Birzeit University

Faculty of Engineering and Technology

Department of Electrical and Computer Engineering

First Semester – 2023/2024

ENCS4320 - Applied Cryptography

Homework # 1

Prepared by: Dana Bornata.

ID: 1200284

Instructor Dr. Mohammed S. Hussein

Date :8/12/2023

Section #2

Q1:

Since we only have the cyphertext and we want to know the key and the plaintext

There are two ways to identify them: The first way is to find the most frequent letter in the sentence (we know that the most frequent letter is E): So, we know the amount of displacement between the repeated letter and the letter E, and we try to move the sentence according to ironing. If the resulting sentence is understandable, it is very likely that we have arrived at the solution.

If the answer is not understood in the sentence: We work on the other method, which is to try the shift from 1 to 26, and the resulting clear sentence is the plaintext and the key.

The highest recurring letter is the H >>>The space between H and E = 3

So, the Key=3;

$M=(C-K)\%26$

	#		Rot-K
I	2	(8-3)%26	F
U	3	(20-3)%26	R
R	2	(17-3)%26	O
P	2	(15-3)%26	M
W	4	(22-3)%26	T
K	2	(10-3)%26	H
H	9	(7-3)%26	E
L	3	(11-3)%26	I

	#		ROT-K
Y	1	(24-3)%26	V
V	1	(21-3)%26	S
D	2	(3-3)%26	A
O	3	(14-3)%26	L
Z	1	(25-3)%26	W
Q	1	(16-3)%26	N
E	1	(4-3)%26	B
U	3	(20-3)%26	R
S	1	(18-3)%26	P

PlainText is :

From The River To The Sea Palestine Will Be Free.

بإذن الله

الاسم عبلة [illegible]

Q2:

Q2:

$\boxed{1}$ number of possible Keys $= 2^{56}$

Test $\Rightarrow 4.2 \times 16 \times 10^9$ per second

$$\text{Time in year} = \frac{\dfrac{\text{number possible key}}{\text{Key Test per second}}}{60 \times 60 \times 24 \times 365}$$

$$= \frac{\dfrac{2^{56}}{4.2 \times 10^9 \times 16}}{60 \times 60 \times 24 \times 365}$$

≈ 34 years

$\boxed{2}$ number of possible Key $= 2^{128}$

$$\text{Time in year} = \frac{\dfrac{2^{128}}{4.2 \times 16 \times 10^9}}{60 \times 60 \times 24 \times 365}$$

$\approx 1.6 \times 10^9$ years

These results show that significantly increasing the key size enhances the security of the system against brute force attack, which is one of the main ways to improve the security of a cryptography-based system.

Q3:

In order for the OTP to be completely confidential, the length of the KEY must be greater than or equal to the length of the MESSAGE

K=M=C={0,1}^n

If we apply the optimization according to Alice's suggestion, that is, if you remove the keys with all zeros from the key space, we have created an encryption that cannot show complete secrecy because the length of the key is one less than the length of the key, and this breaks the O T P conditions.

Therefore, this improvement completely breaks the confidentiality, making this modified password worse than the original.

Q4:

Q4 :

a) $(23+28) \bmod 29$

$= (23 \bmod 29 + 28 \bmod 29) \bmod 29$

$= (23 + 28) \bmod 29$

$= 51 \bmod 29$

$= 22$

$51 = 29q + R$

$51 = 29 \times 1 + R$

$R = 22$

b) $(3 - 11) \bmod 9$

$= (3 \bmod 9 - 11 \bmod 9) \bmod 9$

$= (3 + 7) \bmod 9$

$= 1$

$-11 \bmod 9$

$\Rightarrow -11 = 9 \times -2 + R$

$R = 7$

$10 \bmod 9$

$10 = 9 \times 1 + R$

$R = 1$

(c) $15 \times 29 \pmod{13}$

$= (15 \bmod 13 \times 29 \bmod 13) \bmod 13$

$= (2 \times 3) \bmod 13$

$= 6$

$15 \bmod 13$

$15 = 13 \times 1 + R$

$R = 2$

$29 \bmod 13$

$29 = 13 \times 2 + R$

$R = 3$

(d) $16 \times 13 \pmod{26}$

$= (16 \bmod 26 \times 13 \bmod 26) \bmod 26$

$= (16 \times 13) \bmod 26$

$= 208 \bmod 26$

$= 0$

$208 = 26 \times 8 + 0$

$R = 0$

(e) $2^5 \bmod 31$

$32 = 31q + R$

$\boxed{R = 1}$

f) $2^{103} \bmod 31$

$(2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times$
$2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^5 \times 2^3)$
$\times \bmod 31$

