Network and Telecommunications Systems Security

Homework_1

AM: EN2190001

Name :Evangelos Siatiras

Exercise A

- Deliberate Acts of Espionage or Trespass

Lost Password:

One of the most common goals of a hacker is to obtain a valid user account and password. In fact, sometimes this is the only way a hacker can bypass security measures. If a company uses firewalls, intrusion detection systems, and more, a hacker will need to borrow a real account until he can obtain root access and set up a new account for himself. However, how can a hacker get this information? One of the easiest ways is to trick someone into giving it to them. For example, many organizations use a virtual private network (VPN) that enables remote employees to connect to the network from home and essentially become a part of the local network. This is a very popular method of enabling people to work from home, but is also a potential weak spot in any security perimeter. As VPNs are set up and maintained by the IT department, hackers will often impersonate an actual employee and ask one of the IT staff for the password by pretending to have lost the settings. If the IT employee believes the person, he willingly and often gladly hands over the keys. Voila! The hacker now can connect from anywhere on the Internet and use an authorized account to work his way deeper into the network. Imagine if you were the lowly IT staff person on call and the CEO rang you up at 10:30 p.m. irate about a lost password. Would you want to deny her access, risking the loss of your job? Probably not, which makes this type of fear a hacker's best friend.

This violates the C.I.A triplet in every aspect as the password is confidential and in being handed over to unauthorized person (violates confidentiality) which lead to giving access to the data of the company causing a security issue by having the ability to violate the integrity of the data (as the databases might be corrupted) as well as the availability of the services of the company causing damage needing days to recover.

- Deliberate Acts of Information Extortion

Chatty Technicians:

If you are a home user and think you have nothing to fear from this type of impersonation, think again-you are actually targeted more often by scammers and hackers alike. This is because many Internet newcomers (newbies) will believe anything someone appearing to be their ISP's tech support personnel tells them. For example, hackers will often send out mass messages to people, or sit in chat rooms and wait for a newbie to come along. They will then set up a fake account or use simple tricks to make it appear as if an AOL employee is chatting with them. What the newbies do not realize is that they are actually talking with a hacker in disguise. So, they willingly hand over everything from credit cards to user names and passwords. As you can see, to a beginner it appears that an AOL Administrator is on the other side of this conversation. However, if you look closely, you will see a blank like after Hckr name:. To make it appear as though an AOL System Administrator is talking, we added a line of space characters to the beginning of the text to drop the AOL System Administrator: to the next line. Although the original name does appear, it would not be difficult for a hacker to set up an account using a date or company name to disguise the fact the account was simply another username.

Here confidentiality is violated as the personal details like credit card numbers,username and passwords are exposed to public as well as the availability as the person will not be able to access to his personal accounts or to withdraw money as well as integrity as he thinks that the information in his personal account are true and in correct form for its original purpose.

- Deliberate Acts of Theft

Sniffing:

A sniffer is a program and/or device that monitors all information passing through a computer network. It sniffs the data passing through the network off the wire and deter-mines where the data is going, where it's coming from, and what it is. In addition to these basic functions, sniffers might have extra features that enable them to filter a certain type of data, capture passwords, and more. Some sniffers (for example, the FBI's controversial massmonitoring tool Carnivore) can even rebuild files sent across a network, such as an email or Web page. A sniffer is one of the most important information gathering tools in a hacker's arsenal. The sniffer gives the hacker a complete picture (network topology, IP addresses) of the data sent and received by the computer or network it is monitoring. This data includes, but is not limited to, all email messages, passwords, user names, and documents. With this information, a hacker can form a complete picture of the data traveling on a network, as well as capture important tidbits of data that can help her gain complete control over a network.

This is a characteristic example where all the C.I.A Triangle is violated as hacker have complete unauthorized access to services as well as all the information related passwords and mail addresses while the company employees as well as the security department have complete unawareness of the situation.

The ideas of the scenarios written above where from a nonpublic presentation in my company.

