COMP3355
Assignment 1

Silvan Adrian

September 23, 2019

1 Q1

```
ftqdq uezae gotft uzsme msdqm ffmxq zfiuf tagfs dqmfi uxxba iqd
```

1.1 What is the substitution being used in the above cipher?

Caesar cipher so by shifting each character by an amount of characters. For analyzing I used the `TryAllTranslators` which then goes through every shift until the Text makes some sense.

By doing so I ended up on the following mapping:

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

```
q=e
r=f
s=g
t=h
u=i
v=j
w=k
x=l
y=m
z=n
```

1.2 Recover the cipher text into plain text.

By then using the `Translator` and the above mentioned mapping I end up on the decrypted text:

```
ciphertext:
ftqdq uezae gotft uzsme msdqm ffmxq zfiuf tagfs dqmfi uxxba
iqd

plaintext :
there isnos uchth ingas agrea ttale ntwit houtg reatw illpo wer
```

So by writing it out nicely (right spacing):

```
there is no such thing as a great talent without great willpower
```

2 Q2

2.1 What is the inverse permutation (decryption key)?

We can get the inverse of the permutation just by placing each of the characters back on it's location, so we end up with the following:

```
ssthiiht
64123587
thisisth
```

2.2 Decrypt the cipher text into plain text.

If we repeat on doing this over and over until the end of the text, we get the decrypted text:

```
ssthiihttrefissaensigmtncuoforbyueerscirrotycues
64123587641235876412358764123587641235876412358764123587
thisisthefirstassignmentofourcybersecuritycourse
```

3 Q3

Ok we have the following information:

$$K_0 = 1A5D6D895B4B66DB \tag{1}$$
$$input = A7E2BC3FD4C896D2 \tag{2}$$

So we now take the input and convert it to binary (64 bits long):

```
A7E2BC3FD4C896D2
1010011111100010101111000011111111010100110010001001011011010010
```

Here we have the in put permutation, so let's input our bits:

```
58 50 42 34 26 18 10 2
60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6
64 56 48 40 32 24 16 8
57 49 41 33 25 17 9  1
59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5
63 55 47 39 31 23 15 7
```

```
1 0 1 1 0 0 1 0
1 1 0 1 1 1 0 0
0 1 0 1 1 1 0 1
0 0 0 0 1 0 0 1
1 1 1 1 0 1 1 1
0 0 0 0 1 1 1 1
```

```
0 0 1 0 1 1 0 0
1 1 0 0 1 0 1 1
```

By splitting it up we get L_0:

```
1 0 1 1
1 1 0 1
0 1 0 1
0 0 0 0
1 1 1 1
0 0 0 0
0 0 1 0
1 1 0 0
```

R_0:

```
0 0 1 0
1 1 0 0
1 1 0 1
1 0 0 1
0 1 1 1
1 1 1 1
1 1 0 0
1 0 1 1
```

R_0 and L_0 then get switched for round 1, so that we get for $L_1 = R_0$:

```
0 0 1 0
1 1 0 0
1 1 0 1
1 0 0 1
0 1 1 1
1 1 1 1
1 1 0 0
1 0 1 1
```

For key we have in bits:

```
1A5D6D895B4B66DB
0001101001011101011011011000100101011011010010110110011011011011
```

Then run Permutated Choice 1:

```
1 0 0 0 1 0 0
0 1 1 1 1 0 1
1 0 0 1 0 0 0
1 0 0 1 0 0 1
1 1 1 1 0 0 0
1 0 1 0 0 0 1
1 0 1 0 1 1 1
1 1 1 0 0 1 1
```

That key we split up in 2 halves and shift 1 bit:

```
1 0 0 0 1 0 0
0 1 1 1 1 0 1
1 0 0 1 0 0 0
1 0 0 1 0 0 1

1 1 1 1 0 0 0
1 0 1 0 0 0 1
1 0 1 0 1 1 1
1 1 1 0 0 1 1


after shift:
0 0 0 1 0 0 0
1 1 1 1 0 1 1
0 0 1 0 0 0 1
0 0 1 0 0 1 1

1 1 1 0 0 0 1
0 1 0 0 0 1 1
0 1 0 1 1 1 1
1 1 0 0 1 1 1
```

After the shift we take the permutation choice 2:

```
1 1 1 1 1 0 0 0 1
0 0 1 1 0 0 0 0 1
0 1 0 0 1 0 1 1
1 0 1 1 1 1 1 0
1 0 0 1 1 1 0 1
0 0 1 1 1 0 1 0
```

