ECE 40400: Introduction to Computer Security

Spring 2024

Prateek Yashwant Jannu

Purdue University, West Lafayette

Professor: Dr. Avinash C Kak

Problem 1

∗ **Message.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.

∗ **Key.txt :** zoomzoom

∗ **Encrypted.txt :**

```
0c46d7cd5b7efc319691493448bb36733af8d5e4da962e15e85db329c5031857a154f62cbfb7c82d298c945
6ef29adb8e86cc51ae7f025097f513677406336598e0f3f1f0c5ecaf0b55649222b19a27da886fa8c4d2b9e0e
88a2745b99e6bbb4658cd9fd3606e05d11919eddd39723e333aa813ebd9a9ae6810271c9d634cba829e1b7a
82bd994073d054e62a79d8bbd1ebe00d2288b8c05b0f4d5ec799e3f7d5db8b04a23106d0151c6fea8bd1826
a92e611e73a1bc4949ed703d0174516196ef7faed8a411c7efc9b11b6b44fa864c7692c80a7ac2dc6f5d467e8
b6588845f5c8c1f4493c9d94f3af8d5e4da962e1580d4d42e93e281c6aab31eec856fead76a96c9d84c4a3fce
61ded79fdd9a943cb446a58d881c211b5ba21a1dc81659123283460d36ca20cba580ebd51188824724ec416
aebeff0d01d2be942433af7679b2d5d55a4b8c931151283e60d8e99e90701d26b28a139a46c209a2a93f6250
b902ff25ee8aa0f56ea075b13c3ca4dbd985da7338582b48b412c33ce01dc4bcbb7cb9a3e905deb0caf473c5
b801aa2872c62d06d015b9b7aba88a48889f7b2cd6602ec4311480ef124adff91a834630b41c2f4d29769ca0
93ec31ee4779264af3a6ecd51cc098d3acfb1c5fdeff53a694ea26c872220eb2c75894e9e10b1beba091a6127
9d20154b4c46eda9c3d6b6df07eaaa1dc93f98246eefeb34d8ea72bef7558055080ed4d73afe523bb6723e79
ba8eae813579fc2f74a2a64cdf2484bc8267b7c0b0cc28ab5ba21a1dc8165912c99d911d997a8e829853c23b
cd8681544a3bc6ea2a56ae5844873d757d272114000874af4a2adff08a824e0c1b8dbbb72a02f86fb4c95668
b5bdcb5c3c3d3fc3545d14e6459f7d2b7050edc71e4c58ad593b284e6fee59f41bf13fddf342694530d4e70c2
88d9a61e3515a37674fbb7bc98730a9d700b5c8d332cc75c1a41e39a2ae33cb95d43e92b3f168a97488f8a7c
fbe9993019259ed8cfdc1cddb6e60cb40803c3e931e1278d85ae80815e10b3a7496e30b24e6b996e2400cad
3f3999fdab7d3bcf897a9a376e85932b9d711e634dcf3a756b2a93165df4a192bf0d0a271415986d5e1dbd01
9250095819c5e0b55b095bbb94a00a009e6c9e6a998598c2f98075a8861a43710dbd6cb63a94d66c2d4d77
9ead4200ef8f58a2d2c3ab25ccd2fec9c8489ab4b8bb1c95b3b7da5d9b5eb50e9733bdf981112601bec9feb8
07ef32f154f825a870d7ff1ec081545d343c085bb0bc7b2bee895410488ad30eaec469d6170b2a502a616b4b
55e49e7ab3517db4259cc90e91b70e232ec1f8a1ea85a1b4d4c63fa94fc1b80e7005183f54ace18926dbf3330
252ca26895d60dd71
```

Decrypted.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.

Brief explanation:

1. Initializing all variables and checking the function

- The constructor initializes the instance variables, including the key, S-boxes, permutation boxes, and other variables.
- Reads the key from a file and converts it into a bit vector.
- Initializes S-boxes with predefined values.
- Specifies key permutation values and shifts for round key generation.
- Generates the round keys using the key permutation and shifts.
- Stores the round keys for later use.

2. Encrypt function

- Reads the message from the file and converts it into bit vectors.
- Divides the message into 64-bit blocks.
- For each block, performs the DES encryption rounds:
  - Expansion of the right half to 48 bits.
  - XOR with the round key.
  - Substitution using S-boxes.
  - Permutation using the P-box.
  - XOR with the left half.
  - Swap left and right halves for the next iteration.
- Concatenates the ciphertext blocks.
- Writes the encrypted result to the output file.

3. Decrypt function

- Reads the encrypted message from the file.
- Divides the encrypted message into 16-character (64-bit) blocks, as each hex character represents 4 bits.
- For each block, perform the DES decryption rounds in reverse order:
  - Expansion of the right half to 48 bits.

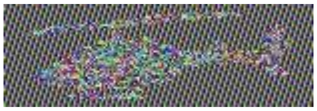
- XOR with the round key (used in reverse order).
- Substitution using S-boxes.
- Permutation using the P-box.
- XOR with the left half.
- Swap left and right halves for the next iteration.

- Concatenates the decrypted blocks.
- Converts the final bit vector into a text string.
- Writes the decrypted result to the output file.

Problem 2

1. **Image.ppm**

2. **Encoded image.ppm**



3. **Brief explanation**

1. PPM encryption

- Takes a message file and an output file as inputs.

- Reads the header lines (first three lines) from the message file and stores them in the `header_lines` list.

- Reads the remaining content of the message file as a BitVector named `message_string`.

- Initializes a block size of 64 bits.

- Initializes an empty BitVector named final for storing the final result.

- Parses through the message, processing 64-bit blocks at a time.

- For each block:

  - Performs the DES encryption rounds:

    - Expansion step to make the right half 48 bits.
    - XOR with the round key.
    - Substitution using S-boxes.
    - Permutation using the P-box.
    - XOR with the left half.
    - Swaps left and right halves for the next iteration.
  - Concatenates the processed block to the final bit vector.
- Opens the output file in binary write mode (`'wb'`).
- Writes each header line followed by a newline character to the output file.
- Writes the contents of the final bit vector to the output file.
- Closes the output file.