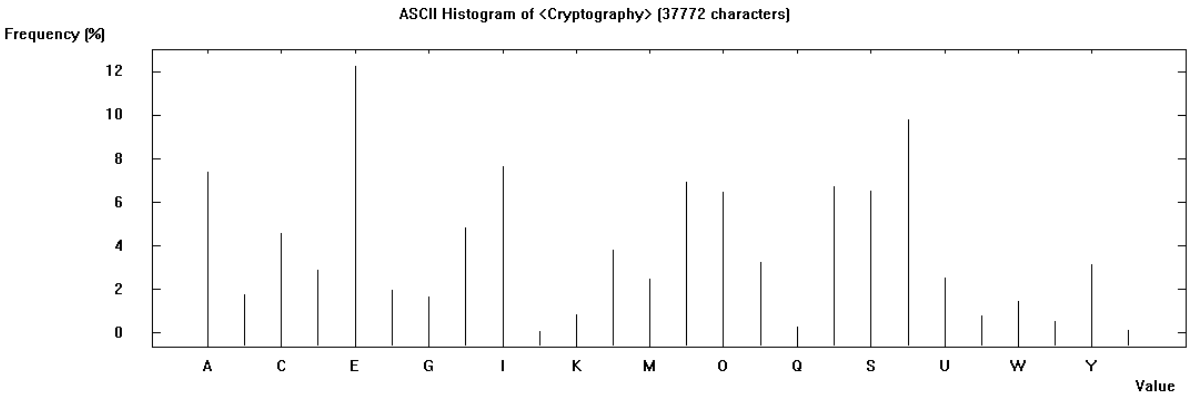
Exercise B_1

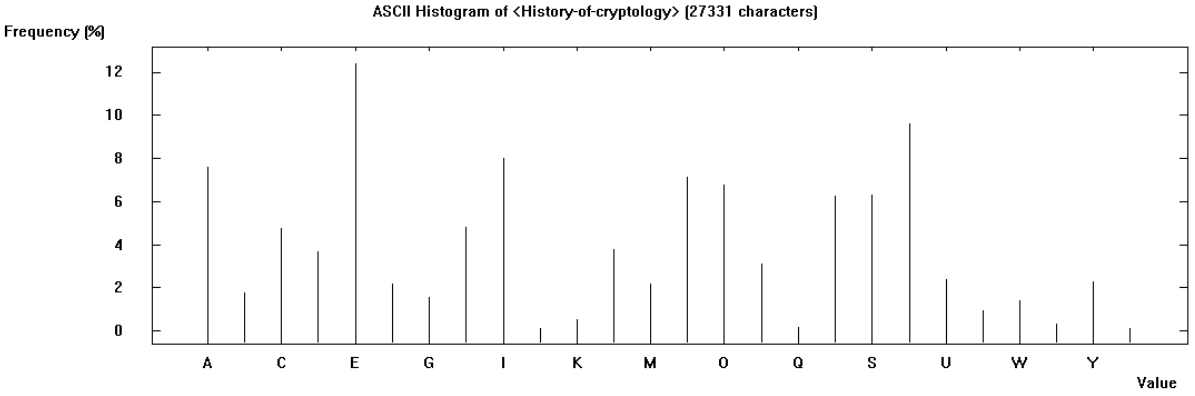
I have chosen two scientific articles from Britannica Library as per the below links:

