Phòng thí nghiệm An toàn Thông tin InsecLab
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: Nhập môn mạng

Tên chủ đề: Lab 1

GVHD: Tô Trọng Nghĩa

Nhóm: Mệt mỏi

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: ATTT2021

STT	Họ và tên	MSSV	Email
1	Nguyễn Thị Minh Châu	21520645	21520645@gm.uit.edu.vn
2	Lưu Thị Huỳnh Như	21521242	21521242@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	100%	1 - 3
2	Yêu cầu 2	100%	3 – 4
3	Yêu cầu 3	100%	4 - 8
4	Yêu cầu 4	100%	8 - 14
5	Yêu cầu 5	100%	14 - 16
6	Yêu cầu 6	100%	16 - 18
7	Bài nâng cao	100%	18 - 21
Điểm tự đánh giá			**10/10**

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

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Task 1:

a) 6, 8, 2 has 1 number placed in right spot and 6, 1, 4 has 1 right number but wrong spot so that 6 is a wrong number. And 7, 3, 8 don't have any right number so the right number is 2 and placed at third spot.

Because 7, 3, 8 are wrong and 7, 8, 0 has 1 right number so the right one is 0.

2, 0, 6 has 2 right numbers but wrong placed and we got 2 right numbers are 2, 0; plus 7,8,0 has 1 right number but wrong placed so we have 0 in the first spot.

6, 1, 4 has 1 right number but wrong placed. We know 6 is the wrong number so the wrong number can be 1 or 4. But we only missing the second spot left so the right number can't be 1. So the right number is 4 and it is in the second spot.

->The code is 0 4 2

b)

Case 1/ 3 + =

All the cases we have:

- =1, =8, =1
- =2, =5, =1
- =3, =2, =1
- =5, =7, =2
- =6, =4, =2
- =7, =1, =2
- =8, =9, =3
- =9, =6, =3

Case2/ 2 +2 =

All the cases we have:

- = 3, = 8, = 2
- = 4, = 7, = 2
- = 5, = 6, = 2
- = 6, = 5, = 2
- = 7, = 4, = 2

- = 8, = 3, = 2 (remove because doesn't include in case 1)

➔ = 2

Because = 2 so all the case 1 only got:

- =1, =8, =1
- =8, =9, =3
- =9, =6, =3

And so that we can remove all the cases that doesn't include in case 1 so all the possible case 2 are

- = 3, = 8, = 2
- = 5, = 6, = 2

We continue remove the case with =8, =9, =2 in case 1 because in case 2 we don't have any case with =9

3/ + +2 =

All the cases we have:

- = 1, = 4, = 9, = 2, = 3
- = 4, = 1, = 9, = 2, = 3

➔ =9, =3

Because =9 so = 6 and because = 6 so =5

So and with be 7 or 8

Call "?" in these cells (3,1), (3,2), (4,1) x, y, z respectively

We have equations (1): $\begin{cases} x + y + 5 + \ = 22 \\ \ + 2 * 9 + y = 33 \\ \ + 9 + x + z = 29 \end{cases} \leftrightarrow \begin{cases} x + y + 5 + \ = 22 \\ 9 + y - x - z = 4 \end{cases}$

Assume that = 7:

We have equation: z+2*9+6=27

->z=3

Replace z in (1) we got $\begin{cases} x + y + 5 + \ = 22 \\ 9 + y - x - 3 = 4 \end{cases}$

Assume that =1 -> x=9, y=7 -> = 8

Assume that ☆=4 ->x=7.5, y=5.5(remove)

Assume that ☆= 8

We have equation: z+2*9+6=28

->z=4

Replace z in (1) we got $\begin{cases} x + y + 5 + ☆ = 22 \\ 9 + y - x - 4 = 4 \end{cases}$

Assume that ☆=1 -> x=8.5, y=7.5 (remove)

Assume that ☆=4 ->x=7, y=6 -> ☆=9 (remove)

So ☆=1, ☆=2, ☆=3, ☆=4, ☆ =5, ☆=6, ☆=7, ☆=8, ☆=9

Task 2:

Code encrypt:

```
def caesar_encrypt(text, shift):
    result = ""
    for i in range(len(text)):
        char = text[i]
        if char.isalpha():
            ascii = ord(char)
            new_ascii = ascii + shift
            if char.isupper():
                new_char = chr((new_ascii - 65) % 26 + 65)
            else:
                new_char = chr((new_ascii - 97) % 26 + 97)
        else:
            new_char = char
        result += new_char
    return result
```

Code decrypt:

