Anish Laddha
Professor Avinash Kak
ECE 404
25 January 2024

Homework 2

Problem 1: Encryption and Decryption

- For encryption and decryption, we follow similar steps.
- First, we pad the plaintext BitVector so that the number of bits are divisible by 64, as the Feistel structure/function requires an input of 64 bits.
    - This is only for encryption, but a file encrypted this way may have extra bits/chars at the end as special characters due to the padding
- We then remove the parity bits from the key, to get a 56 bit key. This is used to permute the round keys.
- Then, we loop through 64-bit chunks of the plaintext bitvector. For each chunk, we will loop through 16 stages of the Feistel structure. At each step, we split it into a right and a left.
- The new left side will be the previous right side.
- The previous right is then expanded to 48 bits through a permutation
- It is XORed with the round key for that structure,
    - (NOTE: for encryption, you go from key0 -> key 15, while decryption is the opposite),
- Then its split into 6-bit chunks to be substituted using the s-boxes
- The result is reconstructed into a 32 bit vector.
- Finally, the chunk is XORed with the original left chunk and becomes the new right chunk.
- This process is repeated 15 more times, with the only difference being the round key changing
- Finally, the resulting 64-bit chunk is appended to the ciphered (or deciphered, if doing decryption) bit vector, which is dumped into the output file when done.

Original 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.

Ciphered Text (Hex)

```
0c46d7cd5b7efc319691493448bb36733af8d5e4da962e15e85db329c5031857a154f62cbfb7c82d298c9456ef29a
db8e86cc51ae7f025097f513677406336598e0f3f1f0c5ecaf0b55649222b19a27da886fa8c4d2b9e0e88a2745b99e
6bbb4658cd9fd3606e05d11919eddd39723e333aa813ebd9a9ae6810271c9d634cba829e1b7a82bd994073d054e6
2a79d8bbd1ebe00d2288b8c05b0f4d5ec799e3f7d5db8b04a23106d0151c6fea8bd1826a92e611e73a1bc4949ed7
03d0174516196ef7faed8a411c7efc9b11b6b44fa864c7692c80a7ac2dc6f5d467e8b6588845f5c8c1f4493c9d94f3
af8d5e4da962e1580d4d42e93e281c6aab31eec856fead76a96c9d84c4a3fce61ded79fdd9a943cb446a58d881c211
b5ba21a1dc81659123283460d36ca20cba580ebd51188824724ec416aebeff0d01d2be942433af7679b2d5d55a4b
8c931151283e60d8e99e90701d26b28a139a46c209a2a93f6250b902ff25ee8aa0f56ea075b13c3ca4dbd985da733
8582b48b412c33ce01dc4bcbb7cb9a3e905deb0caf473c5b801aa2872c62d06d015b9b7aba88a48889f7b2cd6602
ec4311480ef124adff91a834630b41c2f4d29769ca093ec31ee4779264af3a6ecd51cc098d3acfb1c5fdeff53a694ea
26c872220eb2c75894e9e10b1beba091a61279d20154b4c46eda9c3d6b6df07eaaa1dc93f98246eefeb34d8ea72be
f7558055080ed4d73afe523bb6723e79ba8eae813579fc2f74a2a64cdf2484bc8267b7c0b0cc28ab5ba21a1dc8165
912c99d911d997a8e829853c23bcd8681544a3bc6ea2a56ae5844873d757d272114000874af4a2adff08a824e0c1b
8dbbb72a02f86fb4c95668b5bdcb5c3c3d3fc3545d14e6459f7d2b7050edc71e4c58ad593b284e6fee59f41bf13fdd
f342694530d4e70c288d9a61e3515a37674fbb7bc98730a9d700b5c8d332cc75c1a41e39a2ae33cb95d43e92b3f16
8a97488f8a7cfbe9993019259ed8cfdc1cddb6e60cb40803c3e931e1278d85ae80815e10b3a7496e30b24e6b996e2
400cad3f3999fdab7d3bcf897a9a376e85932b9d711e634dcf3a756b2a93165df4a192bf0d0a271415986d5e1dbd0
19250095819c5e0b55b095bbb94a00a009e6c9e6a998598c2f98075a8861a43710dbd6cb63a94d66c2d4d779ead4
200ef8f58a2d2c3ab25ccd2fec9c8489ab4b8bb1c95b3b7da5d9b5eb50e9733bdf981112601bec9feb807ef32f154f
825a870d7ff1ec081545d343c085bb0bc7b2bee895410488ad30eaec469d6170b2a502a616b4b55e49e7ab3517db
4259cc90e91b70e232ec1f8a1ea85a1b4d4c63fa94fc1b80e7005183f54ace18926dbf3330252ca26895d60dd71
```

Decrypted

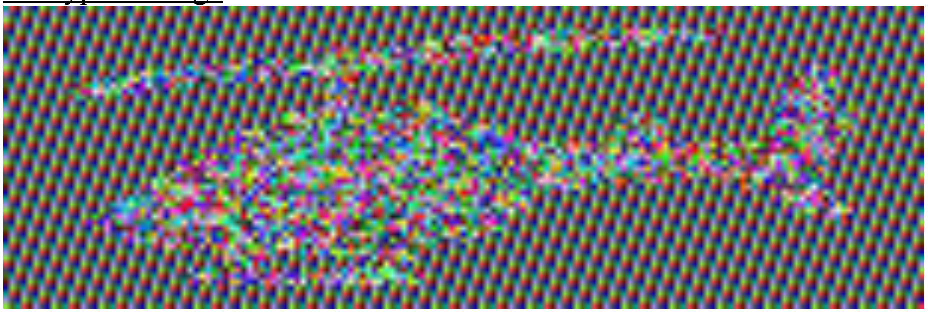
Scuderia Ferrari is the racing division of luxury Italian auto manufacturer Ferrari and the racing team that competes in Formula One racing. The team is also known by the nickname "The Prancing Horse", in reference to their logo. It is the oldest surviving and most successful Formula One team, having 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: Encrypting a PPM file

To encrypt a ppm file, we take very similar steps. However, the only difference is that we must take the previous steps after removing the header, which is to be added on later. I did this by searching for 3 new line characters after going byte by byte through the BitVector class, and then after I hit 3 newlines, everything before is the header and everything after is the actual data. Then I encrypt the data as mentioned previously, but before dumping it back into the output file I re-attach the header to the front.

Original Image:

Encrypted Image



As we can see, the block chunking that DES does makes the outline of the helicopter very clear.