https://www.britannica.com/topic/cryptology/History-of-cryptology

https://www.britannica.com/topic/cryptology/Cryptography

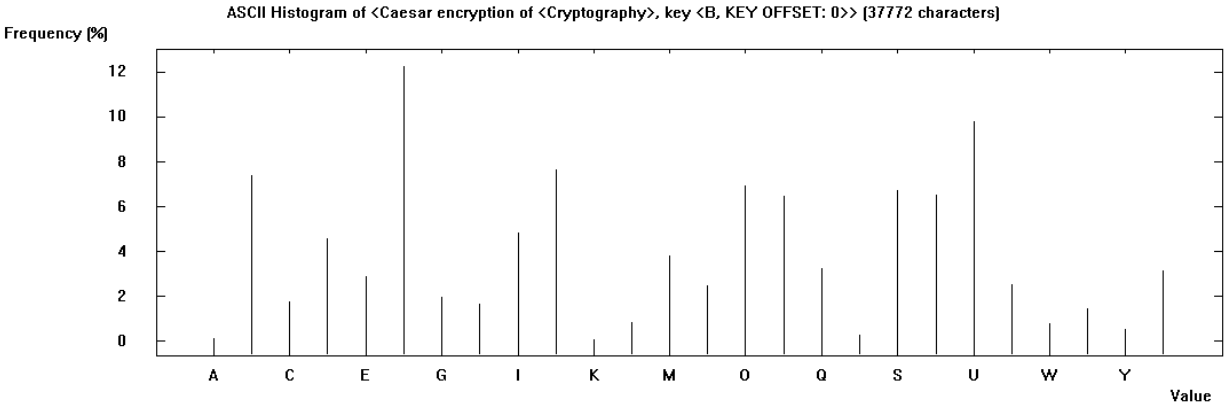
Below find the Frequency analysis of the letters in every document. In title of every plot is appeared the related document title.

