viết:**+ Text: *I'm from VietNam*+ Key:  $a = 3, b = 9$ 

+ Kết quả thu được:



Hình. Kết quả mã hoá đoạn text bằng chương trình vừa viết

+ Giải mã ngược lại đoạn kết quả trên:



Hình. Kết quả giải mã đoạn text bằng chương trình vừa viết

- Kiểm tra lại kết quả (dùng <https://www.dcode.fr/affine-cipher>):

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:  
e.g. type 'boolean'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

$f(x)=3x+9$   
H't yizt Uhvwjzt

**Get started on Google Cloud**

High-performance infrastructure for cloud computing, data analytics & machine learning.

**AFFINE DECODER**

★ AFFINE CIPHERTEXT ?  
H't yizt Uhvwjzt

★ EXPECTED PLAINTEXT LANGUAGE English

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

► AUTOMATIC BRUTE FORCE DECRYPTION

**MANUAL PARAMETERS AND OPTIONS**

★ A COEFFICIENT 3

★ B COEFFICIENT 9

☒ DISPLAY THE DECRYPTED MESSAGE WITH THESE COEFFICIENTS

☐ DISPLAY AFFINE DECODING/DESUBSTITUTION TABLE FOR THESE COEF.

☐ DISPLAY AFFINE CODING/SUBSTITUTION TABLE FOR THESE COEF.

☐ DISPLAY AFFINE COEFFICIENTS BY MODULAR INVERSE

► DECRYPT

See also: Hill Cipher – Multiplicative Cipher – Caesar Cipher

**AFFINE ENCODER**

★ AFFINE PLAIN TEXT ?  
I'm from Vietnam

Hình. Kết quả giải mã đoạn text bằng dcode