CS 641 : ASSIGNMENT : PART 4 : SCHUTZSAS

A PREPRINT

Srinjay Kumar
170722

Abhyuday Pandey
170039

Kumar Shivam
170354

February 29, 2020

1 Path to the Cipher Text

The keyword used to get to the cipher text are :

- Read : We see an empty screen.
- Enter : We reach at the edge of the lake.
- Jump, Jump, Pull : We run out of breath and die.
- We try again.
- Jump, Jump, Back, Dive, Pull : We get the magic wand.
- We then went back to the first screen.
- We tried to read the text but it was still empty.
- Then, we went back to the 3^{rd} level and freed the spirit by using 'wave'.
- We then went back to the first screen of part 4.
- Read
- We then figured out that we had a 3 round DES at our hands.
- We entered "password"
- We get the ciphertext "orrpgnijqipsqpjmomplfijifgskmhpj"

2 Problem

The fourth problem of our assignment is to decipher a 3-round DES. This was clarified on Moodle and in class.
The ciphertext to be decrypted for this part is "orrpgnijqipsqpjmomplfijifgskmhpj".

3 Decryption

3.1 Method

Three round DES can be broken with the help of Known-Plain text attack.

3.2 Known Plain Text Attack[1]

The known-plaintext attack (KPA) is an attack model for cryptanalysis where the attacker has access to both the plaintext (called a crib), and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and code books.

3.3 Constants

The constants as defined for the problem are:

- **ip** : This step is used just after receiving the message to be encrypted. If the message is M, then we calculate **ip(M)**.
- **ipinv** : This step is used after executing all the rounds required in the DES. If the message is D, then we calculate **ipinv(M)**.
- **expand** : We expand a 32 bit plaintext to a 48 bit plaintext.
- **perm** : This step mixes the input text. it converts 32 bits to 32 bits.
- **s** : There are 8 S-boxes. For each S-box, we have 6 bit input and a 4 bit output for each S-box. So, we have 48 bit input and 32 output.
- **pc1** : This is a key permutation which maps 64 bits of key to 56 bits.
- **shift** : This is the shift we perform on output of pc1. The shift is different for each round.
- **pc2** : This is a key permutation which maps 56 bits of output of shift to 48 bit key for a particular round.

3.4 One Round DES

- Let the input to one round DES be **M**.
- Now, we need to derive L_0 and R_0 from the message M.
- First, we need to apply **ip** on the message M and let us call the permuted message P.
- After, we divide P into two equal parts L_0 and R_0.
- The output after 1^{st} round is L_1 and R_1.
- L_1 and R_1 can be calculated as

$$L_1 = R_0$$
$$R_1 = L_0 + f(R_0, K_1)$$

- Any general step can be calculated as

$$L_n = R_{n-1}$$
$$R_n = L_{n-1} + f(R_{n-1}, K_n)$$

- After, we calculate the expansion of the R_0 as a part of the function f. Let the output after expansion be $E(R_0)$.
- Then, we take the xor of K_1 with $E(R_0)$. For any general step, we calculate $E(R_{n-1}) \oplus K_n$.
- Let the current text be $B_1B_2B_3B_4B_5B_6B_7B_8$. Let the S-boxes be $S_1S_2S_3S_4S_5S_6S_7S_8$. Then we calculate the output for the S-boxes as $S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$.
- The final step for the first round will be permutation and can be calculated as $P(S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8))$, where P is the permutation matrix, and let us name the output of output of the S-boxes be D.
- Similarly, we calculate 16 rounds of DES. After 16^{th} round of DES, we calculate the final data by multiplying the matrices **ipinv** and D.
- The feistel structure is summarized in Fig 1.