$= ((\underbrace{1 \times \dots \times 1}_{20}) \times 2^3 \bmod 31) \bmod 31$

$= (1 \times 8) \bmod 31$

$= 8$

Q5:

Q5 : $C \oplus M = K$

(a) plaintext = thirst
= 111 011 010 101 110 111

ciphertext = KITLKE
= 011 010 111 100 011 000

Key = $C \oplus M$
= 100 001 101 001 101 111
= Lhrhrt

(b) plaintext = hikers
= 001 010 011 000 101 110

Key = $C \oplus M$
= 010 000 100 100 110 110
= iellss

Q6:

Q: 6:

a) No, it doesn't work with either OR or And.

* in And For example if message and Key one bit.

m	K	m ∧ K	
0	0	0	m or K
0	1	0	m
1	0	0	K
1	1	1	m or Key

في مرحلة ال Dec لا يوجد شيء يحدد متى يكون الاوتبوت المسج ومتى الكي

So Security is also broken.

- وايضاً عندما يكون الاوتبوت واحد يعرف الشخص انه Key and message الاثنين واحد.

* also in OR

m	K	m ∨ K	
0	0	0	m or K
0	1	1	K
1	0	1	m
1	1	1	m or K

لا يمكن الحصول على Dec لانه لا يوجد شيء يؤدي الى التمييز بين m/k

ايضاً عندما يكون الجواب صفر معروف ان كلاً من المسج والكي صفر.

b) No, this does not have the security guarantees of a one-time pad

K	m	E(K,M)
00	00	00
01	00	01
10	00	10
00	01	01
01	01	00
10	01	11
00	10	10
01	10	11
10	10	00

* نلاحظ هنا انه عندما يكون ال E(K,M) = 11
يكون دائماً الـ ج ليس صفر وهذا يعطي
معلومة عندما يرى ال cipher attack

So $pr[M=m] \neq Pr[M=m / C=c]$

So this not perfect security

(c) To solve problem in b we need an encryption Algorithm That ensures equal probability for each possible outcome. example we need output cipher just {0,1,2} becouse has an equal probability of occurring. and this meeting the requirements of perfect secrecy.

So $E^*(K,M) = M + K \mod 3$

K	M	$E^*(K,M)$
00	00	00
01	00	01
10	00	10
00	01	01
01	01	10
10	01	00
00	10	10
01	10	00
10	10	01

$$pr[M=m] = pr[M=m / C=c]$$

$$pr(b' = b) = \frac{1}{2}$$

Q7:

Shift cipher:

for a shift cipher with a standard English alphabet of 26 letters, the key space (number of possible keys) is 2^26 because there are 26 possible shift values, the encryption of a character m ∈ {0, 1, . . . 25} is c = m + k mod 26 for some k ∈ {0, 1, . . . 25}. Accordingly, and the key k = c − m mod 26.

Substitution cipher

It is better than shift cipher , but It can be hacked by using frequency /analysis to determine the most frequently used letters in the target language , There may be recurring patterns in the ciphertexts that can be detected

Vigenère ciphers

To execute a chosen-plaintext attack on the Vigenère cipher, it's crucial to acquire a ciphertext generated from a message with a length equal to the key length (t). Subsequently, the analysis is performed position-wise, treating each position as an independent Caesar cipher. The comparison of known plaintext and corresponding ciphertext at each position allows for the determination of the shift value for that part of the key.

The success of the attack is contingent upon the length and randomness of the key. A longer, more random key enhances the cipher's resistance to decryption, requiring a substantial amount of chosen plaintext to accurately deduce the key and compromise the encryption.

If we compare them

Shift coding:

Strengths: Simple and easy to understand.

Weaknesses: Vulnerable to brute force attacks due to limited key space. Not suitable for high security applications.

Alternative encryption:

Strengths: Provides better security than base shift encryption. It can resist simple frequency analysis.

Weaknesses: Still vulnerable to more advanced frequency analysis and pattern recognition.

