Q1 Team Name
0 Points

Turing

Q2 Commands
10 Points

List all the commands in sequence used from the start screen of this level to the end of the level. (Use -> to separate the commands)

go->dive->dive->back->pull->go->back->enter->wave->back->back->thrnxxtzy->read->134721542097659029845273957->c->read

Q3 CryptoSystem
5 Points

What cryptosystem was used at this level? Please be precise.

6 Round DES

Q4 Analysis
80 Points

Knowing which cryptosystem has been used at this level, give a detailed description of the cryptanalysis used to figure out the password. (Use Latex wherever required. If your solution is not readable, you will lose marks. If necessary, the file upload option in this question must be used TO SHARE IMAGES ONLY.)

Breaking of 6 round DES

After retrieving magical wand and freeing the spirit in level 3, we came back to the screen of level 4. when we typed 'read' command, a new screen appeared,we got few hints from panel text and typed ‘password’ as was instructed in the message. We then got the cipher-text - ‘kidloqgglgdrejdmmhqqjhrskhekkofq.Now We had to decrypt this ciphertext to cross level 4.

The spirit said that DES can be of 4 rounds or 6 rounds. We tried breaking the 6 round DES first.

Six round DES can be broken using two approaches:
1. Linear cryptanalysis
2. Differential cryptanalysis

we used differential cryptanalysis to break this DES. In this, the attacker creates various samples of plaintexts and get their corresponding ciphertexts.

IP(M) – (Initial Permutation) This is applied on the plaintext M that is to be encrypted.
IP_INV (M) – (Inverse of Initial Permutation) This is applied after all 6 rounds of DES are done on message M.
E (M) – (Expansion Box) Expand 32-bits of text M to 48-bits.
P (M) – This step permutes the 32-bit input M.
S - There are 8 S-boxes. Each S-box has 6-bit input and a 4-bit output.
PC1 - Key permutation that maps 64 bits of key to 56 bits and removes the parity bits
Shift - Shift that is performed on the key obtained as output of PC1
PC2 - Key permutation that maps 56 bits of Shift’s output to 48 bits

Approach used

We have used the characterstics: 40080000 04000000 and 00200008 00000400.

Concept of iterative characterstics is used. We have performed differential cryptanalyis using two 3-round characterstics.

It is given that 2 characters are of size 1 byte means 4 bits are used to represent one character. Since a block size is made up of 64 bits, we can have atmost 16 different characters in cipher text.

After analysing differnt ciphertexts, we inferred that those 16 characters are 'd' to 's'.

size of cipher text: 16 letters
size of plain text: 16 letters

Generating plaing text pairs

The differential characterstics 40 08 00 00 04 00 00 00 and 00 20 00 08 00 00 04 00 is used. Both of them have probablity 1/16.

Next, we generated total of 1000 plaintexts and cipher texts corresponding to each characterstics.

The plaintext pairs are generated such that their XOR is 00 00 80 10 00 00 40 00 (inverse initial permutation of characterstic 40 08 00 00 04 00 00 00).

The other plaintext pairs are generated such that their XOR is 00 00 08 01 00 10 00 00 (inverse initial permutation of characterstic 00 20 00 08 00 00 04 00).

All these pairs are stores in the files named 'plaintexts1.txt' and 'plaintexts2.txt'.

Generating cipher texts of plaintexts

Python library 'pexpect' is used to establish connection to the server. All the code related to this task is present in 'server.py' file.
The cipher texts are stored in 'ciphertexts1.txt' and 'ciphertexts2.txt'

Finding the 6th round key

We first converted the obtained ciphertexts to binary and then applied reverse final permutation on these binary ciphertexts to get L_6R_6 and $L_6^{'}R_6^{'}$. Both of them are the output of 6th round.

We know $R_5(=L_6)$ therefore using the values R_5 and $R_5^{'}$, we can calculate output of expansion box and input XOR of S-boxes for 6th round.

For the first characterstics, $L_5 = 04000000$ and for the second one, $L_5 = 00000400$.

Output of permutation will be $L_5 \oplus (R_6 \oplus R_6^{'})$. We get the output XOR of S-boxes for 6th round by applying inverse permutation on this.

Let,

$$E(R_5) = \alpha_1\alpha_2 \cdots \alpha_8$$
$$E(R_5^{'}) = \alpha_1'\alpha_2' \cdots \alpha_8'$$

$\beta_i' = \alpha_i' \oplus k_{6,i}, \text{where } |\alpha_i| = 6 = |\alpha_i'|$
and
$k_6 = k_{6,1}k_{6,2} \cdots k_{6,8}$
at this point, we know
$\alpha_i, \alpha_i', \beta_i \oplus \beta_i' \text{ and } \gamma_i \oplus \gamma_i'$

We created a 8 * 64 key matrix to store the number of times a key $k \in [1, 64]$ satisfies the possibility of being a key to S_i box, where $i \in [1, 8]$.