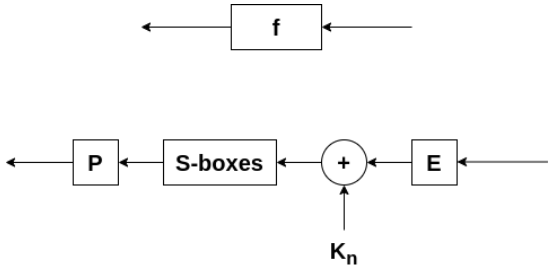

Fig 1: Internals of feistel structure

3.5 Three Round DES

- We first calculate the message P after multiplying M with **ip**.
- Then we derive L_0 and R_0 from the M.
- Then, we calculate L_1 and R_1 by

$$L_1 = R_0$$
$$R_1 = L_0 + f(R_0, K_1)$$

- The function f involves 3 steps
  - Expansion
  - Adding the key
  - Calculating the output of S-boxes
  - Permutation
- The 2^{nd} and 3^{rd} rounds can be calculated as

$$L_2 = R_1$$
$$R_2 = L_1 + f(R_1, K_2)$$
$$L_3 = R_2$$
$$R_3 = L_2 + f(R_2, K_3)$$

- Let the message L_3 and R_3 be grouped as D, and finally calculate **ipinv(D)**.
- Fig 2 below depicts three round DES well.

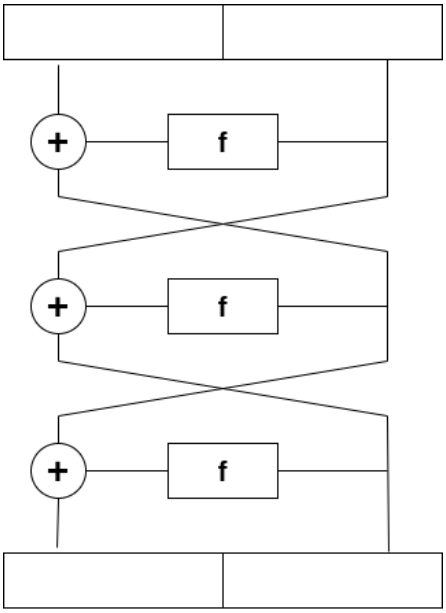

Fig 2: Three Round DES scheme

4 Breaking Three Round DES

4.1 Methodology and Notation

- We will do differential cryptoanalysis and mount a known plaintext attack on the 3 round DES.
- Let the two initial plaintexts be M and M^*. After calculating the message after initial permutation, we have P and P^*.
- Let P be divided into L_0 and R_0 and P^* be L_0^* and R_0^*.
- We took the plaintexts such that R_0 and R_0^* are same, i.e. the difference between R_0 and R_0^* is 0.
- We will be denoting the difference between texts as

$$L_0^{'} = L_0 \oplus L_0^*$$
$$R_0^{'} = R_0 \oplus R_0^*$$

4.2 Information Available

- We would be executing all the steps of a 3 round DES with inputs $L_0^{'}$ and $R_0^{'}$.
- Since $R_0^{'}$ is a 32 bit string with all zeroes since we took both R_0 and R_0^* to be the same.
- We also know $L_3^{'}$ and $R_3^{'}$ since they will be available in the form of the ciphertext after performing **ipinv**.
- Now coming to the output of the first three rounds, we have $L_1^{'}$ and $R_1^{'}$ with

$$L_1^{'} = R_0^{'}$$
$$R_1^{'} = L_0^{'} \oplus f(R_0^{'}, K_1)$$
$$L_2^{'} = R_1^{'}$$
$$R_2^{'} = L_1^{'} \oplus f(R_1^{'}, K_2)$$
$$L_3^{'} = R_2^{'}$$
$$R_3^{'} = L_2^{'} \oplus f(R_2^{'}, K_3)$$

- $L_1^{'}$ is known since $R_0^{'}$ is known.
- $R_1^{'}$ is known since $R_0^{'}$ and $L_0^{'}$ are known.
- $L_2^{'}$ is known since $R_1^{'}$ is known.
- $R_2^{'}$ is known since $R_1^{'}$ and $L_1^{'}$ are known.