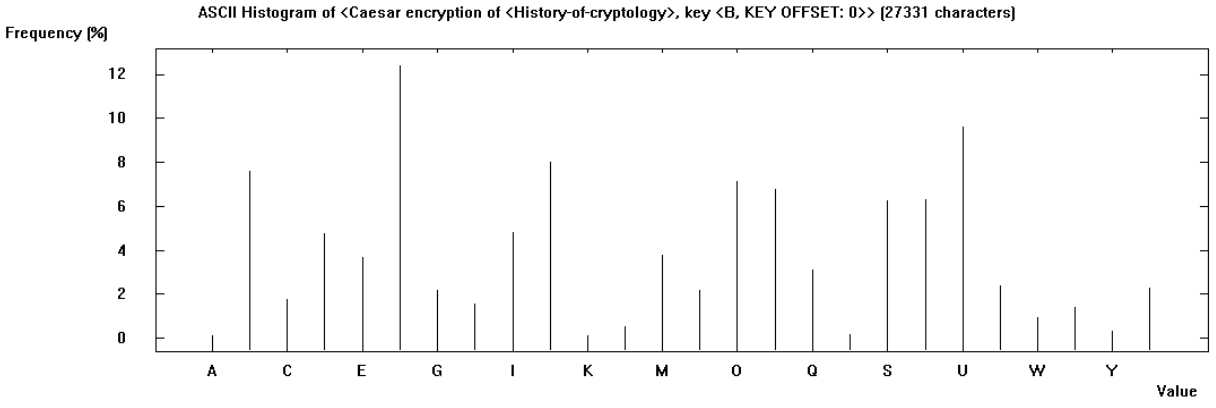


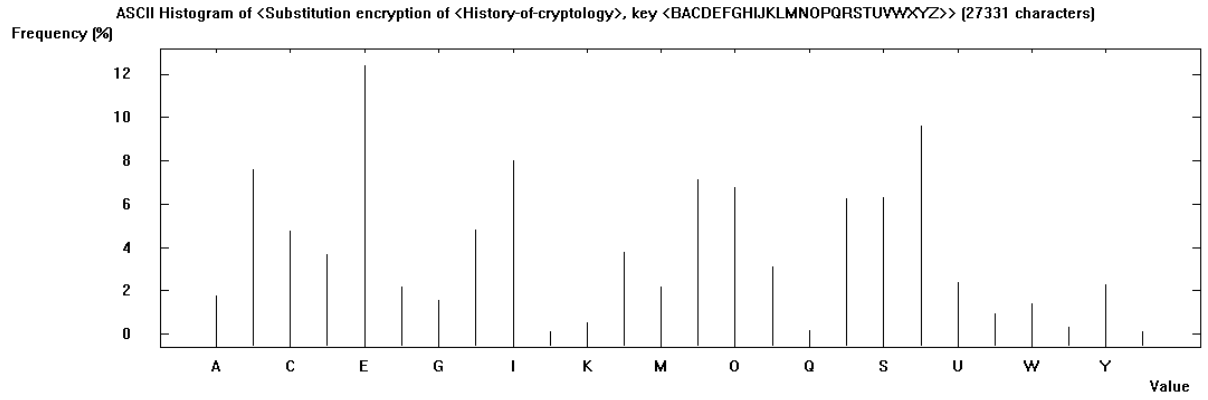


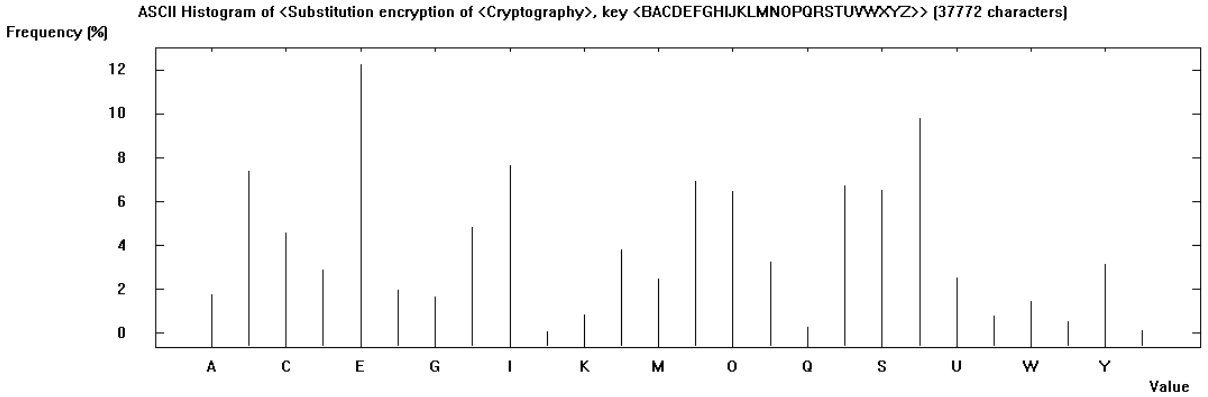
By comparing the above histograms with the relevant histogram showing the percentage frequency of each letter in the English language we can easily see (comparing the plot) the percentage frequencies of each letter are very close and sometimes