F20FO Lab 5

Anti-Forensics & Cryptography

Chandrashekhar R (cr2007)

Contents

Lab 5.1: Symmetric Key Encryption

Shift Cipher

Decrypt the following substitution Cipher, identify the key used, and show both the key and plaintext.

Kbtp fp fkclojxqflk xylrq zroobkq bsbkqp

Plaintext: News is information about current events

Key: 23 (-3)

What does "CAESAR" become with a shift of 6?

"**CAESAR**" with a shift of 6 becomes "**IGKYGX**"

What key do we need to make "CAESAR" become "MKOCKB"?

Key: 10

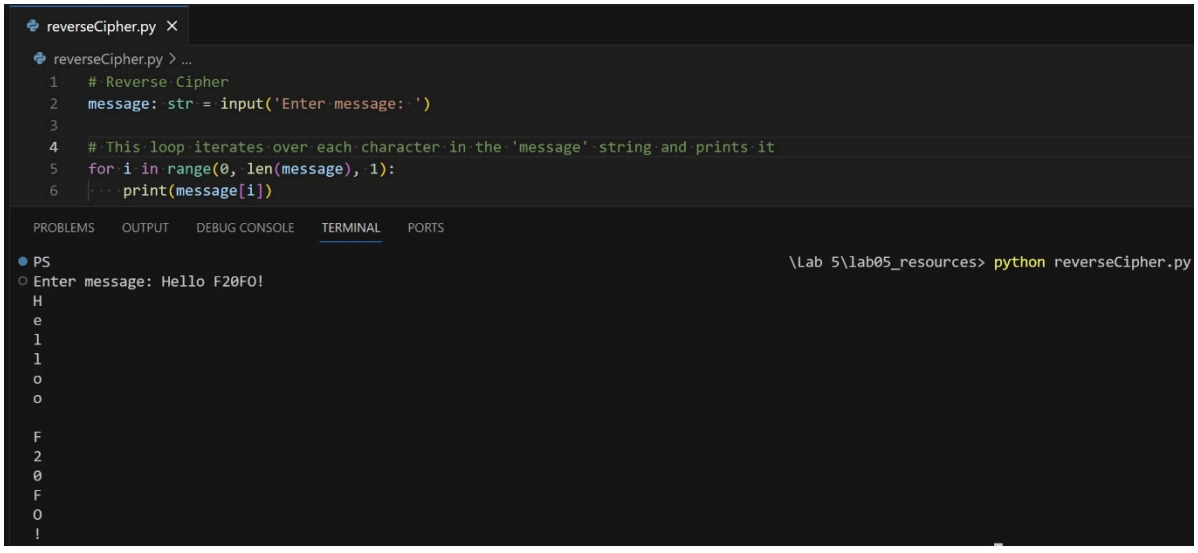
Plain	C	D	E	H	I	N	P	R	S	T	Y
Cipher	X	J	L	A	Z	E	V	K	H	O	M

Given the ciphertext JLXKMVO OAZH, using the above table identify the plaintext.

DECRYPT THIS

Python – Reverse Printing

Upload a screenshot of your code and output



This is a really simple code that simply prints a string backwards - does this offer any security?

This code is not considered a secure method of encryption. It's a very simple transformation that can be easily reversed and doesn't have any sort of key.

It doesn't have any level of confidentiality, integrity, and authenticity that any decent secure encryption algorithm should provide.

Python – Substitution Cipher

It is currently set to be the Caesar Cipher, encrypt only with a shift of 3. Can you modify the code so that it asks the user:

- Whether they want to encrypt or decrypt the message?
- Which key they wish to use?

