CECS 378
Introduction to Computer Security

LAB 02
ENCRYPTION & DECRYPTION

2021

Student : Thanh Nguyen – ID: 026843815

Due date: 02/15/2021

I. Decryption results:

1. Part II-A.2: The hidden Message is:
   "Hello everyone and Delcome to Spring 2021, CLCS 378!. I hope you didn't translate this by hand, that's what computers are for. If you did it by hand, you should redo it becuase doing it by hand is inefficient and that's why this text is so long. Also, this assigment calls for a small python program.One way of solving this, is using string.maketrans() and it is recommended. Hope you had fun working this out.Looking forward to working with all of you this semester! :)"

2. Part II-A.3: The encryption Key used is: 19 (A => T)

II. Encryption results:

1. Part II-A.4: The encrypted message with key = 4 is:
   "Lipps izivcsri erh Hipgsqi xs Wtvmrk 2021, GPGW 378!. M lsti csy hmhr'x xverwpexi xlmw fc lerh, xlex'w alex gsqtyxivw evi jsv. Mj csy hmh mx fc lerh, csy wlsyph vihs mx figyewi hsmrk mx fc lerh mw mrijjmgmirx erh xlex'w alc xlmw xibx mw ws psrk. Epws, xlmw ewwmkqirx geppw jsv e wqepp tcxlsr tvskveq.Sri aec sj wspzmrk xlmw, mw ywmrk wxvmrk.qeoixverw() erh mx mw vigsqqirhih. Lsti csy leh jyr asvomrk xlmw syx.Pssomrk jsvaevh xs asvomrk amxl epp sj csy xlmw wiqiwxiv! :)"

III. Coding:

- For decryption: I run the key from 1 to 25. Then with each key, shifted left the message. Checked that if that new message included some common words in English (I took some words of common words in English on Wiki and put it into the Words.txt file), then this key is the key we need and we found the plaintext.
- For encryption: With the plaintext that we found above, I shifted right the message with key = 4, and then got the ciphertext.

IV. Screenshot of results and Checking with Cryptool:

- Screenshot:

```
========================= RESTART: C:\CECS 378\lab02.py =========================
The provided cipher text is:
Axeeh xoxkrhgx tgw Wxevhfx mh Likbgz 2021, VEVL 378!. B ahix rhn wbwg'm mktgletm
x mabl ur atgw, matm'l patm vhfinmxkl tkx yhk. By rhn wbw bm ur atgw, rhn lahnew
 kxwh bm uxvntlx whbgz bm ur atgw bl bgxyybvbxgm tgw matm'l par mabl mxqm bl lh
ehgz. Telh, mabl tllbzfxgm vteel yhk t lftee irmahg ikhzktf.Hgx ptr hy lheobgz m
abl, bl nlbgz lmkbgz.ftdxmktgl() tgw bm bl kxvhffxgwxw. Ahix rhn atw yng phkdbgz
 mabl hnm.Ehhdbgz yhkptkw mh phkdbgz pbma tee hy rhn mabl lxfxlmxk! :)

The key was used is: 19 ( A -> T )
The plain text is:
Hello everyone and Delcome to Spring 2021, CLCS 378!. I hope you didn't translat
e this by hand, that's what computers are for. If you did it by hand, you should
 redo it becuase doing it by hand is inefficient and that's why this text is so
long. Also, this assigment calls for a small python program.One way of solving t
his, is using string.maketrans() and it is recommended. Hope you had fun working
 this out.Looking forward to working with all of you this semester! :)

The ciphertext with key = 4 is:
Lipps izivcsri erh Hipgsqi xs Wtvmrk 2021, GPGW 378!. M lsti csy hmhr'x xverwpex
i xlmw fc lerh, xlex'w alex gsqtyxivw evi jsv. Mj csy hmh mx fc lerh, csy wlsyph
 vihs mx figyewi hsmrk mx fc lerh mw mrijjmgmirx erh xlex'w alc xlmw xibx mw ws
psrk. Epws, xlmw ewwmkqirx geppw jsv e wqepp tcxlsr tvskveq.Sri aec sj wspzmrk x
lmw, mw ywmrk wxvmrk.qeoixverw() erh mx mw vigsqqirhih. Lsti csy leh jyr asvomrk
 xlmw syx.Pssomrk jsvaevh xs asvomrk amxl epp sj csy xlmw wiqiwxiv! :)
>>>
```

- Cryptool decrypt/encrypt: