Neuron Assignment Submission

By

Name: Vinod Kumar

Enrollment Number: 20121035

Indian Institute of Technology Roorkee

Mail: vinod_k1@ch.iitr.ac.in

Phone: 7900695331

Simplified Problem Statement:

A message is encrypted by three layers of known algorithms, and I need to decrypt it using the final encrypted message and partially encrypted form of first and second layer. We also know that keywords for all algorithms will be part of the final decrypted message.

Given:

Algorithm1: Keyword Cipher

Encrypted1:

"*****RR *R **S ***TS **V *W*S **T **M *Q **V F**F **T ****E, **S **V *B*J **T E***L**"

Algorithm2: Vigenère Cipher

Encrypted2:

T*EJ *W **L B***X **O *W*L **L **M *J **N *L*X **T ****W, **S **A **CO **M ***FQ**"

Algorithm3: Vigenère Cipher

Final Encrypted Message:

"JHWRUKW NP ZTE OSYZL YSC AJXE QBE WMF SX DAB RYRQ EGM QQEXK, QLG QTO OGQH LTF WBESEU."

Solution and Approach

1. Key corresponding to each encryption algorithm, used for decrypting the messages.

Algorithm1: WELL

Algorithm2: FAST

Algorithm3: NOT

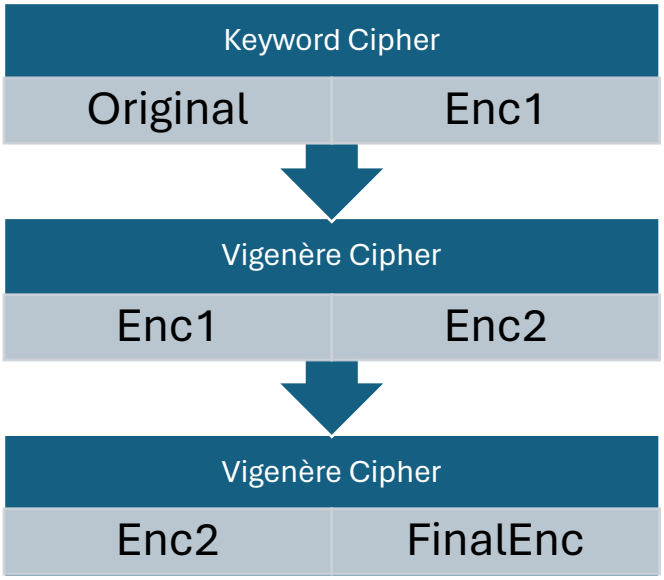
2. Final Encrypted Message:

"SUCCESS IS NOT ABOUT HOW FAST YOU RUN OR HOW HIGH YOU CLIMB, BUT HOW WELL YOU BOUNCE."

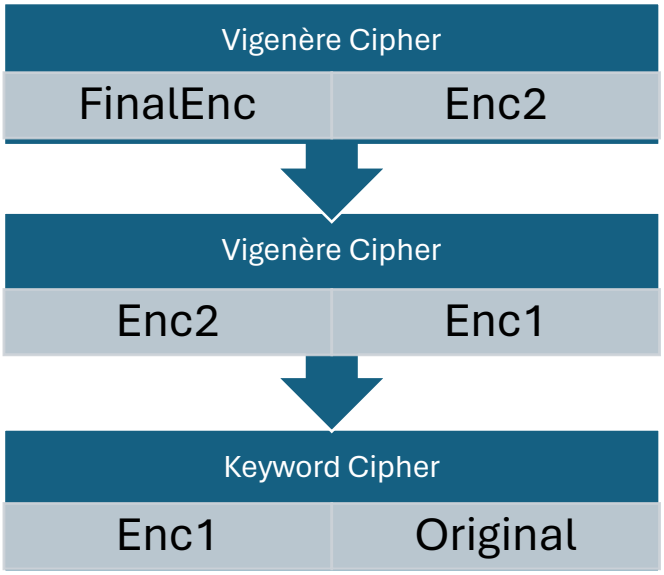
3. Approach:

To get the Final Decrypted message I need to start decrypting from layer 3 and with the help of that decrypted message, I will decrypt the message for layer 2 and similarly for layer 1.

Below figure can help to understand the nomenclature used in my solution



For Encryption



For Decryption

To solve this problem two main steps taken at every layer:

1. **Understanding the dynamics or nature of algorithms.**
2. **How we can undo their effect in encrypted messages.**

Step – 1

FinalEnc is obtained by encrypting Enc2 using Vigenère Cipher algorithm. After looking carefully one can conclude that Keyword is repeatedly taken as window and this algorithm only shifts the character of our text by index number of corresponding keyword's character in alphabetical order.

```
result = input("Enter the result string: ")
input_str = input("Enter the input string: ")

key = list(input_str)

for i in range(len(result)):
    if not(input_str[i].isalpha()):
        continue
    key[i] = chr((ord(result[i]) - ord(input_str[i]) + 26) % 26 + ord('A'))

print("Decrypted key:", "".join(key))
```

I tried to calculate shift by difference between FinalEnc and Partial Enc2 using shift.py (distance between character is shift) with which I should get a pattern of repeating keyword since Enc2 is not complete I got this type of message.

****O*N**N *T **T N***O **O *N*T **T **T *O **O *N*T **T ****O, **O **O **OT **T ***NO**"**

From The Nature of shift it is easy to guess that the keyword is not.

I have utilized this not keyword to in Vigenère Cipher algorithm to get the full version of Enc2.

"WTDEGRJ ZW MFL BEFMX FFO HWJL DNL JYM FJ KNN YLDX RST DCLKW, XYS XGA VTCO YFM JNLFQB."

Step – 2:

Enc2 is obtained by encrypting Enc1 using Vigenère Cipher algorithm. Like step1, I successfully found Enc1.

"***AS *F **T ***TF **T *A*T **S **A *T **S T**S **A ****S, **A **F *S*F **T F***F**"**

One can be obvious from repeating nature that our keyword will be FAST and Enc1 will be:

"RTLLBRR GR MNS WENTS FNV CWRS YNT QTM NQ FNV FGDF YNT LJGKE, ETS FNV VBJJ YNT ENTMLB."

Step – 3:

Enc1 is obtained by encrypting Original Message using Keyword Cipher algorithm. By carefully observing algorithm I have observed that the modified key contains all the letter of alphabets with initial alphabets is key without any duplicates and later characters in alphabetical order.

Briefly We are just replacing the characters of our original text with characters present at its alphabetical index in modified key.

Another thing I know is that FAST and NOT are part of our Original Message.

The only four-letter word with all different characters is CWRS. From this I got the values at some indexes and with help of that further got information about first word that it is SUCESSS and doing this process predicting indexes help me to get initial three keyword which is acting as index.