Problem 1: I created a DES class that reads an 8-character key from a file, permutes it to 56 bits, and generates 16 round keys. The program encrypts and decrypts text files in 64-bit blocks using the standard DES Feistel structure in ECB mode. Each block is padded if necessary and transformed with the initial and final permutations, 16 Feistel rounds, and the correct key scheduling. The encrypted output is written as a single-line hex string, and decrypting with the same key recovers the original plaintext (after optionally removing trailing nulls).

HERE ARE THE ENCRYPTED AND DECRYPTED FILES

Encrypted.txt

7a08fda9cd024e96ad7e94117544cd6b67d3debfac2d93355c6e2e6c9426fcd2a838b1a3e9
4862f020863afa7af7759d024e125f241db9ba1dd8e7c3b2c77030261cc1c18afa0610f8fcb
ea5ef0dc244939969b76bcddd30a83e38214a375bda941a7921412b3b04f90e2825a6f34a
8ab84fb295ec757b2a3a04540997e568137984c5f0a7092eaf63d698f0224f1968a6af599b1
a5507acef1a14fb15a0e7c62277154f4f4b31ee3a6bad0b0d24dc85b69d0bcaddc32973d7f
0c8ce371907ecd57c602c4d2d5e9818582703ba4ffc94491a8430ffcbf4b99112751771eb4a
643c7b37ef1cf99b93ba04d4273d7c790a22adb1dea6f886b8818e14e468c2e1cbd13abf36
a9405443a6a560abfd83f61100efa3b05485b857a1a641e41fe2db5a39f479a63bd65a64c4
80a1c8cdf54d04ca4f8161ab104609aeea2c67bd42bb82304c4b3bdf7d34d7a852c7e801e
54ab9edc3e458e4afe7c218e75a4c7b2603ffc54150e2012444e3c9e15c8778748654c46ec
5fb11f7563636a269c8686755f918334371605229df7034fe470ebe0d3851de62de71aabf1a
75c15bea6cd3194b6b1e07ace5b526a817927146551c299ea77b5c678ee2e4df77205a873
9d0551c4ba80173286e0e96d5b11d8bd7bab41b20da2b00296b00e50dde2d0ef73f2a8e64
8de1f558db60a072946804be57a27d8138c2936ec5a9999fc133a12fca9a35431c9262dd05
f0d86eb985ecf33e2cf63a6422e4d59ff45e1350f7bcf981afcf80482f6e7f85cd262a5dc0307
88ac74113d551f0bdd6f486abe1ed1fd7ffaf478974de006a13efe61e9dbf3e625791766b248
a5486ea7482d5b278cd09f8f4d85e7f5fb2c58f4c62bedb8b7802b42d56ac17d5fefc13f9fc7
e2ef239225ac017c5b2b03e3a0cd5b7bd0350feade91b5032a53e215ac08e790ba7b1f2116
c369100fc677b4704442b4d21639e4bf7b0157a5ef23ce04f4405c11f98d4de9eefed4914f7
7a23047727e25d2199fc6b4b47b76cf8781c31e87f786950385ea4ffc16744358e931e85b1a
febe2989e8d75791e3241f5ec8f8da51cd10d726db8d568e9a7b217fd1a8ed7c0f1198a02a
6d140f90e2825a6f34a8ab84fb295ec757b2a054ac9a133aad4c8f365911d9665f7ac021c38
dc86d2393d13bcc52f8372f240556cfb14a8760fff9c74b4b5811f06552b9a86686193a25c2
b393a5c4dc59525745b83e4b3a053d406fa0e1e91404a59af995712adcb3fbb7cefe8668c0
090d3401068204f363b0d2c2fe258e8c5653b3cf13a2a49466b85972b823e001b7cff25f88d
7db022d8dab6d26b524cd5a97f868458aedb017bd499449c195a6c2beb5169687df1ce6aa
4

Decrypted.txt

The Lord of the Rings franchise, created by J.R.R. Tolkien, is a high fantasy epic set in the fictional world of Middle-earth. It follows the struggle to destroy the One Ring, a powerful artifact created by the dark lord Sauron to control the world. The central story revolves around Frodo Baggins, a hobbit, and his journey to Mount Doom, where the Ring can be destroyed. Along the way, he is aided by the Fellowship of the Ring, including Aragorn, Legolas, Gimli, Gandalf, and others. The franchise includes the original novels, a prequel called The Hobbit, and adaptations like Peter Jackson's critically acclaimed film trilogies, The Lord of the Rings and The Hobbit. It explores themes of friendship, sacrifice, the

corruption of power, and the battle between good and evil. The world of Middle-earth is richly detailed, featuring diverse cultures, languages, and histories, making it one of the most beloved and influential works in fantasy literature and film.

Problem 2: The same DES class is reused to encrypt the pixel data of a PPM file. After preserving the three-line header, the remaining bytes (image data) are read in 64-bit chunks, processed with the same DES ECB approach, and written back in binary. This produces an encrypted PPM file that maintains the correct header but garbles the image visually, demonstrating how ECB mode can still show large-scale patterns despite encrypting each block independently.

The Image