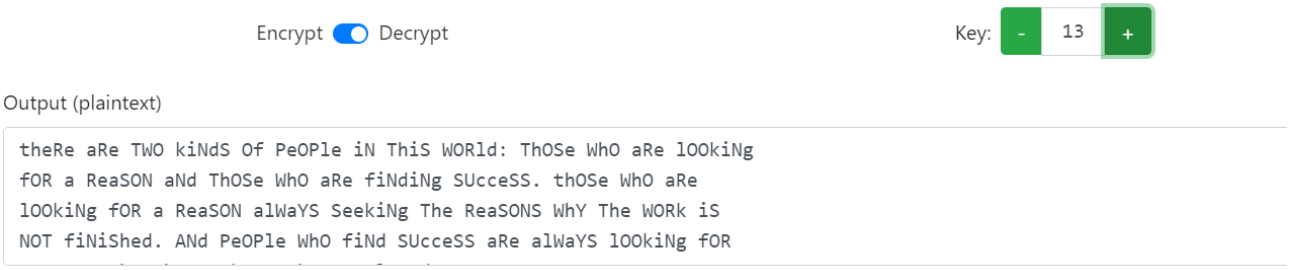
```
def caesar_decrypt(cipher_text):
    for shift in range(26):
        result = ""
        for i in range(len(cipher_text)):
            char = cipher_text[i]
            if char.isalpha():
                ascii = ord(char)
```

```
                new_ascii = ascii - shift
                if char.isupper():
                    new_char = chr((new_ascii - 65) % 26 + 65)
                else:
                    new_char = chr((new_ascii- 97) % 26 + 97)
            else:
                new_char = char
            result += new_char
        print("Shift {}: {}".format(shift, result))
```

The result when using the application:

```
Shift 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.
```

The result when using CrypTool2:



The key used in this ciphertext is 13. This is a common key. It is also called ROT13.

Task 3:

Because of the frequency of “ytn” is the most so I guess this is “the”. Next we can assume that “v” is “a” and “x” is “o” due to the frequency

Look at the frequency we guess “u” is “i” but it appear some meaningless word like “ai”,.. so we assume “u” is “n”

We got some 3-char word start with “en” , “ an” and the last character is “p” so we can replace “p” with “d”

We have a word UVYMXUVI is decrypted to (nat_ona_) so I guess this word is “national”, “m” is “i” and “i” is “l”

VFXMP is decrypted to (a_oid) so we replace “f” with “v”

IXUR is decrypted to “lon_” so we replace “r” with “g”

VHN is decrypted to “a_e” so we replace “h” with “r”

YZHU is decrypted to "t_rn" so we replace "z" with "u"
VGXZY is decrypted to "a_out" so we replace "g" with "b"
VBYNH is decrypted to "a_ter" so we replace "b" with "f"
IMSN is decrypted to " "li_e" so we replace "s" with "k"
CVSN is decrypted to "_ake" so we replace "c" with "m"
CXQY is decrypted to "mo_t" so we replace "q" with "s"
QZUPVD is decrypted to " sunda_" so we replace "d" with "y"
LMYTXZY is decrypted to "_ithout" so we replace "l" with "W"
GNAVZQN is decrypted to "ba_ause" so we replace "a" with "c"
QTVEN is decrypted to "sha_e" so we replace "e" with "r"
JZNQYMXU is decrypted to "_uestion" so we replace "j" with "q"
NKYHV is decrypted to "e_tra" so we replace "k" with "x"
OZQY is decrypted to "_ust" " so we replace "o" with "j"
EMAYZHN is decrypted to "_icture" so we replace "e" with "p"

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
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

Plain text:
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 hollywood women who helped raise millions of dollars to fight sexual harassment around the country

signaling their support golden globes attendees swathed themselves in black sported lapel pins and sounded off about sexist power imbalances from the red carpet and the stage on the air e was called out about pay inequity after its former anchor catt sadler quit once she learned that she was making far less than a male cohost and during the ceremony natalie portman took a blunt and satisfying dig at the allmale roster of nominated directors how could that be topped

as it turns out at least in terms of the oscars it probably wont be

women involved in times up said that although the globes signified the initiatives launch they never intended it to be just an awards season campaign or one that became associated only with redcarpet actions instead a spokeswoman said the group is working behind closed doors and has since amassed million for its legal defense fund which after the globes was flooded with thousands of donations of or less from people in some countries

no call to wear black gowns went out in advance of the oscars though the movement will almost certainly be referenced before and during the ceremony especially since vocal metoo supporters like ashley judd laura dern and nicole kidman are scheduled presenters

another feature of this season no one really knows who is going to win best picture arguably this happens a lot of the time inarguably the nailbiter narrative only serves the awards hype machine but often the people forecasting the race socalled oscarologists can make only educated guesses

the way the academy tabulates the big winner doesnt help in every other category the nominee with the most votes wins but in the best picture category voters are asked to list their top movies in preferential order if a movie gets more than percent of the firstplace votes it wins when no movie manages that the one with the fewest firstplace votes is eliminated and its votes are redistributed to the movies that garnered the eliminated ballots secondplace votes and this continues until a winner emerges

