TP

This TP has been written by Christine Bachoc *and Guilhem* Castagnos *(Institut Mathématiques de Bordeaux).*

Exercise 1.
B32 is a block cipher described by Bart Preneel and Lars Knudsen to learn the mechanisms of linear and differential cryptanalysis.

This is a product cipher scheme (substitution/permutation) which operates on 32 bits blocks. We will use a two-turns scheme which uses three keys of 32 bits K_0, K_1, K_2.
After the initial state which consists in adding K_0 – add means XOR bit by bit – to the plaintext, the *turn function* operates as follow:

1. *Substitution*: the 32 bits are divided in 8 blocks ok 4 bits. The S-box takes as input each block of 4 bits and is given by:
$$S = [7, 3, 6, 1, 13, 9, 10, 11, 2, 12, 0, 4, 5, 15, 8, 14].$$
You must understand: the image of i by S is $S[i]$, where $i \in [0..15]$ is identified by its binary writing (the least significant bit on the right!). For example, the image of $[0, 1, 0, 0]$ is given by $S[4] = 13$, i.e. $[1, 1, 0, 1]$
2. *Permutation*: the block is subjected to a circular shift of 2 to the right;
3. We add the key (K_1 at first round and K_2 at second round).

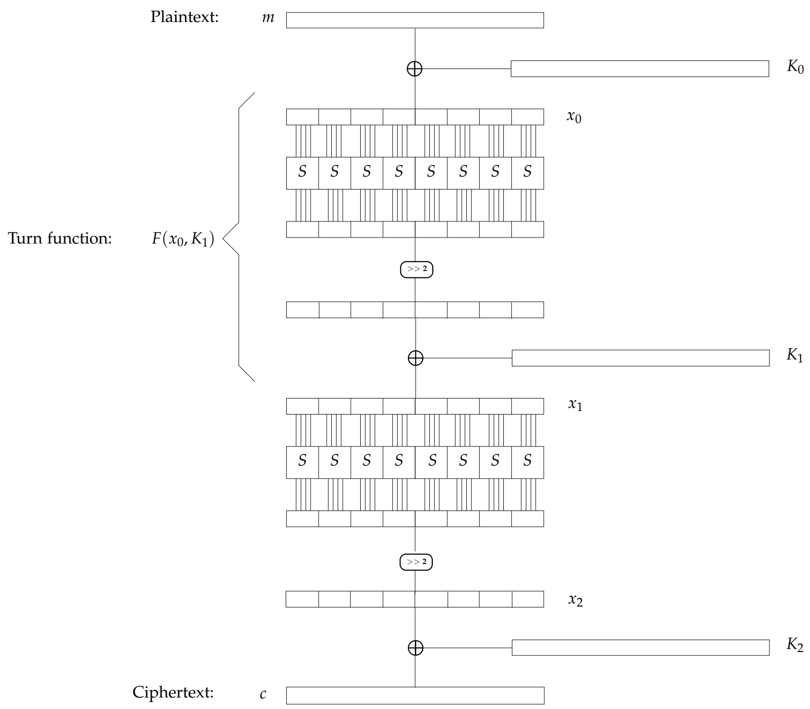

Figure 1: Encryption B32

You will find a list of plaintexts and ciphertexts at the address `http://perso.ens-lyon.fr/adeline.langlois/webpage/Crypto2014/clairs_chiffres.txt`. In this file, for `i` from 1 to 100, `Ciphertext[i]` is the ciphertext of `Plaintext[i]`.

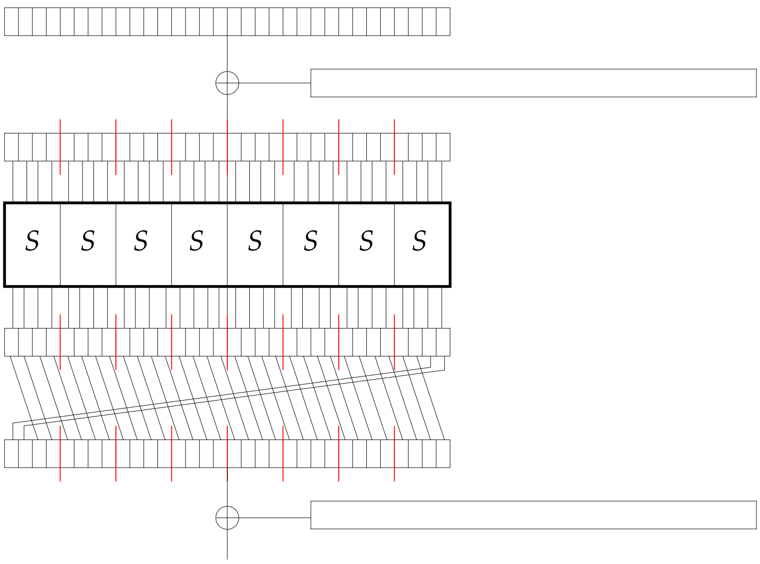

Figure 2: First round of B32

1. Write the turn function, the inverse turn function, a function giving the complete encryption (two rounds and three keys K_0, K_1, K_2), and the decryption function.

