Q1 Team Name

0 Points

Goldfish

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->back->back->go->wave->back->back->thrnxxtzy->read->13472154209765902984527395 7->c->read

Q3 CryptoSystem

5 Points

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

6 Round DES (Block Cipher)

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

Assignment 4 — GRADED

GROUP
Jeet Sarangi
Akshay Kumar Chittora
Alok Kumar Trivedi
View or edit group

TOTAL POINTS
45 / 100 pts

QUESTION 1
Team Name — **0** / 0 pts

QUESTION 2
Commands — **10** / 10 pts

QUESTION 3
CryptoSystem — **5** / 5 pts

QUESTION 4

solution is not readable, you will lose marks. If necessary, the file upload option in this question must be used TO SHARE IMAGES ONLY.)

While exploring we first had to go back and release the spirit from level 3 and then came to level 4 after which we got the magic wall where we realised it as whatever we write there it gets converted to some ciphered text hence we got a hint here.
.We got several hints about the cipher being DES .It was mentioned that cipher could be 4,6 or 10 round DES. As 4 round DES would be very easy to break and 10 round DES be equally difficult, so we went ahead with 6th round DES and used code provided in files Computing Xors for rounds.ipynb,Finding Round 6 Keys.ipynb , Final_key_and_all_roundkey.ipynb and des.cpp to decipher it.
We performed chosen plain text method to decipher the 6 round DES.
- We used two 3 round characteristics to perform differntial cryptanalysis.The characteristics used are 40080000 04000000 and 00200008 00000400.
- As one byte used to store two characters, therefore 4 bits are required for 1 character.hence 4 bits can represent 16 different character. we studied different cipher text and concluded that letters from 'd' to 's' are used .
We mapped each character to a 4 digit bit using following mapping system
{d : 0000, e : 0001, f: 0010, g : 0011, h : 0100, i : 0101, j : 0110, k : 0111, l: 1000, m : 1001, n : 1010, o : 1011, p : 1100, q : 1101, r : 1110, s : 1111},
The input and output size of one DES Block is 64 bits, which means 16 charchters. Hence we will take plaintexts of size 16 letter

Generation of Plaintext Pairs

The differntial characterstic with 40080000 04000000 with probability 1/16 and 00200008 00000400 with probability 1/16 are used.We generated two 1000 pairs of plain text to break the 6 round DES.The first 1000 and second 1000 plain texts are generated such that their xor was 0x0000080100100000 and 0x0000801000004000 respectively. This was determined by applying inverse intial permutation on their characteristics.Plain texts are stored in dummyplain1.txt , dummyplain2.txt file.

determining cipher text of the plain text

In order to generate cipher text for the plain text , we established connections to servers and using valid credentials. we used codes in x.py and y.py to generate ciphertext from file dummyplain1.txt and dummyplain2.txt . Generated Cipher text are stored in file dummycipher1.txt and dummycipher2.txt.

Finding the Key bit

Following steps are taken to find the key

- We converted the obtained cipher text to binary text using the mapping defined above , then we used Computing Xors for rounds.ipynb to apply reverse final permutation on cipher text to get L_6R_6 and $L_6^{'}R'_6$. As $R_5 = L_6$ we got the output of expansion box and and input XOR of S boxes for 6th round DES.
- Using the first characteristic value we get that ,$L_5 =$ and for the second characteristic value we get that ,$L_5 =$. we performed $L_5 \oplus (R_6 \oplus R_6^{'})$ to find output of the permutation box, then we applied inverse permutation to get output xor of s-box for 6th round
- Let $E\left(R_5\right) = \alpha_1\alpha_2 \cdots \alpha_8$ and $E\left(R'_5\right) = \alpha'_1\alpha'_2 \cdots \alpha'_8 and \beta = \alpha_i \oplus k_{6,i}, \beta^{'} = \alpha^{'}i \oplus k^{'}6, i.$ where length of α_i and $\alpha^{'}i = 6$ and $k_6 = k6, 1k_{6,2} \cdots k_{6,8}$ we already know, we know $\alpha_i, \alpha' i, \beta i \oplus \beta' i$ and $\gamma i \oplus \gamma'_i$. To count the number of time key k satisfy the possibility of being a key to one of the 8 S-boxes,We created a 8 by 64 key matrix .