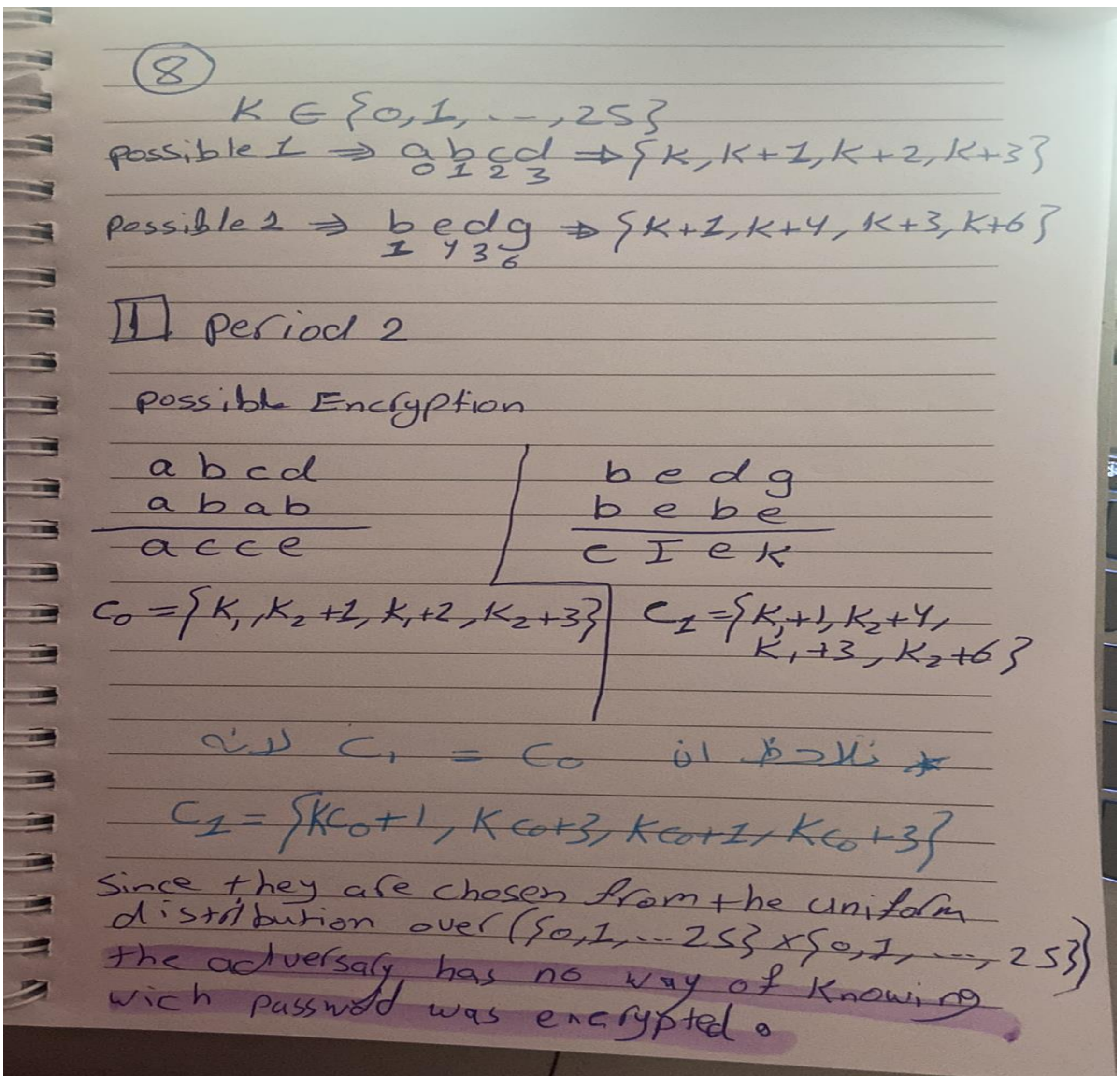
Vigenère encryption:

Strengths: Improved security compared to conversion and replacement ciphers. Using the keyword provides contrast.

Weaknesses: Vulnerable to plaintext attacks, especially with shorter, less random keys. Longer keys increase security but also complexity.

Q8:

When period of 2 or 4, determining the password is not possible due to the equal likelihood of keys.



8

$K \in \{0, 1, \ldots, 25\}$

possible 1 $\Rightarrow$ abcd (0 1 2 3) $\Rightarrow \{K, K+1, K+2, K+3\}$

possible 2 $\Rightarrow$ bedg (1 4 3 6) $\Rightarrow \{K+1, K+4, K+3, K+6\}$

1 period 2

possible Encryption

abcd	bedg
abab	bebe
acce	cIek

$C_0 = \{K_1, K_2+1, K_1+2, K_2+3\}$ | $C_1 = \{K_1+1, K_2+4, K_1+3, K_2+6\}$

* نلاحظ ان $C_1 = C_0$ لذلك

$C_1 = \{K_{C_0}+1, K_{C_0}+3, K_{C_0}+1, K_{C_0}+3\}$

Since they are chosen from the uniform distribution over $(\{0,1,\ldots,25\} \times \{0,1,\ldots,25\})$ the adversary has no way of knowing wich password was encrypted.

