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

" IT IS CERTAINLY RATHER A CURIOUS PRODUCTION, " SAID
HOLMES. " AT FIRST SIGHT IT WOULD APPEAR TO BE SOME CHILDISH
PRANK. IT CONSISTS OF A NUMBER OF ABSURD LITTLE FIGURES DANCING
ACROSS THE PAPER UPON WHICH THEY ARE DRAWN. WHY SHOULD YOU ATTRIBUTE
ANY IMPORTANCE TO SO GROTESQUE AN OBJECT ? " –
SHERLOCK HOLMES IN ADVENTURE OF THE DANCING MENCONGRATULATIONS,
YOU HAVE SOLVED THE FIRST CRYPTO CHALLENGE. THE NEXT CHALLENGE IS
A CHOSEN-PLAINTEXT ATTACK. YOU FIND ALL THE CLUES YOU NEED FOR
SOLVING CRYPTO CHALLENGE 2 ON THE FOLLOWING ADDRESS:
HTTPS://LUNDGREN.PHD/IT754A/2023/E/6763.ZIP

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

I decrypted the cipher using a substitution method in C#. My approach was to take the encrypted text and attempt to decrypt it by switching the letters based on a key. To verify the success of the decryption, I compared the output to common English word patterns using an n-gram model from the Fusion Table wordlist. This wordlist proved pivotal, as it supplied a benchmark of how frequently certain letter combinations (n-grams) appear in English. By consistently refining my decryption attempts and referencing this wordlist, I managed to progressively approach the original text.

A short explanation of how you broke the cipher

Breaking this code was a real challenge. Not only did I learn a lot about the Substitution Cipher, but I also got hands-on experience with C#. I had to figure out how to use C# to try different ways of decoding and then check if the results made sense. The English Letter word list was like my cheat sheet, helping me see if I was getting closer to the real message. It was a mix of coding, testing, and a lot of trial and error until things started to click.

Reflect briefly on what made your attack possible for the particular Crypto Challenge

What really enabled me to crack this challenge was the English Letter word list (n-gram list). This wasn't just about using a decryption method; it was about validating each attempt, ensuring it made sense linguistically. This word list was my compass, guiding each decryption attempt closer to the real message, making the entire process more efficient and accurate.

proof:

https://github.com/robmind/SVQ3NTRB/tree/main/Crypto_Challenge_1