Upload a screenshot of the (modified) code and output)

```python
import string

# Caesar Cipher
# the string to be encrypted/decrypted

try:
    step: int = int(input("Do you want to encrypt or decrypt the message?:\n\n",
                          "1. Encrypt\n2. Decrypt\n\n",
                          "Enter the number of your choice: "))
    while step not in [1, 2]:
        print("Invalid choice. Please enter 1 or 2.")
        step = int(input("Do you want to encrypt or decrypt the message?:\n\n",
                         "1. Encrypt\n2. Decrypt\n\n",
                         "Enter the number of your choice: "))
except KeyboardInterrupt:
    print("\n\nKeyboard Interrupt. Exiting the program.")
    print("Have a nice day!")
    exit()


try:
    message: str = input(f"Enter the secret message to {"encrypt" if step == 1 else "decrypt"}: ")

    key: int = int(input('Enter the key number (1-26): '))
    while key not in range(1, 27):
        print('Invalid key number. Please enter a number between 1 and 26.')
        key: int = int(input('Enter the key number (1-26): '))
except KeyboardInterrupt:
    print("\n\nKeyboard Interrupt. Exiting the program.")
    print("Have a nice day!")
    exit()

# every possible symbol that can be encrypted
LETTERS = string.ascii_uppercase

# stores the encrypted/decrypted form of the message
translated: str = ''

# capitalize the string in message
message: str = message.upper()

# run the encryption code on each symbol in the message string
for symbol in message:
    if symbol in LETTERS:
        # get the encrypted number for this symbol
        num: int = LETTERS.find(symbol) # get the number of the symbol

        num = num + key if step == 1 else num - key

        # handle the wrap-around if num is larger than the length of
        # LETTERS or less than 0
        if num >= len(LETTERS):
            num = num - len(LETTERS)
        elif num < 0:
            num = num + len(LETTERS)

        # add encrypted/decrypted number's symbol at the end of translated
        translated = translated + LETTERS[num]
    else:
        # just add the symbol without encrypting/decrypting
        translated = translated + symbol

# print the encrypted/decrypted string to the screen
print(translated)
```

```
PS C:\Users\
\Labs\Lab 5\lab05_resources> python caesarCipher.py
Do you want to encrypt or decrypt the message:

1. Encrypt
2. Decrypt

Enter the number of your choice: 1
Enter the secret message to encrypt: Know how to use enemies for your own profit.
Enter the key number (1-26): 8
SVWE PWE BW CAM MVMUQMA NWZ GWCZ WEV XZWNQB.
PS C:\Users\
\Labs\Lab 5\lab05_resources> python caesarCipher.py
Do you want to encrypt or decrypt the message:

1. Encrypt
2. Decrypt

Enter the number of your choice: 2
Enter the secret message to decrypt: SVWE PWE BW CAM MVMUQMA NWZ GWCZ WEV XZWNQB.
Enter the key number (1-26): 8
KNOW HOW TO USE ENEMIES FOR YOUR OWN PROFIT.
```

Frequency Analysis

Review the following ciphertext and use frequency analysis to crack it - this is a trial and error process and will take you some time, depending how good you are with puzzles!

VEP HYXHLVHTP MO AWFJYFLT H RFNEPS HJNEHAPV FL VEFU ZHC FU VEHV FV FU PHUC VM KPKMSFUP VEP IPCZMSY MS IPCNESHUP, HLY EPLRP VEP RFNEPS HJNEHAPV. VEFU FU FKNMSVHLV, APRHWUP FO VEP UPLYPS EHU VM IPPN VEP RFNEPS HJNEHAPV ML H NFPRP MO NHNPS, VEP PLPKC RHL RHNVWSP VEP NHNPS, YFURMXPS VEP IPC, HLY SPHY HLC RMKKWLFRHVFMLU VEHV EHXP APPL PLRSCNVPY ZFVE FV. EMZPXPS FO VEP IPC RHL AP RMKKFVVPY VM KPKMSC FV FU JPUU JFIPJC VM OHJJ FLVM PLPKC EHLYU.

You need to start by counting the frequency of the letters and enter them into this table.