almost identical. So the hypothesis for the frequencies of the 26 characters of the English language is confirmed based on the statistics from the two mentioned scientific documents.

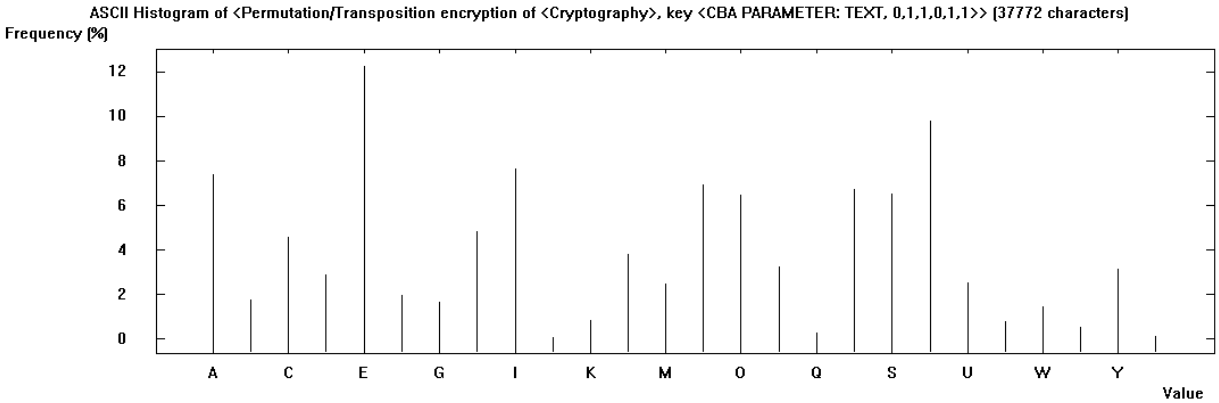
Below we are performing the requested encryptions where the type of encryption and the key is appeared in the title of every histogram.