* period 3:

$$C_0 = \{K_2, K_2+2, K_3+2, K_1+3\}$$

$$\begin{array}{r} abcd \\ abca \\ \hline aced \end{array}$$

$$C_1 = \{K_1+1, K_2+4, K_3+3, K_1+6\}$$

$$\begin{array}{r} bedg \\ bedb \\ \hline cIgH \end{array}$$

These two sets are disjoint due to the relationship between the First and fourth cipher text character

and thus one can deduce the password.

* period 4

$$\begin{array}{r} abcd \\ abcd \\ \hline accg \end{array}$$

With key length the same as the message length, the Vigener One-Time pad this perfectly sercet so cannot be distinguished based on the ciphetext.

$$\begin{array}{r} bedg \\ bedg \\ \hline CI@m \end{array}$$

- Example: **When period of 2 or 4 probability 0.5 and this The attacker does not appreciate discrimination**

1/2

a b c d
a b a b
a c c e

صفر

a b c d
b b b b
b F d H

1

b e d g
a b a b
b F d h

1/2

b e d g
b e b e
c I e K

صفر

~~[illegible]~~

3/4

a b c d
a b c a
a c c d

صفر

a b c d
b e d b
b f d e

2

b e d g
a b c a
b f d g

3/4

b e d g
b e d b
c I e h

صفر

1/2

a b c d
a b c d
a c c g

صفر

a b c d
b e d g
b f d j

٤

1/2

b e d g
a b c d
b f d j

صفر

b e d g
b e d g
c I e m

Key length the same as the message length.
Vigenere cipher → one-Time-pad
So this perfectby secret
because that the two passwords
cannot be distinguished based
on the ciphertext.

Q10:

Results:

The method is through letter ratios, The largest number of letters in a word, the letter is its highest ratio, and so on.

```
Dana Bornata 1200284
 Q10:
Character Counts in the Ciphertext:
Char: R Count: 7
Char: J Count: 9
Char: O Count: 16
Char: G Count: 19
Char: M Count: 4
Char: Y Count: 3
Char: Q Count: 26
Char: H Count: 14
Char: V Count: 15
Char: B Count: 12
Char: W Count: 21
Char: F Count: 37
Char: P Count: 10
Char: D Count: 2
Char: Z Count: 7
Char: K Count: 3
Char: E Count: 4
Char: I Count: 9
Char: C Count: 3
Char: L Count: 17
Char: A Count: 3
Char: S Count: 2
Char: X Count: 1


Char: F Frequency: 0.151639      Expected: E
Char: Q Frequency: 0.106557      Expected: T
```

```
Char: F Frequency: 0.151639     Expected: E
Char: Q Frequency: 0.106557     Expected: T
Char: W Frequency: 0.0860656    Expected: A
Char: G Frequency: 0.0778689    Expected: O
Char: L Frequency: 0.0696721    Expected: I
Char: O Frequency: 0.0655738    Expected: N
Char: V Frequency: 0.0614754    Expected: S
Char: H Frequency: 0.057377     Expected: H
Char: B Frequency: 0.0491803    Expected: R
Char: P Frequency: 0.0409836    Expected: D
Char: J Frequency: 0.0368852    Expected: L
Characters with similar frequencies found:
11. Char: J     Frequency: 0.0368852
12. Char: I     Frequency: 0.0368852
Enter the number of your choice for decryption (or press Enter to use the default): 12
Char: R Frequency: 0.0286885    Expected: U
Characters with similar frequencies found:
13. Char: R     Frequency: 0.0286885
14. Char: Z     Frequency: 0.0286885
Enter the number of your choice for decryption (or press Enter to use the default): 13
Char: M Frequency: 0.0163934    Expected: W
Characters with similar frequencies found:
15. Char: M     Frequency: 0.0163934
16. Char: E     Frequency: 0.0163934
Enter the number of your choice for decryption (or press Enter to use the default): 15
Char: Y Frequency: 0.0122951    Expected: G
```

```
15. Char: M      Frequency: 0.0163934
16. Char: E      Frequency: 0.0163934
Enter the number of your choice for decryption (or press Enter to use the default): 15
Char: Y Frequency: 0.0122951    Expected: G
Characters with similar frequencies found:
17. Char: Y      Frequency: 0.0122951
18. Char: K      Frequency: 0.0122951
19. Char: C      Frequency: 0.0122951
20. Char: A      Frequency: 0.0122951
Enter the number of your choice for decryption (or press Enter to use the default): 20
Char: D Frequency: 0.00819672   Expected: V
Characters with similar frequencies found:
21. Char: D      Frequency: 0.00819672
22. Char: S      Frequency: 0.00819672
Enter the number of your choice for decryption (or press Enter to use the default): 22
Char: X Frequency: 0.00409836   Expected: J
Character Frequencies and Decrypted Letters:
Char: J Frequency: 0.0368852    Decrypted: I
Char: R Frequency: 0.0286885    Decrypted: R
Char: G Frequency: 0.0778689    Decrypted: O
Char: O Frequency: 0.0655738    Decrypted: N
Char: M Frequency: 0.0163934    Decrypted: M
Char: Q Frequency: 0.106557     Decrypted: T
Char: Y Frequency: 0.0122951    Decrypted: A
Char: H Frequency: 0.057377     Decrypted: H
Char: V Frequency: 0.0614754    Decrypted: S
Char: B Frequency: 0.0491803    Decrypted: R
Char: W Frequency: 0.0860656    Decrypted: A
Char: F Frequency: 0.151639     Decrypted: E
Char: P Frequency: 0.0409836    Decrypted: D
```

```
Char: Y Frequency: 0.0122951    Decrypted: A
Char: H Frequency: 0.057377     Decrypted: H
Char: V Frequency: 0.0614754    Decrypted: S
Char: B Frequency: 0.0491803    Decrypted: R
Char: W Frequency: 0.0860656    Decrypted: A
Char: F Frequency: 0.151639     Decrypted: E
Char: P Frequency: 0.0409836    Decrypted: D
Char: D Frequency: 0.00819672   Decrypted: S
Char: Z Frequency: 0.0286885    Decrypted: Z
Char: K Frequency: 0.0122951    Decrypted: K
Char: E Frequency: 0.0163934    Decrypted: E
Char: I Frequency: 0.0368852    Decrypted: I
Char: C Frequency: 0.0122951    Decrypted: C
Char: L Frequency: 0.0696721    Decrypted: I
Char: A Frequency: 0.0122951    Decrypted: A
Char: S Frequency: 0.00819672   Decrypted: S
Char: X Frequency: 0.00409836   Decrypted: J

The ciphertext:
JGRMQOYGHMVBJWRWQFPWHGFFDQGFPFZRKBEEBJIZQQOCIBZKLFAFGQVFZFWWEOGWOPFGFHWOLPHLRLOLFDMFGQWBLWBWQOLKFWBYLBLYLFSFLJGRMQBOLWJV
FPFWQVHQWFFPQOQVFPQOCFPOGFWFJIGFQVHLHLROQVFGWJVFPFOLFHGQVQVFILEOGQILHQFQGIQVVOSFAFGBWQVHQWIJVWJVFPFWHGFIWIHZZRQGBABHZQOC
GFHX

Decrypted Text:
IORMTNAOHMSRIARATEDAHOEESTOEDEZRKREERIIZTTNCIRZKIEAEOTSEZEAAENOANDEOEHANIDHIRINIESMEOTARIARATNIKEARAIRIAIESEIIORMTRNIAIS
EDEATSHTAEEDTNTSEDTNCEDNOEAEIIOETSHIHIRNTSEOAISEDENIEHOTSTSEIIENOTIIHTETOITSSNSEAEORATSHTAIISAISEDEAHOEIAIHZZRTORARHZTNC
OEHJ

C:\Users\Lenovo\Desktop\ConsoleApplication2\x64\Debug\ConsoleApplication2.exe (process 22592) exited with code 0.
```

The ciphertext:

**JGRMQOYGHMVBJWRWQFPWHGFFDQGFPFZRKBEEBJIZQQOCIBZKLF
AFGQVFZFWWEOGWOPFGFHWOLPHLRLOLFDMFGQWBLWBWQOLKF
WBYLBLYLFSFLJGRMQBOLWJVFPFWQVHQWFFPQOQVFPQOCFPOGFW
FJIGFQVHLHLROQVFGWJVFPFOLFHGQVQVFILEOGQILHQFQGIQVVOS
FAFGBWQVHQWIJVWJVFPFWHGFIWIHZZRQGBABHZQOCGFHX**

Decrypted Text:

**IORMTNAOHMSRIARATEDAHOEESTOEDEZRKREERIIZTTNCIRZKIEAEO
TSEZEAAENOANDEOEHANIDHIRINIESMEOTARIARATNIKEARAIRIAIESE
IIORMTRNIAISEDEATSHTAEEDTNTSEDTNCEDNOEAEIIOETSHIHIRNTSE
OAISEDENIEHOTSTSEIIENOTIIHTETOITSSNSEAEORATSHTAIISAISEDEA
HOEIAIHZZRTORARHZTNCOEHJ**

- **The code is in another file that was delivered with PDF**