- We computed the set $X_i = (\beta, \beta') | \beta \oplus \beta' = \beta_i \oplus \beta'_i$ and $S(\beta) \oplus S(\beta') = \gamma_i \oplus \gamma'_i X$. We found the value of k such that $\alpha_i \oplus k = \beta$ and $(\beta, \beta') \in X_i$ for some β' All values of k which satisafies the condition for s-box , we incremented their value in the matrix by 1.
- Following value for the charchteristic 40080000 04000000 is found.

S-box	Key	Max_Key_frequency	Mean_Key_frequency
S1	61	130	130
S2	51	321	321
S3	37	120	120
S4	7	117	117
S5	27	151	151
S6	22	307	307
S7	21	196	196
S8	62	197	197

Xor value will be zero for S2 , S5 , S6 , S7 and S8 box in round 4 for above characteristic. Hence, in round 6 these S-boxes will give the corresponding key bits of K_6 . as we can see there is significant difference in value of Max_Key_frequency and Mean_Key_frequency, which further strengthen the idea of key being correct. We

proceeded by taking the key bits for S2, S5, S6, S7 and S8 boxes as 51, 27, 22, 21 and 62 respectively.
- Same process yield following result for characteristic.

S-box	Key	Max_Key_frequency	Mean_Key_frequency
S1	61	147	67
S2	51	170	67
S3	37	146	67
S4	7	306	77
S5	27	169	69
S6	22	308	74
S7	21	118	70
S8	62	102	70

Xor value will be zero for S2 , S5 , S6 , S7 and S8 box in round 4 for above characteristic.
For this characteristic, in round 4, XOR will be zero for S1, S2, S4, S5 and S6. Hence, in round 6 these S-boxes will give the corresponding key bits of K_6. as we can see there is significant difference in value of Max_Key_frequency and Mean_Key_frequency, which further strengthen the idea of key being correct. We proceeded by taking the key bits for S2, S5, S6, S7 and S8 boxes as 51, 27, 22, 21 and 62 respectively.

As we can see for Both characteristics, they have S2, S5 and S6 s-boxes as common and we also have obtained same key value for them , which verify our claims. Hence we have obtained 42 bits out 56 bits key.

Determining key value

As we lack 14 keys to obtain actual key value. we will use brute force method to obtain the rest of the missing key value.
To obtain rest of key value we will iterate 2^{14} $$ times for a given a plane text and corresponding cipher text. Our chose plain text is "ddddddddddddddd" and it's cipher text would be "fgslshkgfkqkiljf".
After this step we obtained the actual key value as
01101110010111100111101100101011011101101010010101010011

Now we will obtain 48 bit round key for each round.

ROUND	KEY IN BINARY
Round 1	111011000100111110000111001111111110010110010100

Round 2 01101111001101111011000101001011000111010011011111
Round 3 11101010110111001110110101110110101110111111110000
Round 4 11011001111000110101101000110001101011010111101 1
Round 5 00100100110111111011101101101111101111100000010010
Round 6 11110111001110010100011101101101011001010111111 0

The cipher text assigned to us is “sqmeijrjogiogndgsipojsjinhjgpgdg” , In order to get password we need to decrypt the cipher text. As each character is represented by 4 bits and cipher text has total 32 character so this could be represented as 128 bit string, which is 2 block of DES ciphertext. Upon using our mapping , It can be shown as {253, 145, 86, 230, 179, 91, 58, 3, 245,203,111,101,164,99,195,3}
- After performing decryption on the ciphetext using our code , the plaintext obtained is "ovtsgidffu000000" and after removing the zeros we obtained "ovtsgidffu" . we removed the zero and obtained the actual password.

No files uploaded

Q5 Password

5 Points

What was the password used to clear this level?

ovtsgidffu

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.

Goldfish_Assignment4.zip Download

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