**ECE 404 – HW 2**

**Saumya Navani**

**Problem 1:**

The text encryption DES script reads a message from the specified input file and uses the 64-bit DES key (provided in another input file) to encrypt the message and store it in another file as encrypted content. The encryption script also pads the input with zeros if the plaintext bit size is not divisible by the DES block size. It applies permutation (key permutation 2) to the key used and generates the round key, the two halves of which go to the next round for the same process 16 times.

The encryption key is generated using key permutation 1 using the eight input characters as the key. The bit vector to be encrypted is divided into blocks, which is further divided into two halves. The right half is XORed with the first round-key in the round key list, and then permutated with the P box permutation to produce the output encrypted content, which is written to the output file.

The decryption works in a similar way, but the contents are XORed with the last round key in the beginning along with the application of permutations used in the encryption algorithm, which effectively reverses the encryption for DES.

**Examples:**

**Encryption key:**

zoomzoom

**Message:**

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.

**Encrypted message:**



**Decrypted message:**

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:**

The image encryption algorithm is extremely similar to the text encryption algorithm. The only difference is that the ppm file consists of a header, which needs to be processed before the encryption starts to the output file. The encryption algorithm itself is almost the same, except it only runs after reading three of the top lines from the input file.

**Examples:**

**Encryption key:**

zoomzoom

**Input image:**

A picture containing text, helicopter, aircraft

Description automatically generated

**Decrypted image:**

A picture containing fabric

Description automatically generated