it is all terribly confusing but apparently the consensus favorite comes out ahead in the end this means that endofseason awards chatter invariably involves tortured speculation about which film would most likely be voters second or third favorite and then equally tortured conclusions about which film might prevail

in it was a tossup between boyhood and the eventual winner birdman in with lots of experts betting on the revenant or the big short the prize went to spotlight last year nearly all the forecasters declared la la land the presumptive winner and for two and a half minutes they were correct before an envelope snafu was revealed and the rightful winner moonlight was crowned

this year awards watchers are unequally divided between three billboards outside ebbing missouri the favorite and the shape of water which is the baggers prediction with a few forecasting a hail mary win for get out

but all of those films have historical oscarvoting patterns against them the shape of water has nominations more than any other film and was also named the years best by the producers and directors guilds yet it was not nominated for a screen actors guild award for best ensemble and no film has won best picture without previously landing at least the actors nomination since braveheart in this year the best ensemble sag ended up going to

three billboards which is significant because actors make up the academys largest branch that film while divisive also won the best drama golden globe and the bafta but its filmmaker martin mcdonagh was not nominated for best director and apart from argo movies that land best picture without also earning best director nominations are few and far between

Task 4:

Code:

```
void vitri(char p, int& h, int& c, char matran[][5])
{
    for (int i=0;i<5;i++)
        for (int j = 0; j < 5; j++) {
            if (matran[i][j] == p) {
                h = i;
                c = j;
                return;
            }
        }
    return;
}

void cungdong(int h, string& c, int c1, int c2, char matran[][5], bool func)
{
    if (func) {
        if (c1 + 1 < 5) c += matran[h][c1 + 1];
        else c += matran[h][0];
       if (c2 + 1 < 5) c += matran[h][c2 + 1];
        else c += matran[h][0];
    }
    else {
        if (c1 - 1 >= 0) c += matran[h][c1 - 1];
        else c += matran[h][4];
        if (c2 - 1 >= 0) c += matran[h][c2 - 1];
        else c += matran[h][4];
    }
    return;
}

void cungcot(int co, string& c, int h1, int h2, char matran[][5], bool func)
{
    if (func) {
        if (h1 + 1 < 5)
            c += matran[h1 + 1][co];
        else c += matran[0][co];
```

```
        if (h2 + 1 < 5)
            c += matran[h2 + 1][co];
        else c += matran[0][co];
    }
    else {
        if (h1 - 1 >= 0)
            c += matran[h1 - 1][co];
        else c += matran[4][co];
        if (h2 -1 >=0)
            c += matran[h2 - 1][co];
        else c += matran[4][co];
    }
    return;
}

void khacdongkhaccot(int h1, int c1, string& c, int h2, int c2, char matran[][5])
{
    c+=matran[h1][c2];
    c+=matran[h2][c1];
    return;
}


void mahoa(string c, char matran[][5])
{
    bool func = 1;
    string code;
    int i = 0, j = 0;
    int h1, c1, h2, c2;
    while (i < c.length())
    {
        vitri(c[i], h1, c1, matran);
        i++;
        while (c[i] == ' ') {
            i++;
        }
        vitri(c[i], h2, c2, matran);
        if (h1 == h2)
        {
            cungdong(h1, code, c1, c2, matran, func);
        }
        else if (c1 == c2)
        {
            cungcot(c1, code, h1, h2, matran,func);
        }
        else
        {
            khacdongkhaccot(h1, c1, code, h2, c2, matran);
```

```
        }
        i++;
        while (c[i] == ' ') {
            i++;
        }
    }
    cout << code;
    return;
}
void giaima(string c, char matran[][5]) {
    bool func = 0;
    string code;
    int i = 0, j = 0;
    int h1, c1, h2, c2;
    while (i < c.length())
    {
        vitri(c[i], h1, c1, matran);
        i++;
        while (c[i] == ' ') {
            i++;
        }
        vitri(c[i], h2, c2, matran);
        if (h1 == h2)
        {
            cungdong(h1, code, c1, c2, matran, func);
        }
        else if (c1 == c2)
        {
            cungcot(c1, code, h1, h2, matran, func);
        }
        else
        {
            khacdongkhaccot(h1, c1, code, h2, c2, matran);
        }
        i++;
        while (c[i] == ' ') {
            i++;
        }
    }
    for (int i = 0; i < code.length(); i++) {
        if (code[i] == 'X')
            continue;
        cout << code[i];
    }
    return;
}
void chuanhoachuoi(string &c) {
    for (int i = 0; i < c.length(); i++) {
```

```
        if (c[i] >= 'a' && c[i] <= 'z')
            c[i] -= 32;
        if (c[i] == 'J') c[i] = 'I';
    }
}
void tachchuoimahoa(string& c) {
    int l = 0;
    for (int i = 0; i < c.length(); i++) {
        if (c[i] != ' ') l++;
        if (l%2!=0&&c[i] == c[i + 1]) {
            c += c[c.length() - 1];
            for (int j = c.length()-1; j > i; j--) {
                c[j] = c[j - 1];
            }
            c[i+1] = 'X';
            l++;
            i++;
        }
    }
    if (l % 2 != 0) {
        c += 'X';
    }
}

int main()
{
    string msg;

    std::cout << "Enter the Encrypted Message:";
    getline(cin, msg);
    chuanhoachuoi(msg);
    tachchuoimahoa(msg);

    cout << "Enter the key: ";
    string key;
    cin >> key;
    chuanhoachuoi(key);

    bool t[26]={};
    char matran[5][5];
    int h = 0, c =0;
    for (int i = 0; i < key.length(); i++) {
        if (key[i] == ' ') continue;
        if (i == 'J' && t['I' - 65] != 0)
            continue;
        if (t[key[i] - 65] == 0)
        {
            if (key[i] == 'J') {
```

```
                matran[h][c++] = 'I';
                t['I' - 65]++;
            }
            else {
                matran[h][c++] = key[i];
                t[key[i] - 65]++;
            }
        }
        if (c == 5) {
            h++;
            c = 0;
        }
    }
    for (int i = 'A'; i <= 'Z'; i++) {
        if (i == 'J' && t['I' - 65] != 0)
            continue;
        if (t[i - 65] == 0)
        {
            if (i == 'J') {
                matran[h][c++] = 'I';
                t['I' - 65]++;
            }
            else {
                matran[h][c++] = i;
                t[i - 65]++;
            }
        }
        if (c == 5) {
            h++;
            c = 0;
        }
    }
    cout << "Encrypt(1) or decrypt(0): ";
    bool flag;
    cin >> flag;
    for (int i = 0; i < 5; i++) {
        for (int j = 0; j < 4; j++) {
            cout << matran[i][j] << " ";
        }
        cout << matran[i][4] << "\n";
    }
    if (flag)
        mahoa(msg, matran);
    else giaima(msg, matran);
    return 0;
}
```