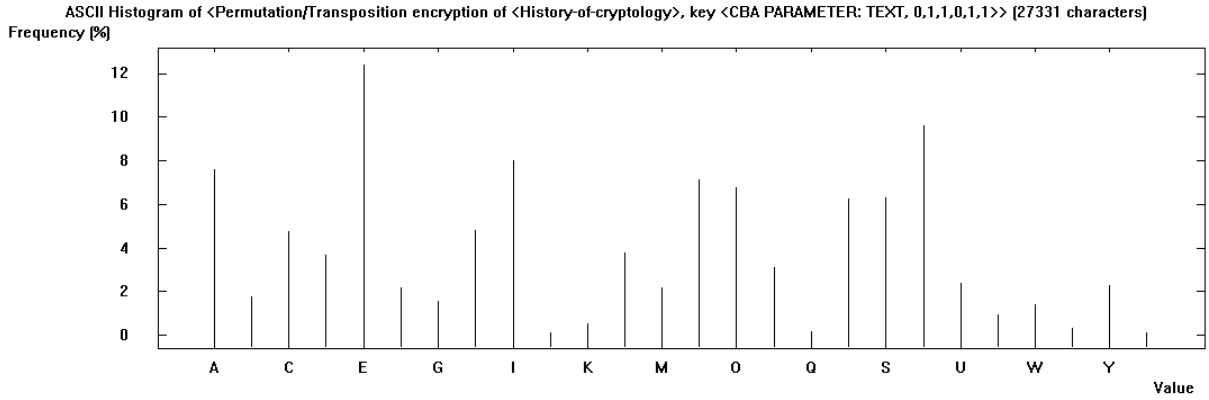






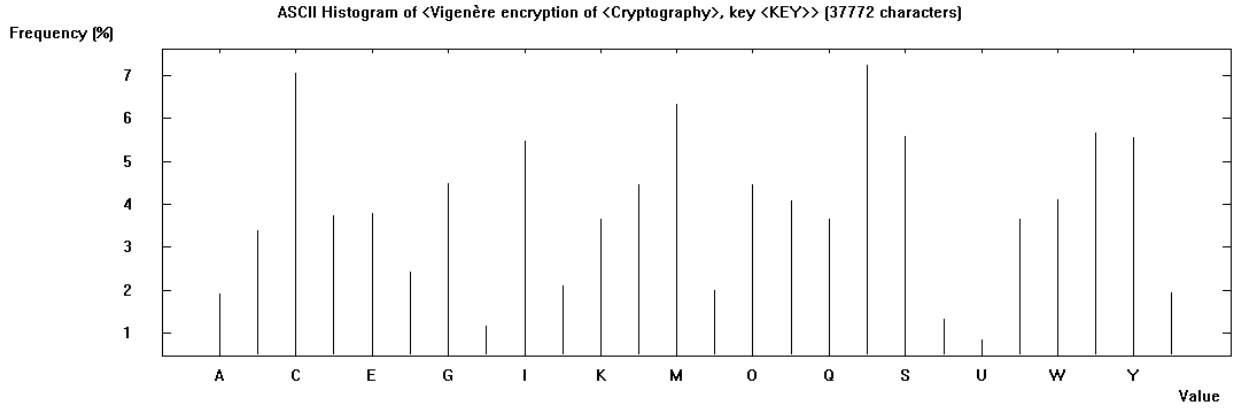


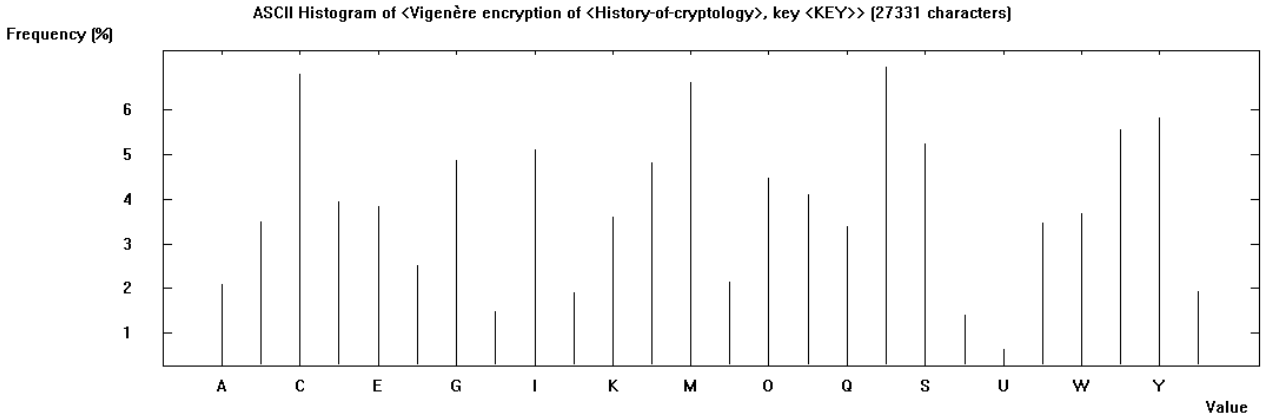




Referring to Caesar cipher ,monoalphabetic substitution cipher as well as permutation cipher , are related to substitutions in the alphabet. In the examples above the key for Caesar cipher is shifting by 1 the alphabet, in the monoalhabetic substitution we replace “b” with “a” and vice versa and with permutation cipher we transpose the vector

containing the ciphertext, by changing the first with the third column. So the results were as expected, where the resulting plots are close but the letters (in each ciphertext coming from different cipher) are different.





The final distribution, for the Vigenère Cipher, is different to the others, and the distribution of letters is much more smoothed out. This shows that the same letter can be achieved by different plaintext letters. We can conclude that is very difficult, almost impossible to break this cipher with frequency analysis.

Generally we can deduce a lot of details from block sizes, encryption modes, relative key size to block size padding method, ciphertext length, non-random plaintext etc. but I think that Output of a cryptography algorithm should be like an output of a pseudo random number generator. If it's possible to deduce details like the above mentioned the cryptography algorithm is not a good cryptography algorithm.

