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

VKORETSTOREMAINSECRETPASTTHEENDOFYOURLIFEEXPECTANCY,
THEN,INORDERTOCHOOSEAKEYLENGTH,YOUHAVETOBEAFUTURIST.
-NEALSTEPHENEONINCRYPTONOMICON
NEXTCHALLENGE:HTTPS://LUNDGREN.PHD/IT754A/2023/F/2701.ZIP

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

This challenge taught me the intricacies of XOR encryption and its vulnerabilities when used with a repetitive key. Leveraging a partial known plaintext allowed for a more efficient decryption attempt.

A short explanation of how you broke the cipher

By using a repetitive key and XOR operation, I was able to decrypt the message. I leveraged the given plaintext snippet, "A One-Time Mistake", and used it as a basis for a brute-force approach. Iteratively trying different key lengths, I managed to decrypt a significant portion of the original message.

What factors facilitated your attack on this Crypto Challenge?

The repetitive use of the key was the primary vulnerability in the encryption method. The XOR operation's properties, combined with the known partial plaintext, provided enough insight to break the cipher. Also, understanding the patterns and structure of the encrypted message proved beneficial.

Proof: https://github.com/robmind/SVQ3NTRB/tree/main/Crypto_Challenge_3