COSC 3371 HW1
Professor Dr. Huang
Maximillian Chalitsios
1808500

This homework had three parts. In part 1 we were to create a frequency table for the ciphertext displayed below:

Letter	Frequency
Q	97
H	68
J	63
V	53
N	51
W	47
O	43
X	43
D	34
F	32
M	29
K	26
G	23
U	15
T	15
Y	14
R	13
L	12
I	12
Z	10
A	8
E	4
S	2
B	1
C	1
P	1

COSC 3371 HW1
Professor Dr. Huang
Maximillian Chalitsios
1808500

The process of the decryption strategy is as follows: To first create a frequency table of the ciphertext and relate those frequencies to common typical frequencies provided. The frequencies did not match entirely but were very close. A key was gathered based on mapping the ciphertext letters to a plaintext letter as follows:

Key:

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

COSC 3371 HW1
Professor Dr. Huang
Maximillian Chalitsios
1808500

The function problem1() ran a loop to help the user decrypt the ciphertext letter by letter and output the plaintext into a problem1.txt file. After decrypting, the plaintext reads as follows:

```
-----------------------------
Decrypted message:
-----------------------------
URGENT MESSAGE: I BELIEVE THAT DR. ON IS A MEMBER OF A SECRET CRIME
ORGANIZATION CALLED P.H.A.N.T.O.M., WHOSE GOAL IS TOTAL WORLD DOMINATION.
THEIR PLAN IS TO ACQUIRE A SUPERWEAPON AND TO HOLD THE WORLD RANSOM. I
AM AFRAID THAT WE DO NOT HAVE MUCH TIME BEFORE THEY SUCCEED.
I HAVE RECENTLY INTERCEPTED AN ENCRYPTED MESSAGE (ATTACHMENT
CIPHER2.TXT) THAT WAS SENT BY DR. ON TO ONE OF HIS CONSPIRATORS, THE
INFAMOUS MR. BLOWFIELD. I MANAGED TO DISCOVER THAT THE MESSAGE WAS
ENCRYPTED USING THE JACKAL CIPHER (SEE SOURCE CODE), BUT I WAS NOT ABLE
DISCOVER THE SECRET KEY, AND THE CIPHER SEEMS TO BE UNBREAKABLE. I AM
AFRAID THAT DECRYPTING THIS MESSAGE IS THE ONLY WAY TO STOP DR. ON'S
ORGANIZATION.
PLEASE SEND REINFORCEMENTS IMMEDIATELY! I TRIED TO ACT CAUTIOUSLY, BUT I
HAVE A FEELING THAT DR. ON'S HENCHMEN ARE ONTO ME. I DON'T KNOW HOW LONG
I HAVE BEFORE THEY DISCOVER MY REAL IDENTITY AND MY SECRET HIDING PLA
```

Then for problem 2 brute force, a jackal_decrypt(i,j,cipherText) function was given to decrypt. The method of decryption was brute force by checking each pair of (i, j) along with the cipherText. The key pair i=127 and j=127 was the one that decrypted the ciphertext giving us the message below:

Mr. Blowfield, my associate will deliver the payment to you next Friday at noon. The location of the exchange is 20.893360, -156.438838. I expect you to deliver the plans for the super-weapon in exchange. Do not dare to fail me. You should encrypt the plans with one-time-pad to prevent anyone from stealing them. Use the following 11 byte values as the key: {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31} . If the plaintext is longer, then just repeat the key as many times as necessary.

For problem 3 we use the One-Time Pad approach to decrypt the third ciphertext3.txt with the key given from problem 2’s plaintext. We use the binary XOR operator to achieve this. The decrypted message is as follows when using key and the one time pad:

"Dr. On, I will deliver the plans personally to your secret underwater base at 30.395871, -46.471452 on September 15 at midnight."

COSC 3371 HW1
Professor Dr. Huang
Maximillian Chalitsios
1808500

After discovering the location of Dr. On's underwater base, you are finally ready to defeat him. Soon, P.H.A.N.T.O.M. will fall. You hop into your supersonic submarine and set course for Dr. On's secret lair. It is time for him to learn the name Vond. James Vond.