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**

Then compare these values against the second table (which is the expected frequency of letters within English), the most frequent letters in each should be a straight swap - the more text you have to look at the more accurate these straight swaps become. The remaining swaps are educated guesses.

a(B)	b	c(Y)	d	e(H)	F(i)	g	h(A)	i(K)	j(L)	k(M)	l(N)	m(O)
7	0	12	0	26	27	0	32	6	9	11	20	18
n(P)	**o(N)**	**p(E)**	**q**	**r(C)**	**s(R)**	**t(G)**	**u(S)**	**v(T)**	**w(U)**	**x(V)**	**y(D)**	**z(W)**
16	5	55	0	14	17	2	17	35	4	4	11	4

```
the advantage on building a cipher alphabet in this way is that it is easy to
memorise the keyword or keyphrase, and hence the cipher alphabet. this is important,
because in the sender has to keep the cipher alphabet on a piece on paper, the enemy
can capture the paper, discover the key, and read any communications that have been
encrypted with it. however in the key can be committed to memory it is less likely to
fall into enemy hands.
```

Vigenère Cipher

See if you can decrypt the following message that has been encrypted using the Vigenère cipher: `Mjxa xl Xxotgggm Rbrwmg`. The passphrase (keyword) used was `TCPIP`.

Key	T	C	P	I	P	T	C	P	I	P	T	C	P	I	P	T	C	P	I	P
Ciphertext	M	J	X	A	X	L	X	X	O	T	G	G	G	M	R	B	R	W	M	G
Plaintext	T	H	I	S	I	S	V	I	G	E	N	E	R	E	C	I	P	H	E	R

This is Vigenère Cipher.

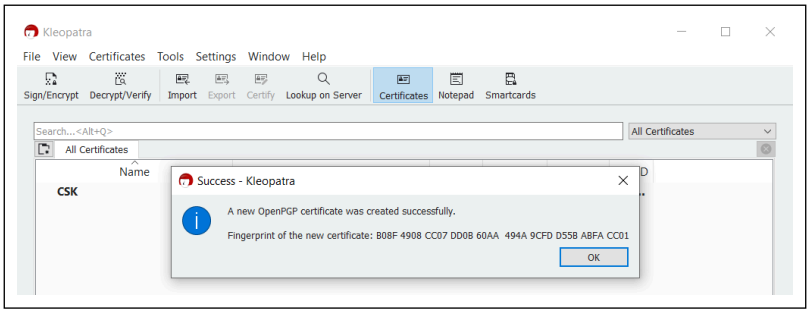
What are the security advantages of the Vigenère Cipher over a simple substitution cipher?

Vigenère Cipher has a major security advantage over a simple substitution cipher. Due to its polyalphabetic nature, i.e. using multiple substitution alphabets, it makes frequency analysis a lot more challenging. Since a Vigenère Cipher requires a keyword to encrypt and decrypt the message, if a keyword is long enough and chosen in random, it can significantly increase the complexity of breaking the cipher command to a simple substitution cipher.

And since there are 26 possible ways to shift the position of the keyword, it makes a lot more secure than a substitution cipher, which has only one fixed substitution alphabet.

Lab 5.2: Asymmetric Encryption

GNU Privacy Guard (GPG)



What happens? What have you just achieved?

Upon decryption using my private key, I successfully accessed the contents of the encrypted file, originally encrypted with my colleague's private key, and transmitted securely. This achievement underscores the utilization of secure communication protocols, ensuring the safe exchange of sensitive information.

Null Cipher

Can you work out the null cipher message? It uses a fixed point in each word.

The **h**airy **e**lephant, **c**ame **a**nd **t**ook **s**alt **a**nd **t**ea **o**ver **n**ear **t**he **h**azardous **e**nergy **m**aking **a**pparatus **t**oday.

The cat sat on the mat.

Word Shifting

Can you work out the shifted message below?

```
One reason people lie is  to  achieve personal power. Achieving personal  power is
helpful for someone who pretends to be more confident than he really is. For example,
one of my friends threw a party at his house last month. He asked me to come to his
party and bring a date. However, I didn't have a girlfriend. One of my other friends,
who had a date to go to the party with, asked me about my date. I didn't want to be
embarrassed, so I claimed that I had a lot of work to do. I said I could easily find
a date even better than his if I wanted to. I also told him that his date was ugly. I
achieved power to help me feel  confident; however, I embarrassed my friend and his
date. Although this  lie helped me at the time, since then it has made me look down
on myself.
```

To achieve power find a confident friend lie.

Lab 5.3: Password Cracking

Dictionary Attack

Generate an MD5 hash and try to crack one or more passwords. Upload screenshots of your MD5 hash and John output for the cracked(?) password(s).