Now set X_i = $(\beta, \beta')|\beta \oplus \beta' = \beta_i \oplus \beta_i'$
and
$S(\beta) \oplus S(\beta') = \gamma_i \oplus \gamma_i'$

Then, we found the key k, such that $\alpha_i \oplus k = \beta$ and $(\beta, \beta') \in X_i$ for some β'.

For all the keys k which satisfied this condition for S_i box,

we incremented their count in the key matrix i.e. key_matrix[i][k] was incremented.

After performing the above analysis to find the keys, we obtained the following results for characteristic 40 08 00 00 04 00 00 004008000004000000:

S-box Key Max_Key_Frequency Mean_Key_Frequency
S1 45 93 62
S2 51 211 70
S3 37 97 64
S4 40 87 64
S5 21 113 69
S6 22 193 67
S7 12 126 65
S8 54 135 68

For this characteristic, in round 4, XOR will be zero for S2, S5, S6, S7 and S8. Therefore, in round 6 these S-boxes will give the corresponding key bits of K_6
6

Also, it can be observed that a significant difference is seen in the maximum key frequency and mean key frequency for these S-boxes which further assures of these key values being correct. We proceeded by taking the key bits for S2, S5, S6, S7 and S8 boxes as 51, 23, 52, 28 and 54 respectively.

The above analysis gave the following results for characteristic 00 20 00 08 00 00 04 0000020000800000400:

S-box Key Max_Key_Frequency Mean_Key_Frequency
S1 45 90 63
S2 51 99 65
S3 37 93 64
S4 7 191 70
S5 21 117 68
S6 22 180 70
S7 12 95 64

S8 39 83 64

For this characteristic, in round 4, XOR will be zero for S1, S2, S4, S5 and S6. Therefore, in round 6 these S-boxes will give the corresponding key bits of K_6

Also, it can be observed that a significant difference is seen in the maximum key frequency and mean key frequency for these S-boxes. We proceeded by taking the key bits for S1, S2, S4, S5 and S6 boxes as 45, 51, 7,23 and 52 respectively.

Both the characteristics have S2, S5 and S6 as common S-boxes and we obtained same key values for these three S-boxes which further verified that our computations so far are correct.

Therefore, we proceeded by taking key values for S1, S2, S4, S5, S6, S7 and S8 as 45, 51, 7, 23, 52, 28 and 54 for round key K_6K
6

Thus, at this point we know 42 bits of the 56 bit key.

Step 4: Extracting the actual key from the kno

We will apply the key scheduling algorithm and obtain the actual positions of the 42 known bits in the original 56 bits key and we get:

X11XX1XX01011X100XX11X11000X0000010X11100010X11X110
1X011 (let's call it a 'Master Key')
here X means the bit is not known at that position

Now, we will have 14 bits which are not known and for these unknown bits of key we iterate through all 2^{14} possible permutations of the key, by doing this we will get the full correct key.

we choose plaintext = ffffffff ffffffff and,
ciphertext = nfmmssmq sqqskifi

we then performed 6 round DES encryption. The key which encrypts this plaintext and produce the correct ciphertext is the real key. we finally obtained the following key :

Actual 56 Bit Key =
01101110010111100111101100000000010011100010111111011011

After obtaining the 56 bit key, we can obtain the 48 bit round key for each round.

Final step: password decryption

-The ciphertext corresponding to our password is “kidloqgglgdrejdmmhqqjhrskhekkofq”,so to obtain the password we performed decryption on this ciphertext. This ciphertext consists of 32 characters and since each character corressponds to 4 bits, so this is a 128 bit string, and as we know one block in DES is 64 bit so, it makes 2 blocks of DES ciphertext. As per our mapping this is {117,8,189,51,131,14,22,9,148,221,100,239,116,23,123,45}

- Now we have obtained our key, we perform decryption on this ciphertext by considering 16 characters (=64 bits) at a time using $decrypt.cpp$, which uses decryption function of DES for 6 rounds.

-The resultant plaintext is - osuvicekiv000000. there are zeros at the end so We removed them as they must have been used for padding.

- on entering the plaintext ‘osuvicekiv’ in the game we were directed to the next level.

No files uploaded

Q5 Password
5 Points

What was the password used to clear this level?

Q6 Codes

0 Points

Unlike previous assignments, this time it is MANDATORY that you upload the codes used in the cryptanalysis. If you fail to do so, you will be given 0 marks for the entire assignment.

Assignment 4.zip Download

```
1  Large file hidden. You can download it using the button above.
```

Assignment 4

GRADED

48 MINUTES LATE

GROUP
Dinkar Tewari
Rohit kushwah
Deepak Raj
View or edit group

TOTAL POINTS
35 / 100 pts

QUESTION 1
Team Name **-10** / 0 pts

QUESTION 2
Commands **10** / 10 pts

QUESTION 3
CryptoSystem **5** / 5 pts

QUESTION 4

Analysis **80** / 80 pts

QUESTION 5

Password **5** / 5 pts

QUESTION 6

Codes **-55** / 0 pts