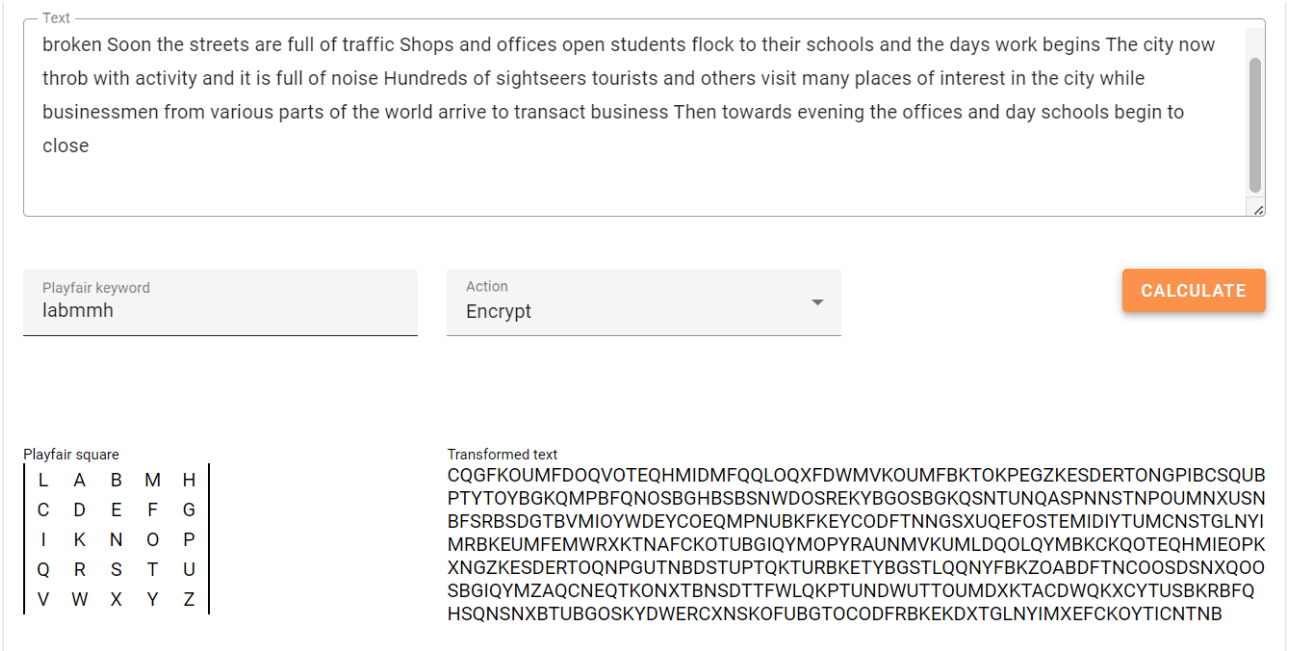
Plain text: Life in the city is full of activity Early in the morning hundreds of people rush out of their homes in the manner ants do when their nest is broken Soon the streets are full of traffic Shops and offices open students flock to their schools and the days work begins The city now throb with activity and it is full of noise Hundreds of sightseers tourists and others visit many places of interest in the city while businessmen from various parts of the world arrive to transact business Then towards evening the offices and day schools begin to close

