Chan Ng Cashin
ECE 404
HW 2

**Problem 1:**

Description:

In my DES.py file I completed problem one by implementing my own encrypt and decrypt functions. I used the s-boxes, permutation boxes, a shift for round key generation list, substitution function and round key generation function provided by Lecture 3 to encrypt and decrypt the message file. The encryption function goes through the file blocks of message.txt and implements the Feistel function to the current block of plaintext by the number of rounds generated by the round generation function given in lecture 3. This was debugged by using the first_round.txt file provided in the homework file. By the end an encryption file is generated from message.txt. For the decryption function the same procedure was used but reversed as described in the DES section in Lecture 3. In the main of my DES class file there is an if statement handling the arguments inputted by the user when running the file.

encrypt.txt:

0c46d7cd5b7efc319691493448bb36733af8d5e4da962e15e85db329c5031857a154f62cbfb7c82
d298c9456ef29adb8e86cc51ae7f025097f513677406336598e0f3f1f0c5ecaf0b55649222b19a27
da886fa8c4d2b9e0e88a2745b99e6bbb4658cd9fd3606e05d11919eddd39723e333aa813ebd9a9
ae6810271c9d634cba829e1b7a82bd994073d054e62a79d8bbd1ebe00d2288b8c05b0f4d5ec79
9e3f7d5db8b04a23106d0151c6fea8bd1826a92e611e73a1bc4949ed703d0174516196ef7faed8a
411c7efc9b11b6b44fa864c7692c80a7ac2dc6f5d467e8b6588845f5c8c1f4493c9d94f3af8d5e4da
962e1580d4d42e93e281c6aab31eec856fead76a96c9d84c4a3fce61ded79fdd9a943cb446a58d8
81c211b5ba21a1dc81659123283460d36ca20cba580ebd51188824724ec416aebeff0d01d2be94
2433af7679b2d5d55a4b8c931151283e60d8e99e90701d26b28a139a46c209a2a93f6250b902ff2
5ee8aa0f56ea075b13c3ca4dbd985da7338582b48b412c33ce01dc4bcbb7cb9a3e905deb0caf473
c5b801aa2872c62d06d015b9b7aba88a48889f7b2cd6602ec4311480ef124adff91a834630b41c2
f4d29769ca093ec31ee4779264af3a6ecd51cc098d3acfb1c5fdeff53a694ea26c872220eb2c75894
e9e10b1beba091a61279d20154b4c46eda9c3d6b6df07eaaa1dc93f98246eefeb34d8ea72bef755
8055080ed4d73afe523bb6723e79ba8eae813579fc2f74a2a64cdf2484bc8267b7c0b0cc28ab5ba
21a1dc8165912c99d911d997a8e829853c23bcd8681544a3bc6ea2a56ae5844873d757d272114
000874af4a2adff08a824e0c1b8dbbb72a02f86fb4c95668b5bdcb5c3c3d3fc3545d14e6459f7d2b
7050edc71e4c58ad593b284e6fee59f41bf13fddf342694530d4e70c288d9a61e3515a37674fbb7
bc98730a9d700b5c8d332cc75c1a41e39a2ae33cb95d43e92b3f168a97488f8a7cfbe9993019259
ed8cfdc1cddb6e60cb40803c3e931e1278d85ae80815e10b3a7496e30b24e6b996e2400cad3f39
99fdab7d3bcf897a9a376e85932b9d711e634dcf3a756b2a93165df4a192bf0d0a271415986d5e1
dbd019250095819c5e0b55b095bbb94a00a009e6c9e6a998598c2f98075a8861a43710dbd6cb6
3a94d66c2d4d779ead4200ef8f58a2d2c3ab25ccd2fec9c8489ab4b8bb1c95b3b7da5d9b5eb50e9
733bdf981112601bec9feb807ef32f154f825a870d7ff1ec081545d343c085bb0bc7b2bee8954104

88ad30eaec469d6170b2a502a616b4b55e49e7ab3517db4259cc90e91b70e232ec1f8a1ea85a1b
4d4c63fa94fc1b80e7005183f54ace18926dbf3330252ca26895d60dd71

decrypt.txt

Scuderia Ferrari is the racing division of luxury Italian auto manufacturer Ferrari and the racing team that competes in Formula One racing. The team is also known by the nickname "The Prancing Horse", in reference to their logo. It is the oldest surviving and most successful Formula One team, having competed in every world championship since the 1950 Formula One season. The team was founded by Enzo Ferrari, initially to race cars produced by Alfa Romeo. By 1947 Ferrari had begun building its own cars. Among its important achievements outside Formula One are winning the World Sportscar Championship, 24 Hours of Le Mans, 24 Hours of Spa, 24 Hours of Daytona, 12 Hours of Sebring, Bathurst 12 Hour, races for Grand tourer cars and racing on road courses of the Targa Florio, the Mille Miglia and the Carrera Panamericana. The team is also known for its passionate support base, known as the tifosi. The Italian Grand Prix at Monza is regarded as the team's home race.

**Problem 2:**

Description:

For Problem 2 I simply added an encrypt_img function to the DES class that handled the encryption of the image.ppm file. The only difference between this function and the encrypt function in the same class is how the input file is read and how the output file is written. To read the .ppm file the BitVector more_to_read and read_bits_from_bitvector() boolean and function were used to iterate through the file and construct a bitvector for the plaintext. Another iteration was used when reading this file to not count the header of the .ppm file in the bit vector. From here the same Feistel function was used to encrypt the image file. Instead of writing a hex encryption to the output file the bits were written to it. Below is the encrypted image output file.

image_enc.ppm: