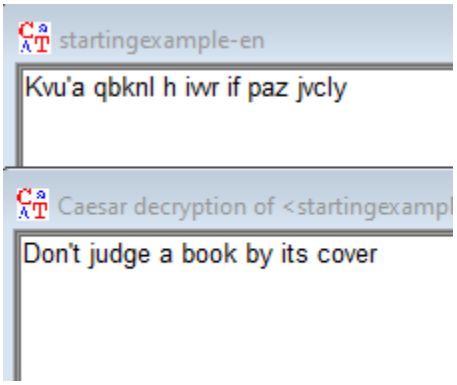
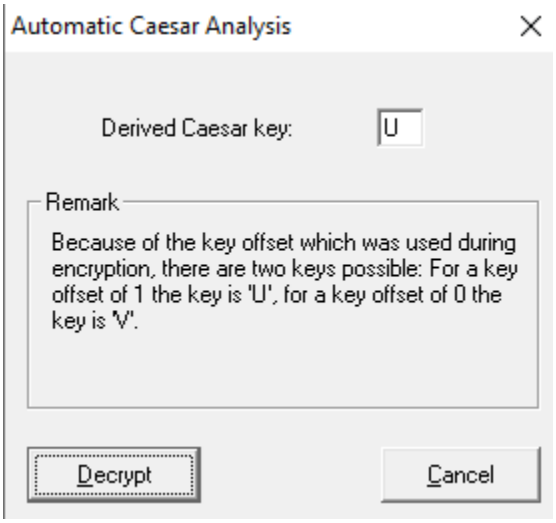
Kabeer Ahmed SE-19028

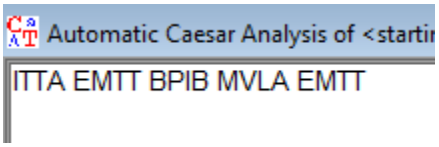
NIS Lab Quiz-1

Question : 1

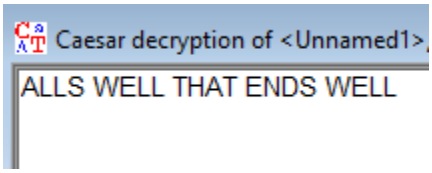


Question : 2



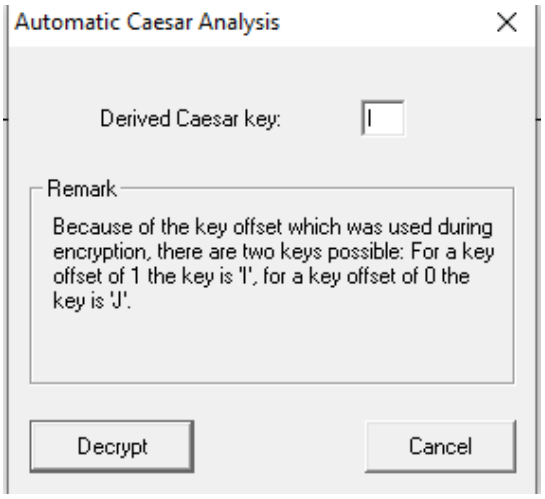


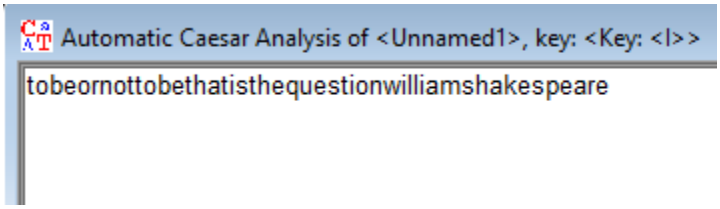
The above decrypted text is not readable so after my assumptions key is .
Key = D



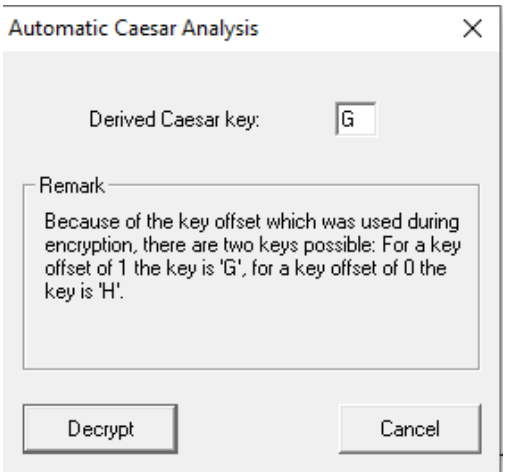
Kabeer Ahmed SE-19028

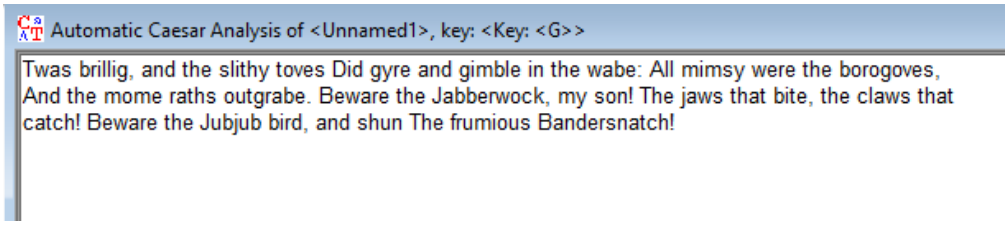
Question : 3





Question : 4

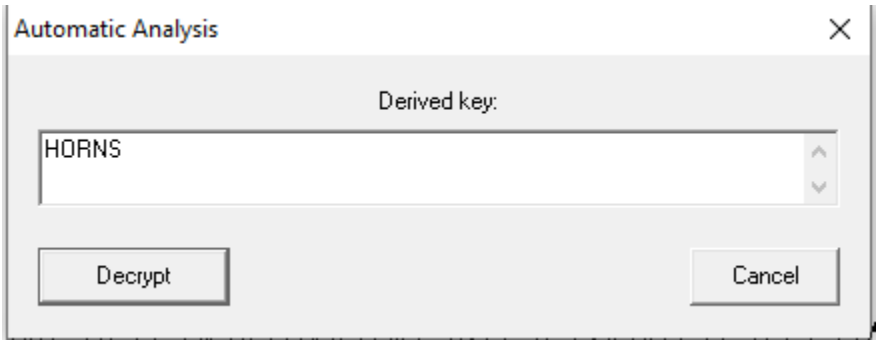




Kabeer Ahmed SE-19028

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.

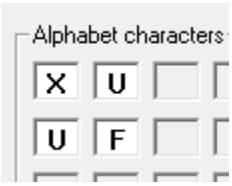
Kabeer Ahmed SE-19028

Question : 6

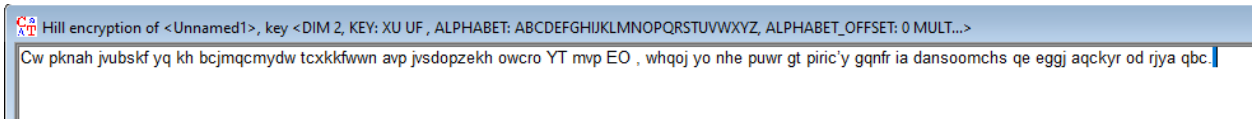
Plaintext: My final project is on ransomware detection and prevention using ML and AI , which is the need of today's world as ransomware is most common in this era.

Encryption using Hill:

Key

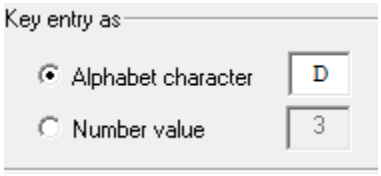


Ciphertext

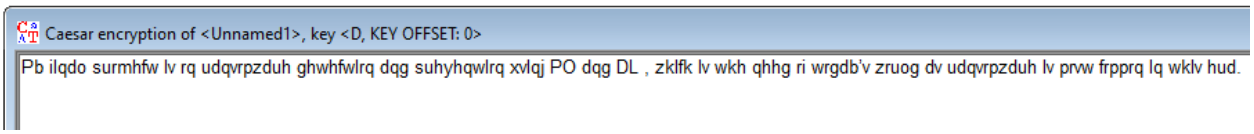


Encryption using Caeser:

