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:

```
c6d80665196641a1bba15e161d81395b152197d2dcade2d203105c559383da6a81892f0cfba8f349aaab0
edfbbc420a47af2e1fce559a2163a520e9fc00211e2f73ea73d511cd1e17dc11052e31ed2996e755b2af37e
79abcdb0f0989680d1ccde13f9858462d0575139cdd53c61d0335132ad498d7b81c1cb8217b731760c781
04d829cbf0ece166b0fe2d15cc49dc863716fdafab205e3642c3cbfbdc1339c9ef905b38e2e36b2c4dfda1bc
00d31c0ebea00311a47c6e54d7642f8d3de4396fe1ba0ee3309585713612c1351a8546bb0b18dd66d2dee
64554d22046309e59699975d414e1d4dd2ffc1d052af0f5ae10392195cf8351a6d23010e07750ef4e1c6ed
16d52fafa8d632b1cdd20a4051ec5961a50f8ecbdaeefce77b9c83effe16af00c301fab16eef790a756a3cb6
b97fdcb49467fa265a119ba81792231ae15ab97140aad0e1e2e2843feaea9723793f4ae46ee68884ce855e
0de291f63f723e32058fb537b99435db0035e0ea8b0a44516d3c07860c11f31ce612331b1d32dd0df5aef5
c75f59a8a16b3e743081f4da8a70a3b7540061ca8a741b39d1d54f26aa9b205d59f1e6f72a2a849ea3c3af9
f0434f8ecac2aa556b0a77208a50eed8fd7df099e5956c3bc88137c28a3ebcf4baa189b616987314484643c
d7f23bb9d314d4495f096d918131c6125ea36ecea4d24fd56b1caf927fb9e2ac224bca4d1907e54ef31c4f5
e39bb9c6bc3b60bd6dda0d2c1e1983d81952585909b01ed9020148ef776977cde0898495cdefd509fc654
dd5b87c994aa8e122b12caaa80fccb6c9f15656275749ba1bfe006aeab6993c92cd409c7fb28f6feb345590
730a0ac970872ad95895f69673b328760b4c1e1d58e28539e117d8f288e18c5da7eb84e7db47f68ddc87b
cc02aeb27e15ae90ed20ecfe9c827073e6d7c56e15cef4d3565f15a7cba6a36f8e7d9e1ee51ddebd3d0a8bc
5a7b3fdc8e4aa4113c6ebe6c7bc0c2f1b2afe5159efbfd9b6e03124422dcb9c476a1f1ab40c796e12af30669
82330065b18b7e1149b7144db2f03b4c876f5139370752d121eb78e6f20c409b0e92e555cf6d87907dd50
222e5531a37c58dcc61c630cbfcc0d53f61bddce64f2178fabdf7b02f279d3f1d8d2103c70909ec5fe143cc9
aaeef07fe323cb803646cc5c687bbe5d1eb071a72ce6d92601e80c2e7290bb1313ceaa93c2af42fd8b4f430
aa371eb123e490bcff9e18d4407db1607f3b655e02b0883556d40f4edf3d63439f91de6112e388f534be43
e6c540178f58d54ebd0be617235e6c8d2d9e0850a46f51e168993973532f7e97d2990063788531d0c0831
bcb232f7e97d29900637cefc0c7b39ebd4dc32f7e97d29900637fc33e6e02f4bafd532f7e97d299006374bc
a1971770d1a6632f7e97d299006371bb599c88aec1d163844e9837a4ba27c4e805bd8017d74050ec365b6
e9192729ecd9443195fadea4dfeb06aefe0c2cb3b8fc0ce0e806d6df42d85a4cef1c2852fcd77dc415d49438
```

```
2cd8dfbd854b2578c8f0970e8bc5e57264a3ef16b730afd81235ae66053429bb9323e912d22b7d06e19c4b3c9259319d
```

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:

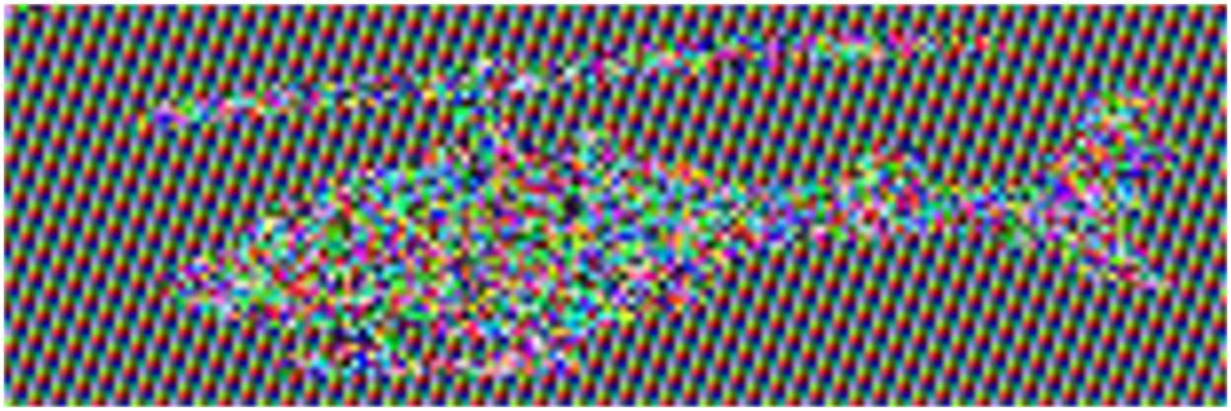
Smartphone devices from the likes of Google, LG, OnePlus, Samsung and Xiaomi are in danger of compromise by cyber criminals after 400 vulnerable code sections were uncovered on Qualcomm's Snapdragon digital signal processor (DSP) chip, which runs on over 40% of the global Android estate. The vulnerabilities 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:



Raw Output:

```
P6

155 51

255

Ύɯ]+  �
```

```
a 8   =�  ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   ���Cle   �
��Cle   ���Cle  0�L
```