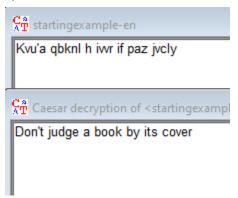
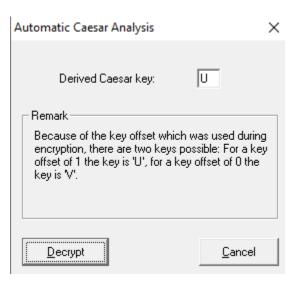
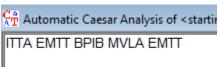
NIS Lab Quiz-1

Question: 1

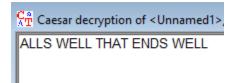


Question: 2





The above decrypted text is not readable so after my assumptions key is . Key = D



Question: 3

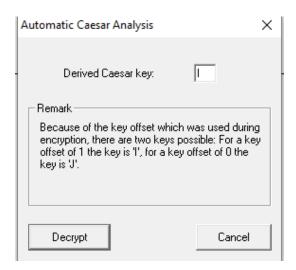


Table 2 Automatic Caesar Analysis of <unnamed1>, key: <Key: <I>> tobeornottobethatisthequestionwilliamshakespeare

Question: 4

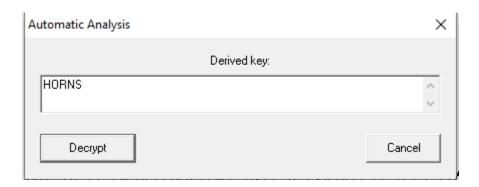


Can Automatic Caesar Analysis of <Unnamed1>, key: <Key: <G>>

Twas brillig, and the slithy toves Did gyre and gimble in the wabe: All mimsy were the borogoves, And the mome raths outgrabe. Beware the Jabberwock, my son! The jaws that bite, the claws that catch! Beware the Jubjub bird, and shun The frumious Bandersnatch!

Question: 5

Key:



🚰 Automatic Vigenère Analysis of < Unnamed1>, key: < HORNS>

LADIES AND GENTLEMEN: I AM GLAD YOU GAVE AN AWARD TO THE PRESS TONIGHT. BECAUSE THAT GAVE THEM THE OPPORTUNITY TO TELL US JUST WHAT THEY COULD DO. NOW WE HAVE COME HERE TONIGHT BECAUSE OF CIVIL LIBERTIES. I IMAGINE A GREAT MANY OF YOU COULD GIVE MY TALK FAR BETTER THAN I COULD, BECAUSE YOU HAVE HAD FIRST-HAND KNOWLEDGE IN THE THINGS YOU HAVE HAD TO DO IN CHICAGO OVER THE YEARS TO PRESERVE CIVIL LIBERTIES. PERHAPS, HOWEVER, I AM MORE CONSCIOUS OF THE IMPORTANCE OF CIVIL LIBERTIES IN THIS PARTICULAR MOMENT OF OUR HISTORY THAN ANYONE ELSE. BECAUSE AS I TRAVEL THROUGH THE COUNTRY AND MEET PEOPLE AND SEE THINGS THAT HAVE HAPPENED TO LITTLE PEOPLE. I REALIZE WHAT IT MEANS TO DEMOCRACY TO PRESERVE OUR CIVIL LIBERTIES. ALL THROUGH THE YEARS WE HAVE HAD TO FIGHT FOR CIVIL LIBERTY, AND WE KNOW THAT THERE ARE TIMES WHEN THE LIGHT GROWS RATHER DIM, AND EVERY TIME THAT HAPPENS DEMOCRACY IS IN DANGER. NOW, LARGELY BECAUSE OF THE TROUBLED STATE OF THE WORLD AS A WHOLE. CIVIL LIBERTIES HAVE DISAPPEARED IN MANY OTHER COUNTRIES. IT IS IMPOSSIBLE, OF COURSE, TO BE AT WAR AND TO KEEP FREEDOM OF THE PRESS