Key



Ciphertext



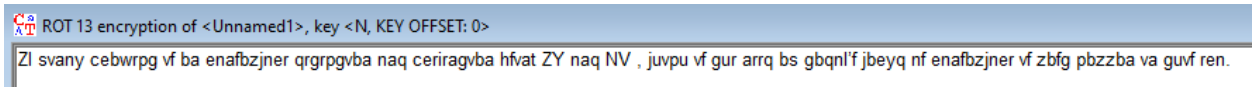
Encryption using ROT-13:

Key

Kabeer Ahmed SE-19028

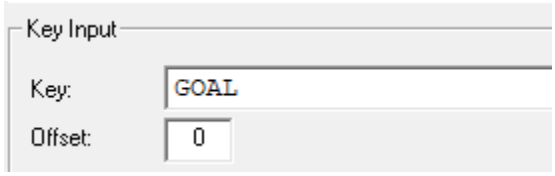
Key is already know which is 13 or “N”

Ciphertext

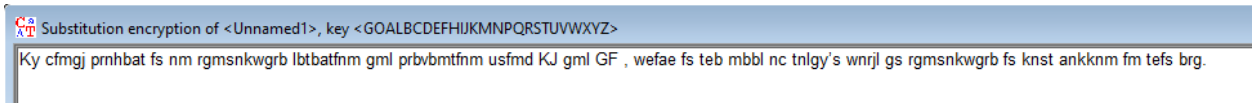


Encryption using Atbash:

Key

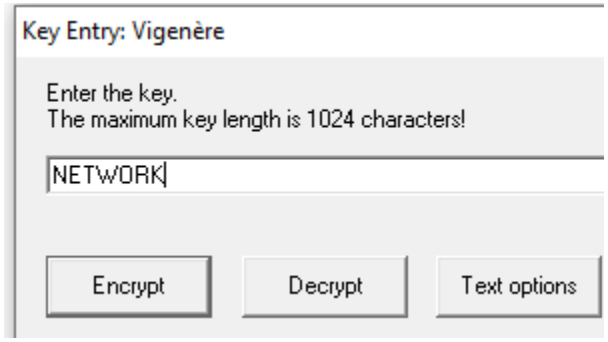


Ciphertext



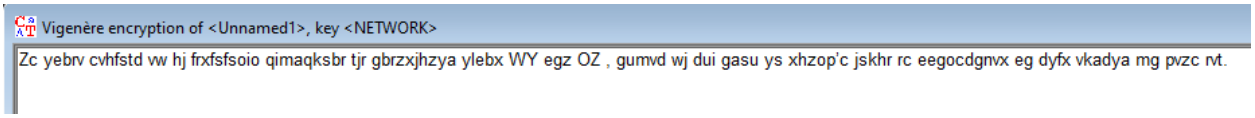
Encryption using Vigenere:

Key



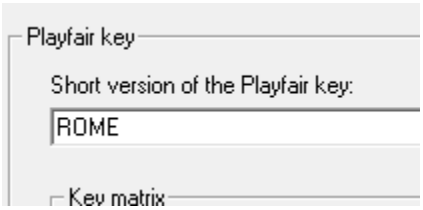
Ciphertext

Kabeer Ahmed SE-19028

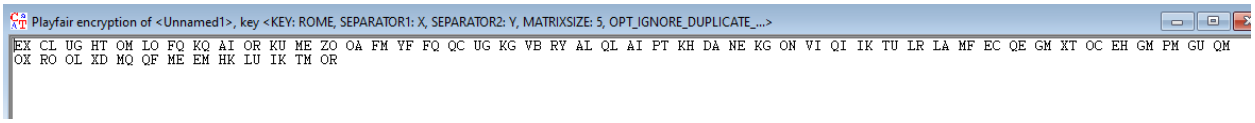


Encryption using Playfair:

Key



Ciphertext



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.