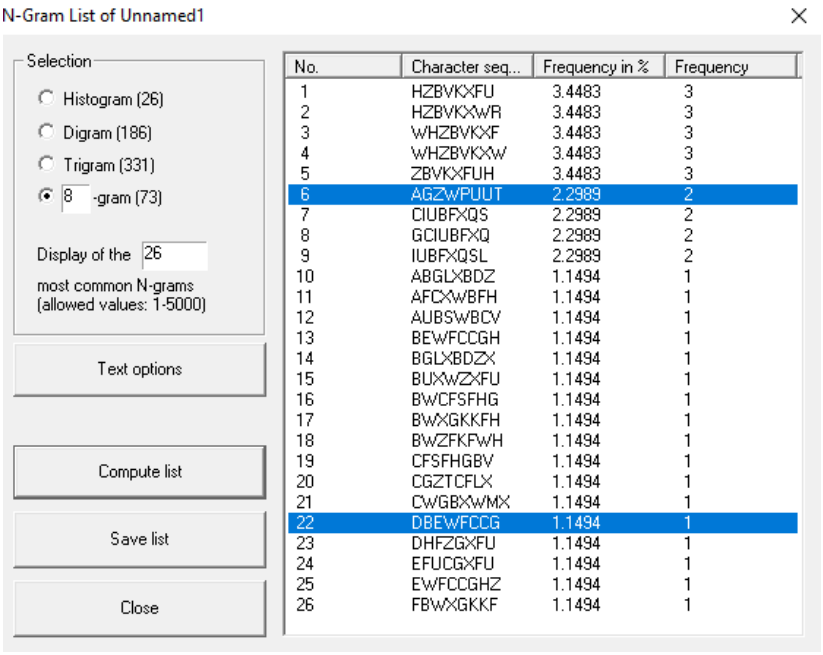
Exercise B_2

After following the above mentioned steps we get the following decrypted message :

The apility of encrybtion to shield a user's communications rests ubon the assumbtion that the sender and recibient's devices are themselves secure, with the encrybted channel the only weak boint. Put Facepook announced earlier this year breliminary results from its efforts to move a glopal mass surveillance infrastructure directly onto users' devices where it can pybass the brote ctions of end-to-end encrybtion. In Facepook's vision, the actual end-to-end encrybtion client itself such as WhatsAbb will include empedded content moderation and placklist filtering algorithms. These algorithms will pe continually ubdated from a central cloud service, put will run locally on the user's device, scanning each cleartext message pefore it is sent and each encrybted message after it is decrybted. The combany even noted that when it detects violations it will need to quietly stream a coby of the formerly encrybted content pack to its central servers to analyze further, even if the user opjects, acting as true wiretabbing service.

Is obvious that the message did not decrypted correctly due to the wrong key chosen by the tool. The process of frequency analysis uses various subtle properties of the language, and for this reason, it is near impossible to have a computer do all the work. Inevitably, an element of human input is necessary in this process to make educated decisions about which letters to substitute.

b) Knowing that the word Facebook is contained within the original text we expect to find one sequence of letters with the length 8 (length of the word facebook) and ideally more than one time.So let's check for repeating 8-graphs using the tool.We are looking for any sequence with the same second and third letter from the last as facebook has "oo" in that position.



No.	Character seq...	Frequency in %	Frequency
1	HZBVKXFU	3.4483	3
2	HZBVKXWR	3.4483	3
3	WHZBVKXF	3.4483	3
4	WHZBVKXW	3.4483	3
5	ZBVKXFUH	3.4483	3
6	AGZWPUUT	2.2989	2
7	CIUBFXQS	2.2989	2
8	GCIUBFXQ	2.2989	2
9	IUBFXQSL	2.2989	2
10	ABGLXBDZ	1.1494	1
11	AFCXWBFH	1.1494	1
12	AUBSWBCV	1.1494	1
13	BEWFCCGH	1.1494	1
14	BGLXBDZX	1.1494	1
15	BUXWZXFU	1.1494	1
16	BWCFSFHG	1.1494	1
17	BWXGKKFH	1.1494	1
18	BWZFKFWH	1.1494	1
19	CFSFHGBV	1.1494	1
20	CGZTCFLX	1.1494	1
21	CWGBXWMX	1.1494	1
22	DBEWFCCG	1.1494	1
23	DHFZGXFU	1.1494	1
24	EFUCGXFU	1.1494	1
25	EWFCCGHZ	1.1494	1
26	FBWXGKKF	1.1494	1

From the image above we see that the are two possible choices with the choice 6 more likely correct.

So assuming that choice 6 is encoded to facebook I substitute all the letter with the related ones from the word facebook respectively.

At a first glance we see that we decoded the word "of" in our ciphertext so we probably made the right choice.Let's continue with a frequency analysis of our ciphertext.We see that X is the second most probable letter(the "W" is the first one but it is already decoded to "e") so probably it should be decoded as "t" which is the second most probable letter in the English language.After doing so we see that our ciphertext starting with "tqe" so probably 2 should be decoded to "h".Then with a small investigation we see that there is a word "thele" so a possible substitution of "l" is "r".We continue with the same way and we end up with the following substitution key: etnisarocldhupymfvbwgkxqjz.

Excersise B_3

As first step and by just looking in the ciphertext realized that the only repeating unit is the "usj".By using the n-graph report of the cryptool I am finding all the repeating n-graphs starting from 3-graph.

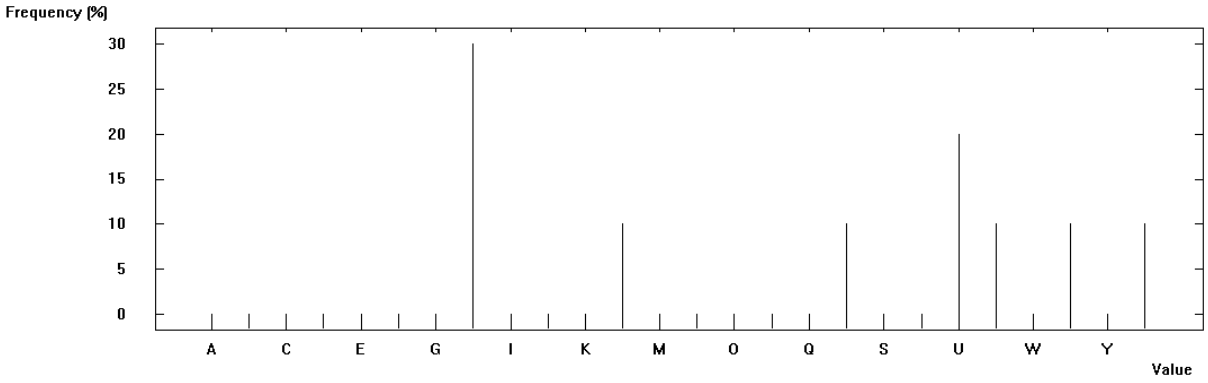
After trying with 3-gram and 4-gram and so on, the only sequence of unit with frequency >1 is "usj" as showing in the picture below.

No.	Character seq...	Frequency in %	Frequency
1	USJ	7.4074	2
2	BHG	3.7037	1
3	BHM	3.7037	1
4	FYH	3.7037	1

Also from the ciphertext we see that the distance of the two repeating units is 9 letters suggesting a keyword length of 9 or 3 or 1 letter. As the text is small we can easily realize that the most likely key length is 3. In general case when we look down the whole set of repeating units we are looking for the highest number that is selected in most of the pairs of repeating units. Then we analyze each set of ciphertext letters that was encoded by the same keyword letter by writing the ciphertext out in 3 columns, each headed by a letter of the keyword.

KeyWord_Letter_1	KeyWord_Letter_2	KeyWord_Letter_3
Z	S	g
U	S	J
L	G	I
R	J	K
U	S	J
V	O	B
H	M	U
X	F	Y
H	Z	B
H	g	

Now for the KeyWord_Letter_1 we are performing frequency analysis in this column and we are comparing it with the frequency analysis of the English language.



We can extract that if we shift the column by 3 the frequency analysis now will be closer to the one of the English language. Similarly if we shift the starting KeyWord_Letter_1 = “a” by 3 we get KeyWord_Letter_1 = “d” . Now I update the decrypt message where every letter in the ciphertext that is encoded using this letter of the keyword is changed to what it would be if decrytped by this key letter.So the decrypt message now is wSGrSJiGIoJKrSJsOBeMUuFYeZBeG .With small letters are the characters changed in that step. If we proceed by the same way for the second column we see that we should shift the column by 14 and with that way we get the KeyWord_Letter_2 = “o” and the decrypted message will be weGreJisIovKreJsaBeyUurYelBes .We follow the same procedure for the KeyWord_Letter_3.We end up with KeyWord_Letter_3 = “g” and the decrypted message is wearediscoveredsaveyourselves .