Homework Number: Homework 2

Name: Tycho Halpern

ECN Login: thalper

Due Date: January 27, 2022

**Problem 1**

Description of Encryption:

I looked at the notes from lecture 3 and created a loop that loops through each of the generated round keys and follows the flow chart on page 21. For each of the boxes in the chart, I used the code provided in lecture to complete each step. After I looped through all of the round keys for a generated block, I added the output LE and RE to my final output. After all blocks were encrypted, I wrote the final output to the output file.

Encryption output:



Description of Decryption:

I copy and pasted my encryption algorithm, changed the file names, and looped through the round keys in reverse order. Then I wrote the decrypted message to the output file.

Decryption output:

Smartphone devices from the likes of Google, LG, OnePlus, Samsung and Xiaomi are in danger of compromise by cyber criminals after 400 vulnerable code sections were uncovered on Qualcomm's Snapdragon digital signal processor (DSP) chip, which runs on over 40% of the global Android estate. The vulnerabilities were uncovered by Check Point, which said that to exploit the vulnerabilities, a malicious actor would merely need to convince their target to install a simple, benign application with no permissions at all.The vulnerabilities leave affected smartphones at risk of being taken over and used to spy on and track their users, having malware and other malicious code installed and hidden, and even being bricked outright, said Yaniv Balmas, Check Point's head of cyber research. Although they have been responsibly disclosed to Qualcomm, which has acknowledged them, informed the relevant suppliers and issued a number of alerts - CVE-2020-11201, CVE-2020-11202, CVE-2020-11206, CVE-2020-11207, CVE-2020-11208 and CVE-2020-11209 - Balmas warned that the sheer scale of the problem could take months or even years to fix.

**Problem 2**

Description:

I copy and pasted my entire file from the DES\_text.py file, then deleted the decryption function and updated main. I then changed the sys.argv arguments in the encrypt function to match what the input would be. I then changed the read and write parameters of the files to be binary and changed the final bitvector write to file method. I also needed to add a few lines of code to handle the header at the beginning of the input file.

Converted output to JPG:

A picture containing fabric

Description automatically generated

Raw Output:

P6

155 51

255

ϓߘ]+�a8=����CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe���CIe0�L