This Key we then need to xor with the Expanded input R_1, here is the expanded input:

```
1 0 0 1 0 1
0 1 1 0 0 1
0 1 1 0 1 1
1 1 0 0 1 0
1 0 1 1 1 1
1 1 1 1 1 1
1 1 1 0 0 1
0 1 0 1 1 0
```

After Xor of key and R_1:

```
011001001010011110111001000000010110001101101100
```

Now we need to use the S-Boxes substitute:

```
011001 -> 1 / 9 in S1
001010 -> 0 / 5 in S2
011110 -> 0 / 15 in S3
111001 -> 3 / 12 in S4
000000 -> 0 / 0 in S5
010110 -> 0 / 11 in S6
001101 -> 1 / 6 in S7
101100 -> 2 / 6 in S8
```

After we read out all the number from the S-Boxes:

```
0110 -> 6
1011 -> 11
```

```
1000 -> 8
1100 -> 12
0010 -> 2
0100 -> 4
0001 -> 1
1110 -> 14
```

After that xor it with L_1 and we end up on R_1:

```
xor:
01101011100011000010010000011110
00101100110110010111111111001011
```

Then we get R_1:

```
0 1 0 0
0 1 1 1
0 1 0 1
0 1 0 1
0 1 0 1
1 0 1 1
1 1 0 1
0 1 0 1
```

So we end up having both R_1 and L_1.

4 Q4

4.1 What type of cipher is it? (Monoalphabetic / Polyalphabetic)

It's a Polyalphabetic cipher, I did the test by using the `TryAllTranslator` which didn't end up with a proper solution. And by using the `Analyzer` from which we can see the Index of coincidence which shows us that it was actually encrypted by using a Polyalphabetic cipher.

4.2 Give the permutation(s) (if any) or the substitution(s) used in the cipher.

As a key length 7 got used and for encryption with vigenere the key "rosebud" got used, as from the Movie Citizen Kane.

4.3 Recover the cipher text into plain text.

We start by analyzing the cipher text by using the `Analyzer` from which we get the longest repeated sequence:

```
--- 12-grams counting ------------
evmwiodmbbdj 2 position=459,746
```

Then 746-459 = 287 and get the factor:

```
Factor of 287 include:
7 41 287
```

I will go for the factor 7 since it's the smallest one which makes the most sense. So we expect the key length to be 7.

From here on we need to find the 7 characters with which the cipertext has been encrypted, I ended up on the following sequence (with support of the Kasiski method) and guessing:

```
java PolyTranslator ../q4.txt  7 RR.txt OO.txt SS.txt EE.txt
↪  BB.txt UU.txt DD.txt
```

Which then gives me the following decrypted text:

```
overr ecent decad esaus trali asfor eignr elati onsha vebee
ndriv enbya close assoc iatio nwith theun iteds tates throu
ghthe anzus pacta ndbya desir etode velop relat ionsh ipswi
thasi aandt hepac ificp artic ularl ythro ughas eanan dthep
acifi cisla ndsfo rumth reeye arsag oaust ralia secur edani
naugu ralse atatt heeas tasia summi tfoll owing itsac cessi
ontot hetre atyof amity andco opera tiona ustra liais amemb
eroft hecom monwe altho fnati onsin which theco mmonw ealth
heads ofgov ernme ntmee tings provi dethe mainf orumf orcoo
perat ionau stral iahas energ etica llypu rsued theca useof
inter natio naltr adeli beral isati onaus trali aledt hefor
matio nofth ecair nsgro upand asiap acifi cecon omicc ooper
ation itisa membe rofth eorga nisat ionfo recon omicc ooper
ation andde velop menta ndthe world trade organ izati onthe
reare sever almaj orbil atera lfree trade agree ments austr
```

```
aliah aspur suedm ostre centl ythea ustra liaun iteds tates
freet radea greem entan dclos ereco nomic relat ionsw ithne
wzeal andaf oundi ngmem berco untry ofthe unite dnati onsau
stral iaals omain tains anint ernat ional aidpr ogram under
which somes ixtyc ountr iesre ceive assis tance thebu dgetp
rovid esove rtwoa ndaha lfbil lionf ordev elopm entas sista
nceas aperc entag eofgd pthis contr ibuti onisl esssth antha
tofth eunmi llenn iumde velop mentg oals
```