Key = labmmh

The result when using the application:

```
Enter the Encrypted Message:Life in the city is full of activity Early in the morning hundreds of people rush out of the
ir homes in the manner ants do when their nest is broken Soon the streets are full of traffic Shops and offices open stu
dents flock to their schools and the days work begins The city now throb with activity and it is full of noise Hundreds
of sightseers tourists and others visit many places of interest in the city while businessmen from various parts of the
world arrive to transact business Then towards evening the offices and day schools begin to close
Enter the key: labmmh
Encrypt(1) or decrypt(0): 1
L A B M H
C D E F G
I K N O P
Q R S T U
V W X Y Z
CQGFKOUMFDOQVOTEQHMIDMFQQLOQXFDWMVKOUMFBKTOKPEGZKESDERTONGPIBCSQUBPTYTOYBGKQMPBFQNOSBGHBSBSNWDOSREKYBGOSBGKQSNTUNQASPNNS
TNPOUMNXUSNBFSRBSDGTBVMIOYWDEYCOEQMPNUBKFKEYCODFTNNGSXUQEFOSTEMIDIYTUMCNSTGLNYIMRBKEUMFEMWRXKTNAFCKOTUBGIQYMOPYRAUNMVKUM
LDQOLQYMBKCKQOTEQHMIEOPKXNGZKESDERTOQNPGUTNBDSTUPTQKTURBKETYBGSTLQQNYFBKZOABDFTNCOOSDSNXQOOSBGIQYMZAQCNEQTKONXTBNSDTTFWL
QKPTUNDWUTTOUMDXKTACDWQKXCYTUSBKRBFQHSQNSNXBTUBGOSKYDWERCXNSKOFUBGTOCODFRBKEKDXTGLNYIMXEFCKOYTICNTNB
```

The result when using the online decoder:



b)

Key Matrix:

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

Plaintext: NGUYEN THI MINH CHAU LUU THI HUYNH NHU BAI LAB MOT MON MAT MA HOC

Plaintext diagram: NG UY EN TH IM IN HC HA UL UX UT HI HU YN HN HU BA IL AB MO TM ON MA TM AH OC

Ciphertext diagram: QA SZ CQ HM TB CV IE IG PR QZ PB MT BQ VS IQ BQ IR TA RI FM HB AS IO HB GI AF

Ciphertext: QASZCQHMTBCVIEIGPRQZPBMTBQVSIQBQIRTARIFMHBASIOHBGIAF

Task 5:

Code :

```
def pad_key(plaintext, key):
    padded_key = ''
    i = 0
    for char in plaintext:
        if char.isalpha():
            padded_key += key[i % len(key)]
            i += 1
        else:
            padded_key += ' '
    return padded_key

def _encrypt_decrypt_char(plaintext_char, key_char, mode='encrypt'):
    if plaintext_char.isalpha():
        first_alphabet_letter = 'a'
        if plaintext_char.isupper():
            first_alphabet_letter = 'A'

        old_char_position = ord(plaintext_char) - ord(first_alphabet_letter)
        key_char_position = ord(key_char.lower()) - ord('a')

        if mode == 'encrypt':
            new_char_position = (old_char_position + key_char_position) % 26
        else:
            new_char_position = (old_char_position - key_char_position + 26) % 26
        return chr(new_char_position + ord(first_alphabet_letter))
    return plaintext_char

def encrypt(plaintext, key):
```

```
    ciphertext = ''
    padded_key = _ _key(plaintext, key)
    for plaintext_char, key_char in zip(plaintext, padded_key):
        ciphertext += _encrypt_decrypt_char(plaintext_char, key_char)
    return ciphertext

def decrypt(ciphertext, key):
    plaintext = ''
    padded_key = pad_key(ciphertext, key)
    for ciphertext_char, key_char in zip(ciphertext, padded_key):
        plaintext += _encrypt_decrypt_char(ciphertext_char, key_char,
mode='decrypt')
    return plaintext
```

a.

ciphertext = “The development of Internet of Things technology and the decline of hardware costs have made large-scale camera interconnection possible. Security vendors have cooperated with governments to develop various security standards to achieve interconnection and unified management among cameras of different brands and models. However, there are still some security issues in some standards and their specific implementations. This article takes an existing camera security standard as an example, analyzes these issues in detail and proposes corresponding enhancements. We propose a camera security compliance testing system to test various security capabilities including the one-way authentication capability, the two-way authentication capability and the signaling authentication capability”

key = “helloholle”

