

Readable cleartext (i.e., formatted with blank spaces, dashes, numbers, and so on)

”YOUAREENTERINGTHEVICINITYOFANAREAADJACENTTOALLOCATION.
THEKINDOFPLACEWHEREETHEREMIGHTBEAMONSTER,ORSOMEKINDOFWEIRDMIRROR.
THESEAREJUSTEXAMPLES:ITCOULDALSOBESOMETHINGMUCHBETTER.
PREPARETOENTERTHESCARYDOOR.”
–FUTURAMAINAHEADINTHEPOLLS
EXCELLEN2RK.ITSEEMSTHEVIGENEREORACLEMIGHTNOTPROVIDEGOODSECURITYAFTERALL.
TO”CHARLESBABBAGE,THEFIRSTKNOWNTOEVERBREAKTHEVIGENERECIPHER:1
OFTHEMOSTSINGULARCHARACTERISTICSOFTHEARTOFDECIPHERINGISTHESTRONG
CONVICTIONPOSSESSEDBYEVERYPerson,EVENMODERATELYACQUAINTEDWITH
IT,THATHEISABLETOCONSTRUCTACIPHERWHICHNOBODYELSECANDECIPHER.
YOUHAVEPROVENTOBEAFORMIDABLEANDSHREWD CODEBREAKERINDEED.
THENEXTCHALLENGEISAKNOWN-PLAINTEXTATTACK.
YOUFINDALLTHECLUESYOU NEEDFORSOLVINGCRYPTOCHALLENGE3ONTHE
FOLLOWINGADDRESS:
HTTPS://LUNDGREN.PHD/IT754A/2023/T/9983.ZIP

In your own words, explain what you learned solving the challenge

I used an n-gram analysis to break the cipher. By comparing the frequency of trigrams in the English language to those in the translated text, I made educated suppositions about the implicit decryption key. This system, while not the chosen-plaintext attack explicitly mentioned in the challenge, allowed me to identify a probable key for decryption. still, I am apprehensive that the deciphered text is not impeccably clear; it's concatenated and might not be the most readable. This could be due to the system I used, which was not the specified chosen-plaintext attack.

A short explanation of how you broke the cipher

From this challenge, I have learned the significance of statistical analysis in cryptography. Using n-gram analysis was informational, showing how language patterns can be a important tool against encryption indeed without knowing the exact key. still, I fete that the outgrowth, while decipherable, is not as clean as one would hope. I know that the text is jumbled, and words are concatenated, making it a bit grueling to read. This might be because the system I used was not the exact chosen-plaintext attack that was explicitly needed. Still, I believe the result is scrutable enough to move on to the coming challenge.

What factors facilitated your attack on this Crypto Challenge?

The vulnerability in the cipher was its vulnerability to frequency analysis. The patterns in the English language, especially the trigrams, handed enough suggestions to make educated suppositions about the decryption key. still, I am conscious that the system I used was not the chosen-plaintext attack, which was the clear demand for this challenge. Despite this, I was still suitable to crack the cipher, albeit with a less- than-perfect result. The deciphered text, while not entirely clear, is still decipherable, which I believe might be sufficient for the coming stage of the challenge.

proof: https://github.com/robmind/SVQ3NTRB/tree/main/Crypto_Challenge_2