Homework Number: 2

Name: Andrew Wu

ECN Login: wu1795

Due Date: 1/25/24

Problem 1:

For the encrypt part, I turned the message file into a bitvector and then generated the round keys by calling get_encryption_key and generate_round_keys. I then read the bitvector by 64 bits, adding an if loop that exits the loop if there is no more to read. I then padded the bitvector to ensure that the file is of proper size. I then divide the bitvector into two, and then for each of the 16 round keys, I coded up the DEA process. I used expansion_permutation to expand the right half of the bitvector from 32 bits to 48 bits, xor'd the expanded right half of the bitvector with the round key of that round and used the substitute function to substitute the output with the s boxes. I then used the output to permutate with the p box, and then xor'd that output with the left half of the input to form the new right half, with the new left half being the original right half of the bitvector. After all the rounds were done, I combined the right and left halves of the output and wrote the final output in hex to the outfile, creating the cipher text below.

For the decrypt part, I first opened the encrypted file and converted it from hex into a bitvector. I then generated the round keys and reversed them, since decryption happens in the reverse order of encryption. I then created blocks of 64 bits from the bitvector and then repeated the same process that I did for encryption. I start with adding an if loop to exit once there was no more to read, and then ran through the DEA process after the loop. After all the rounds of DEA, I wrote the output in ASCII to the outfile, which created the decrypted text below.

Cipher text:

0c46d7cd5b7efc319691493448bb36733af8d5e4da962e15e85db329c5031857a154f62cbfb7c82d
298c9456ef29adb8e86cc51ae7f025097f513677406336598e0f3f1f0c5ecaf0b55649222b19a27da8
86fa8c4d2b9e0e88a2745b99e6bbb4658cd9fd3606e05d11919eddd39723e333aa813ebd9a9ae681
0271c9d634cba829e1b7a82bd994073d054e62a79d8bbd1ebe00d2288b8c05b0f4d5ec799e3f7d5d
b8b04a23106d0151c6fea8bd1826a92e611e73a1bc4949ed703d0174516196ef7faed8a411c7efc9b
11b6b44fa864c7692c80a7ac2dc6f5d467e8b6588845f5c8c1f4493c9d94f3af8d5e4da962e1580d4
d42e93e281c6aab31eec856fead76a96c9d84c4a3fce61ded79fdd9a943cb446a58d881c211b5ba21
a1dc81659123283460d36ca20cba580ebd51188824724ec416aebeff0d01d2be942433af7679b2d5
d55a4b8c931151283e60d8e99e90701d26b28a139a46c209a2a93f6250b902ff25ee8aa0f56ea075b
13c3ca4dbd985da7338582b48b412c33ce01dc4bcbb7cb9a3e905deb0caf473c5b801aa2872c62d0
6d015b9b7aba88a48889f7b2cd6602ec4311480ef124adff91a834630b41c2f4d29769ca093ec31ee
4779264af3a6ecd51cc098d3acfb1c5fdeff53a694ea26c872220eb2c75894e9e10b1beba091a61279
d20154b4c46eda9c3d6b6df07eaaa1dc93f98246eefeb34d8ea72bef7558055080ed4d73afe523bb6
723e79ba8eae813579fc2f74a2a64cdf2484bc8267b7c0b0cc28ab5ba21a1dc8165912c99d911d997
a8e829853c23bcd8681544a3bc6ea2a56ae5844873d757d272114000874af4a2adff08a824e0c1b8d

bbb72a02f86fb4c95668b5bdcb5c3c3d3fc3545d14e6459f7d2b7050edc71e4c58ad593b284e6fee5
9f41bf13fddf342694530d4e70c288d9a61e3515a37674fbb7bc98730a9d700b5c8d332cc75c1a41e
39a2ae33cb95d43e92b3f168a97488f8a7cfbe9993019259ed8cfdc1cddb6e60cb40803c3e931e127
8d85ae80815e10b3a7496e30b24e6b996e2400cad3f3999fdab7d3bcf897a9a376e85932b9d711e6
34dcf3a756b2a93165df4a192bf0d0a271415986d5e1dbd019250095819c5e0b55b095bbb94a00a0
09e6c9e6a998598c2f98075a8861a43710dbd6cb63a94d66c2d4d779ead4200ef8f58a2d2c3ab25cc
d2fec9c8489ab4b8bb1c95b3b7da5d9b5eb50e9733bdf981112601bec9feb807ef32f154f825a870d
7ff1ec081545d343c085bb0bc7b2bee895410488ad30eaec469d6170b2a502a616b4b55e49e7ab35
17db4259cc90e91b70e232ec1f8a1ea85a1b4d4c63fa94fc1b80e7005183f54ace18926dbf3330252
ca26895d60dd71

Decrypted text:

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:

For problem 2, I followed the same method that I used for the encryption problem in problem 1. However, since the first three lines of the image were used as a header, I first created a for loop that read the first three lines and wrote them directly to the output. I then followed the same method I used for encryption above and obtained the image of a helicopter as my output.