Exercise sheet 4, 07 December 2017

You can find the authoritative description of DES at `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf` Part of the learning target for these exercises is that you learn how to read a crypto standard, so you should use this document for the following exercises. For context I give some explanation here.

DES is a Feistel cipher, that means that the message block of 64 bits is split into a left half of 32 bits and a right half of 32 bits. In every round the right half is used to encrypt the left half and the sides flip; more formally to compute (L_i, R_i) from (L_{i-1}, R_{i-1}) put $L_i = R_{i-1}$ and $R_i = L_{i-1} \oplus f_i(R_{i-1})$. Here f_i is a function f that takes the round key k_i.

At tbe beginning and end of DES the input bits are permuted using permutation IP and its inverse $FP = IP^{-1}$.

The key schedule takes the 64 bit key (read the spec to see how this relates to the 56 bits of effective key length) and expands it into 16 subkeys $k_1, k_2, \ldots, k_{16}$ of 48 bits each, one per round of DES.

The function f takes the 32-bit input, expands it into 48 bits, XORs those with the round key and splits the resulting 48 bits into 8 blocks of 6 bits. Each of those blocks then gets fed through some substitution box (S-box) $S_1, S_2, \ldots, S_8$ which maps 6 bits to 4 bits. Finally those 32 bits get combined, permuted and output.

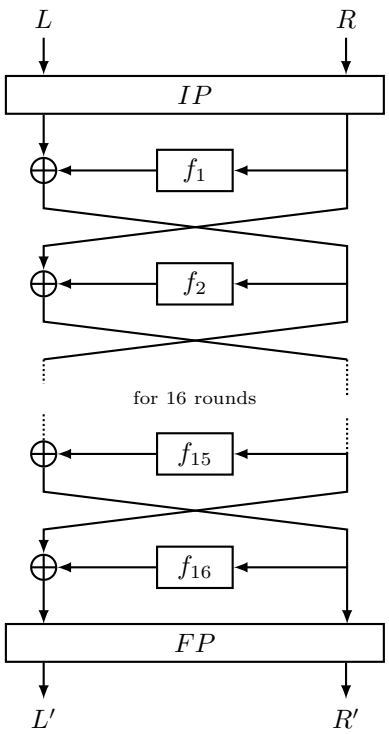


Image: Jérémy Jean at `https://www.iacr.org/authors/tikz/`

1. Explain how decryption works (note that f is not invertible). State how to recover (L_{i-1}, R_{i-1}) from (L_i, R_i).

2. Take S_5 and compute $S_5(x_1) \oplus S_5(x_2)$ and compare the result with $S_5(x_1 \oplus x_2)$ for the following values:

   (a) $x_1 = (000000), x_2 = (100000)$

   (b) $x_1 = (111111), x_2 = (000001)$

   (c) $x_1 = (000000), x_2 = (101010)$

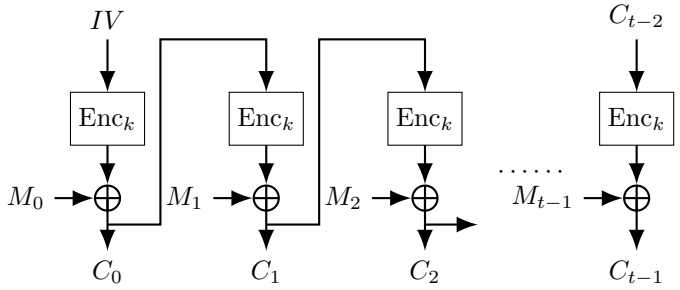
3. Compute the first subkey if the 56-bit key consists of 56 zeros.

4. Compute the output of the first round (i.e. include the initial permutation, the split into left and right, the function f, the xor and the swap) when the input is the all-zero string and the key is 56 zeros.

5. Compute the output of the first round (i.e. include the initial permutation, the split into left and right, the function f, the xor and the swap) when the input is the all-zero string with the rightmost bit replaced by 1 and the key is 56 zeros. Do not forget the initial permutation.

6. The Electronic-Code-Book (ECB) mode encrypts long texts by chopping them into blocks matching the input size of the block cipher (possibly after padding to match the length) and encrypting them individually. We've seen that this is a bad idea.

   Here is another mode, called Cipher Feedback Mode (CFB).



   Show how to encrypt $(IV, M_0, M_1, M_2, \ldots)$ and to decrypt $(IV, C_0, C_1, C_2, \ldots)$.

7. Check out
   `https://blog.fortinet.com/2014/03/31/angecryption-at-insomni-hack`.

8. Read up on the POODLE attack (e.g `https://en.wikipedia.org/wiki/POODLE#POODLE_attack_against_TLS` and references).