4.3 Getting K_3

- Since $R_2^{'}$ is known, we know $E(R_2^{'})$ because

$$E(R_2^{'}) = E(R_2) \oplus E(R_2^*) = E(R_2 \oplus R_2^*) = E(R_2)^{'}$$

- We know $E(R_2^{'})$, therefore, we know $E(R_2^{'}) \oplus K_3$ because

$$E(R_2^{'}) \oplus K_3 = E(R_2) \oplus K_3 \oplus E(R_2^*) \oplus K_3 = E(R_2 \oplus R_2^*) = E(R_2^{'})$$

- We **do not** know the output of the S-boxes because they are the non-linear step for the DES and cannot be eliminated by taking two consecutive xors.
- We know $L_2^{'}$ and $R_3^{'}$, so we know the output differential of permutation. Let it be P'. We know that

$$R_3^{'} = L_2^{'} \oplus P'$$

- We calculate P' by

$$R_3^{'} \oplus L_2^{'} = L_2^{'} \oplus P' \oplus L_2^{'}$$
$$R_3^{'} \oplus L_2^{'} = P'$$

- Therefore, we know the input and output to the S-box. Let the input and output be $S_{in}^{'}$ and $S_{out}^{'}$.
- Here, we have expected 4 pairs of inputs and outputs corresponding to a given differential input and output for each S-box.
- We can reduce the number of possibilities by sending further plaintexts and therefore, we can get the key for the third round.

4.4 Decrypting DES

- We have got K_3.
- Therefore, we have 48 bits of the key of the 64 bits.
- Similarly, by decrypting K_2, we have 48 bits. Therefore, we can get some more bits of the entire 64 bit key.
- Now, for the remaining bits of the key, we can iterate through all the possibilities and finally get all the 64 bits of the key.

5 Decryption by Code

5.1 Getting the ciphertext from command line

To fully automate the process, we opened the console in browser while playing the game and quickly realized that query to the server can be automated by performing a POST request on the server with valid credentials.
Following is a sample command for the same:

```
curl -H "Content-Type: application/json" --request POST --data '{"plaintext": "vsbsfg",
"password": "7d1480a22895004ec4879c98dacc6d32", "teamname": "SchutzSAS"}'
-k https://172.27.26.181:9999/des
```

Output is a JSON file with fields "ciphertext" and "success".

5.2 Getting the key for three round DES

- We observed output is always in range $f - u$ and it was written that two characters represent $1-$byte, so we quickly concluded that $f - u$ are hexadecimal numbers from 0 to F as they are precisely 16 in number.

$$f = 0000$$
$$g = 0001$$
$$i = 0010$$
$$.....$$
$$t = 1110$$
$$u = 1111$$

- We described a procedure above to get the key for DES.
- Initially, we decrypted the key for the 3^{rd} round of the DES.
- It gives us 48 bits of the required 64 bits of the entire key for DES.
- Next, we reverse the 3^{rd} round of the DES. We now have a 2 round DES.
- We can now decrypt the 2^{nd} round of the DES. Thus, we had K_3 and K_2 now.
- We applied $pc2$ inverse, left shift inverse and $pc1$ inverse on both K_3 and K_2. It turned out, that both keys have only 8 unknown bits in common. In other words, using K_3 and K_2 we figured out 56 bits of the key.
- Now only 256 i.e 2^8 possibilities of keys remained with us. Moreover, we found that since K_1, K_2 and K_3 come from same 56 bits there was no point of expecting more bits. The key is,

`1001111x0101000x0011101x0000110x0110100x0110111x1101100x1100000x`

- x denotes unknown bits.

5.3 Encryption of "orrpgnijqipsqpjmomplfijifgskmhpj"

- The second screen of the problem after entering 'password' gives the string "orrpgnijqipsqpjmomplfijifgskmhispj".
- As we know that there are 4 bits corresponding to each character. Therefore, this is 2 block of ciphertext.
- Since, we already have 256 possibilities for K, we evaluated all possibly decryptions of this ciphertext. As expected there was only 1 possibility because K_1, K_2, K_3 were coming from same 56 bits of the key.

5.4 Checking all possibilities for answer

- We obtained the decryption of "orrpgnijqipsqpjmomplfijifgskmhpj" and we received a plaintext.
- We entered this plaintext in the the game, and we were redirected to next level. Hence, this was the password!

6 Decrypting the Password

`Password : grhrlgipjlffhfontnhushtpjntpmhhk`

7 Conclusion

We were able to break the 3 round DES with just 13 plain-texts by chosen plaintext attack.
The password for this level is mentioned in the previous section.
Fully automated code for this process is in the folder.

8 References

- https://en.wikipedia.org/wiki/Known-plaintext_attack
- http://page.math.tu-berlin.de/ kant/teaching/hess/krypto-ws2006/des.htm