The result when using the application:

```
Enter a message: The development of Internet of Things technology and the decline of hardware costs have made large-scale camera in
terconnection possible. Security vendors have cooperated with governments to develop various security standards to achieve intercon
nection and unified management among cameras of different brands and models. However, there are still some security issues in some
standards and their specific implementations. This article takes an existing camera security standard as an example, analyzes these
 issues in detail and proposes corresponding enhancements. We propose a camera security compliance testing system to test various s
ecurity capabilities including the one-way authentication capability, the two-way authentication capability and the signaling authe
ntication capability
Enter a key: helloholle
Ciphertext: Alp oscswzttiye cm Wyeiyrpe cm Hstrnw epqobzwsnc lyr avp oijptys vt slvkalcs jcdew oegp ahrp weykp-dqhzp neticl wuhpcgv
rypqawzy tvwdtpss. Dpgbvtem csyosyw sljl qzztlvlesk ktel nsgpfuapyxz xz oscswzt cectcbg dpgbvtem zhlyhhvod hv onsmlzp tbascnsurpnhp
cy lrk yyttpso xeuerpalbe lqvrr notsclw vj ottmscpra fclbkg lyh tsopzz. Vzhicic, evlfp lvl wetzs gzxi zinffphj twzypd wu gzxi zxlyr
hfod euh esspf daijmqtq paawitiyeoawzyw. Altd oyhtnpl xlvsz oy pbpwetbn qlxiye dpqbftec zxlyrhfo lw hr piotdwp, euewjnlg esizi tdgb
sd tr kielws oyo tysazglg nzvyidacurtyk lrslbjsxpraw. Hp dycazwl e nlalfl dijycthf qzxtsmlyql hpdxprr dmzhpx xv xpdh coctsbw dpqbft
ec jealppztemlw tyqsiotrn xsp cus-hlc hyessuhtneamzy qhdlmmsmej, hos ehs-dej liavpyxpglewvb nlthftwwam lyh alp dwnblwmuk lfhosyemje
etcu qlaeimwthf
Decrypted Plaintext: The development of Internet of Things technology and the decline of hardware costs have made large-scale camer
a interconnection possible. Security vendors have cooperated with governments to develop various security standards to achieve inte
rconnection and unified management among cameras of different brands and models. However, there are still some security issues in s
ome standards and their specific implementations. This article takes an existing camera security standard as an example, analyzes t
hese issues in detail and proposes corresponding enhancements. We propose a camera security compliance testing system to test vario
us security capabilities including the one-way authentication capability, the two-way authentication capability and the signaling a
uthentication capability
```

The result when using online tool dcode.fr :

Vigenere HELLOHOLLE

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

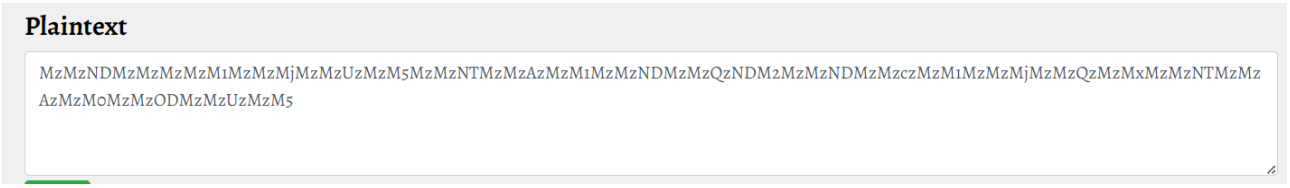
```
Alp oscswzttiye cm Wyeiyrpe cm Hstrnw
epqobzwsnc lyr avp oijptys vt slvkalcs jcdew
oegp ahrp weykp-dqhzp neticl wuhpcgvrypqawzy
tvwdtpss. Dpgbvtem csyosyw sljl qzztlvlesk
ktel nsgpfuapyxz xz oscswzt cectcbg dpgbvtem
zhlyhhvod hv onsmlzp tbascnsurpnhpcy lrk
yyttpso xeuerpalbe lqvrr notsclw vj ottmscpra
fclbkg lyh tsopzz. Vzhicic, evlfp lvl wetzs
gzxi zinffphj twzypd wu gzxi zxlyrhfod euh
esspf daijmqtq paawitiyeoawzyw. Altd oyhtnpl
xlvsz oy pbpwetbn qlxiye dpqbftec zxlyrhfo lw
hr piotdwp, euewjnlg esizi tdgbsd tr kielws
oyo tysazglg nzvyidacurtyk lrslbjsxpraw. Hp
dycazwl e nlalfl dijycthf qzxtsmlyql hpdxprr
dmzhpx xv xpdh coctsbw dpqbftec jealppztemlw
tyqsiotrn xsp cus-hlc hyessuhtneamzy
qhdlmmsmej, hos ehs-dej liavpyxpglewvb
nlthftwwam lyh alp dwnblwmuk lfhosyemjeetcu
qlaeimwthf
```

