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)



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.