AND FREEDOM OF SPEECH AND FREEDOM OF ASSEMBLY. THEY DISAPPEAR AUTOMATICALLY. AND SO IN MANY COUNTRIES WHERE ORDINARILY THEY WERE SAFE, TODAY THEY HAVE GONE. IN OTHER COUNTRIES, EVEN BEFORE WAR CAME, NOT ONLY FREEDOM OF THE PRESS AND FREEDOM OF ASSEMBLY, AND FREEDOM OF SPEECH DISAPPEARED, BUT FREEDOM OF RELIGION DISAPPEARED. AND SO WE KNOW THAT HERE IN THIS COUNTRY, WE HAVE A GRAVE RESPONSIBILITY.

Question: 6

Plaintext: My final project is on ransomware detection and prevention using ML and AI, which is the need of today's world as ransomware is most common in this era.

Encryption using Hill:

Key



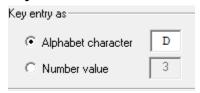
Ciphertext

Hill encryption of <Unnamed1>, key <DIM 2, KEY: XU UF , ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ, ALPHABET_OFFSET: 0 MULT...>

Cw pknah jvubskf yq kh bcjmqcmydw tcxkkfwwn avp jvsdopzekh owcro YT mvp EO , whqoj yo nhe puwr gt piric'y gqnfr ia dansoomchs qe eggj aqckyr od rjya qbc.

Encryption using Caeser:

Key



Ciphertext



Encryption using ROT-13:

Key

Key is already know which is 13 or "N"

Ciphertext

```
ROT 13 encryption of <Unnamed1>, key <N, KEY OFFSET: 0>

ZI svany cebwrpg vf ba enafbzjner qrgrpgvba naq ceriragvba hfvat ZY naq NV , juvpu vf gur arrq bs gbqnl'f jbeyq nf enafbzjner vf zbfg pbzzba va guvf ren.
```

Encryption using Atbash:

Key



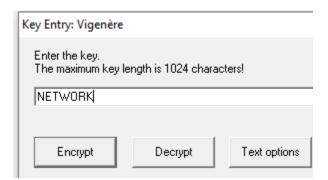
Ciphertext

\$\frac{\alpha}{\sqrt{\gamma}}\$ Substitution encryption of <Unnamed1>, key <GOALBCDEFHI/KMNPQRSTUVWXYZ>

Ky cfmgj prnhbat fs nm rgmsnkwgrb lbtbatfnm gml prbvbmtfnm usfmd KJ gml GF , wefae fs teb mbbl nc tnlgy's wnrjl gs rgmsnkwgrb fs knst ankknm fm tefs brg.

Encryption using Vigenere:

Key



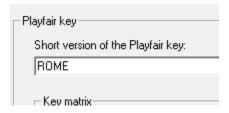
Ciphertext

🚰 Vigenère encryption of <Unnamed1>, key <NETWORK>

Zc yebrv cvhfstd ww hj frxfsfsoio qimaqksbr tjr gbrzxjhzya ylebx WY egz OZ, gumvd wj dui gasu ys xhzop'c jskhr rc eegocdgnvx eg dyfx vkadya mg pvzc rvt.

Encryption using Playfair:

Key



Ciphertext

The Playfair encryption of <Unnamed1>, key <KEY: ROME, SEPARATOR1: X, SEPARATOR2: Y, MATRIXSIZE: 5, OPT_IGNORE_DUPLICATE_...>

EX CL UG HT OM LO FQ KQ AI OR KU ME ZO OA FM YF FQ QC UG KG VB RY AL QL AI PT KH DA NE KG ON VI QI IK TU LR LA MF EC QE GM XT OC EH GM PM GU QM OX RO OL XD MQ QF ME EM HK LU IK TM OR

Prefered Algorithm:

I would prefer the Hill cipher algorithm as it is hard to break using frequency analysis and it effectively hides single letter and two letter frequencies.