Task 6:

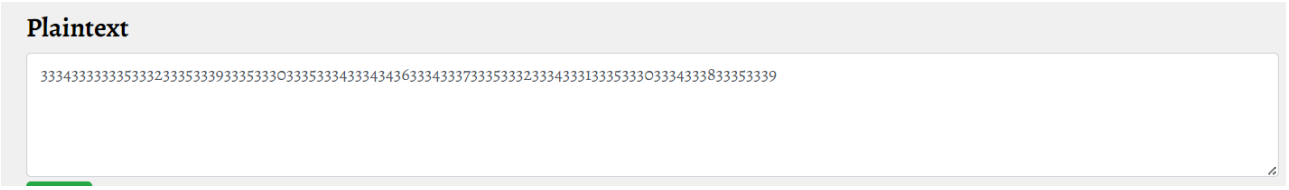
a.

1. Go to boxentriq.com to find out which type of cipher is. It is said Base64

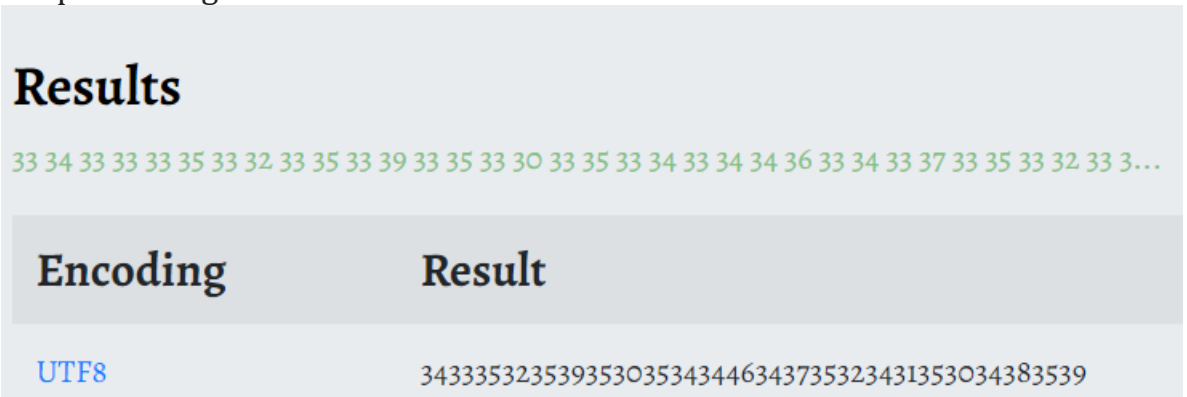
2. Go to Base64 Decoder Tool, we got this plaintext. It still contain both numbers and characters so we will continue decode



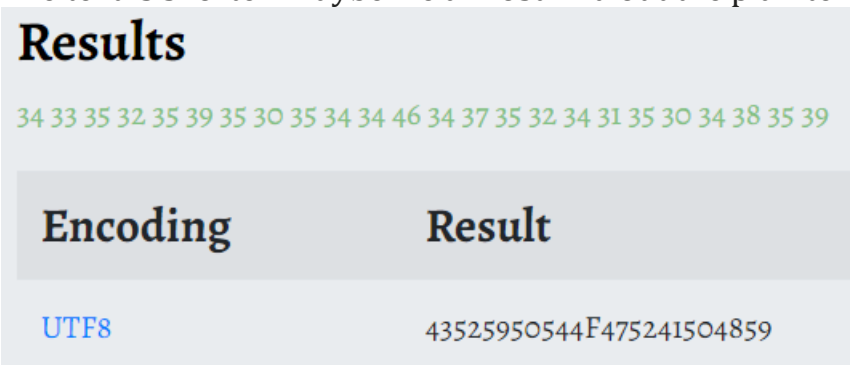
3. We got full of numbers now so I think about Hexadecimal decoder



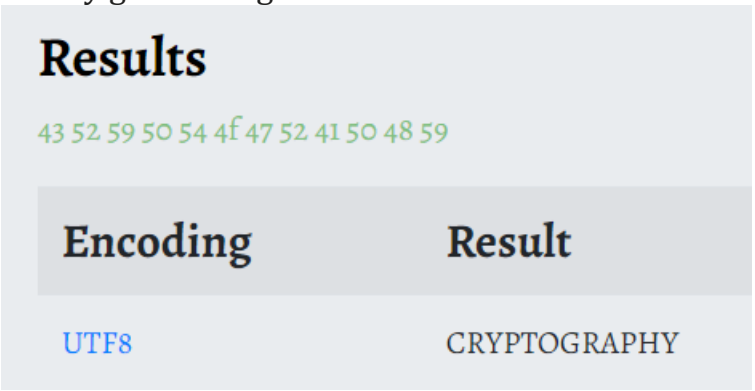
4. Keep decoding with Hexadecimal decoder



5. The text is shorter. Maybe we almost find out the plaintext



6. Finally got the flag CRYPTOGRAPHY !



b. Hill Cipher

Hill Cipher is a polygraphic substitution cipher. Each letter is represented by a number modulo 26. To encrypt a text, each block of n letters (n-component vector) is multiplied by an invertible n x n matrix, agains modulus 26. To decrypt a text, each block is multiplied by the inverse of the matrix used for encryption. This matrix a the cipher key.

Assume that all the alphabets are in upper case and we have an 3x3 matrix key. Below is the example code for the encryption and decryption

```
#Initial key matrix
keyMatrix = [[0] * 3 for i in range(3)]

# Generate vector for the plain text
messageVector = [[0] for i in range(3)]

# Generate vector for the cipher text
cipherMatrix = [[0] for i in range(3)]

# Function: Generates the key matrix for the key string
def getKeyMatrix(key):
    k = 0
    for i in range(3):
        for j in range(3):
            keyMatrix[i][j] = ord(key[k]) % 65
            k += 1

# Function: Encrypt the message
def encrypt(messageVector):
    for i in range(3):
        for j in range(1):
            cipherMatrix[i][j] = 0
            for x in range(3):
                cipherMatrix[i][j] += (keyMatrix[i][x] *messageVector[x][j])
            cipherMatrix[i][j] = cipherMatrix[i][j] % 26

# Function:
def HillCipher(message, key):

    # Get key matrix from the key string
    getKeyMatrix(key)

    # Generate vector for the plain text
    for i in range(3):
        messageVector[i][0] = ord(message[i]) % 65

    # Generate the encrypted vector
    encrypt(messageVector)

    # Generate the encrypted text from the encrypted vector
    CipherText = []
    for i in range(3):
        CipherText.append(chr(cipherMatrix[i][0] + 65))

    # Print the ciphertext
```

```
print("Ciphertext: ", "".join(CipherText))
```

Advance Task 1:

We will count all the characters and have the table below

8	33
;	26
4	19
‡ ,)	16
*	13
5	12
6	11
† , 1	8
0	6
9 , 2	5
: , 3	4
?	3
¶	2
- , .	1

The most frequently occurs is e. In English, ‘the’ is the most usual words. We find no less than 7 arrangements, it is ‘;48’. We may assume that the ‘;’ is ‘t’ and the ‘4’ is ‘h’.

Next, we will see if ‘‡’ is ‘a’ or ‘o’. We can find many ‘‡‡’, so it is ‘o’.

53oo†305))6*the26)ho.)ho)te06*the†e¶60))e5t1o(t:o*e†e3(ee)
5*†th6(tee*96*?te)*o(the5)t5*†2:*o(th956*2(5*-h)e¶e*th0692
e5)t)6†e)hoot1(o9the0e1te:eo1the†e5th)he5†52ee06*e1(o9the
t(eeth(o?3hthe)hot161t:1eeto?t

Next is ‘)’ as we can see the selected phrase, it can not be the vowel etheir ‘a’ nor ‘i’. So maybe it is ‘s’

We can see ‘5’ frequently and it is at the begin of the paragraph so it is ‘a’

We got 2 vowel left: ‘i’ and ‘u’. But the frequent of ‘i’ is much higher than ‘u’ so ‘6’ is ‘i’

a3oo†30assi*the2isho.shoste0i*the†e¶i0sseat1o(t:o*e†e3(ees a*†thi(tee*9i*?tes*o(theasta*†2:*o(th9ai*2(a*-hse¶e*th0i92 eastsi†eshoot1(o9the0e1te:eo1the†eathshea†a2ee0i*e1(o9the t(eeth(o?3htheshot1i1t:1eeto?t

'?' is a vowel and only appear 3 times so it is 'u'

:1i1t:1eet

This layout of word is not much. So we can assume '1' is 'f' and ':' is 'y'

t(eeth

This layout can't be any word so it will be 't(ee' so '(' will be 'r'

:throu3

With this layout we can assume that '3' is 'g'

:fro9the

With this layout we can assume that '9' is 'm'

ithe0efteye

With this layout we can assume that '0' is 'l'

agoo†glass

We can assume '†' is 'd' for a meaningful phrase

agoodglassi*the

So ‘*’ is ‘n’

With this layout ‘2’ is ‘b’

With this layout ‘-’ is ‘c’

With this layout ‘.’ is ‘p’

And with this we can finish the decryption with ‘v’ for ‘¶’

agoodglassinthebishopshostelinthedevilsseatfortyonedegrees andthirteenminutesnortheastandbynorthmainbranchseventhli mb
eastsideshootfromthelefteyeofthedeathsheadabeelinefromthe treethroughtheshotfiftyfeetout