   You could write the blocks and the keys as lists of $\mathbb{F}_2$ elements. We could also write conversion functions from sequences of 4 elements of $\mathbb{F}_2$ to integers from 0 to 15.

To test the function: the ciphertext of B32 of $(0,0,\ldots,0,0)$ with the keys $K_0 = (1,0,0,\ldots,0,0,1)$, $K_1 = (1,1,\ldots,1,1)$ and $K_2 = (0,1,1,\ldots,1,1,0)$ must return

$$(0,0,1,1,1,0,0,1,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0).$$

2. The matrix of linear approximations L of a box $S : \mathbb{F}_2^s \to \mathbb{F}_2^s$ is defined by its inputs:

   $$L[a,b] = \#\{x \in \mathbb{F}_2^s \mid a \cdot x = b \cdot S(x)\}$$

   for all $a, b \in \mathbb{F}_2^s$, where $a \cdot x$ means $\bigoplus_i a_i x_i$ where the a_i's and the x_i's are the bits of a and x. We have

   $$p_{a,b} := \Pr(a \cdot x = b \cdot S(x)) = \frac{L[a,b]}{2^s}.$$

   Compute this matrix for the box S of B32.

3. What are the probabilities $p_{a,b}$ the farthest from $1/2$? Made a list of the corresponding couples (a,b). Which one will be useful for linear cryptanalysis ?

4. If $x \in \mathbb{F}_2^{32}$, we write $x^{(0)}, x^{(1)}, \ldots, x^{(7)}$ the 4 bits blocks which establish it. We choose a couple (a,b) in the previous list, and we write

   $$A = (a, 0, 0, \ldots, 0, 0) \in \mathbb{F}_2^{32},$$

   such that $A^{(0)} = a$, and for $i \geq 1$, $A^{(i)} = 0000$, and also $B = (b, 0, 0, \ldots, 0, 0)$.

We denote by F the function of B32. Let K_0, K_1, K_2 be the three keys of B32. Let m be a random plaintext, chosen uniformly in the blocks of 32 bits. We recall that the ciphertext c of m from B32 with 2 rounds with the keys K_0, K_1, K_2 is given by:

$$\begin{cases} x_0 = m + K_0 \\ x_1 = F(x_0, K_1) \\ c = F(x_1, K_2) \end{cases}$$

Using the matrix L, show that $A \cdot m = P(B) \cdot x_1$ with probability $1/2 \pm 6/16$, where P is the permutation function (the second step of the turn function). Check experimentally this probability (take some keys and test them with a high number of random m).

5. We call *active boxes* at second round, the boxes of index $i \in \{0, 1, \dots, 7\}$, such that $P(B)^{(i)}$ is not equal to 0000. Explain why, in the linear cryptanalysis attack on the last round, we can restrict ourselves to determine the value of the bits of the key K_2 in some indexes $j \in \{0, \dots, 31\}$.

6. Give a summary tab of the couples (a, b) such that $p_{a,b} = 1/2 \pm 6/16$, the expression of $P(B)$, the expression of the linear equation connecting the bits of m and those of x_1, the number of the corresponding active boxes, and the indices j of the bits of the key K_2 that we can set.

7. Choose a couple (a, b) given only one active box. Find the bits of the key K_2 in some indices by using the couples plaintexts/ciphertexts given in the beginning. Do the same for a couple (a, b) with two active boxes.

8. Iterate the attack of the previous question (with one and two active boxes) by constructing A and B such that we approximate the boxes S corresponding to the other 4 bits blocks. Give the totality of the key K_2. Compare the efficiency of the method with an active box to the method with two active boxes.

9. The given couple plaintext/ciphertext has been built from an algorithm B32 using an algorithm of construction of keys. The secret key K_1, K_2 and K_3 has been constructed by taking some bits from a secret key K of 32 bits. The following tab gives the order of the 32 bits using to construct the 3 keys:

key	bits of K used
K_0	17, 31, 0, 0, 18, 7, 20, 18, 8, 1, 27, 27, 2, 4, 11, 20, 25, 13, 17, 10, 24, 9, 29, 15, 21, 18, 28, 20, 4, 5, 24, 15
K_1	15, 2, 5, 0, 13, 31, 5, 10, 18, 2, 3, 14, 14, 0, 11, 1, 20, 15, 14, 27, 6, 11, 19, 3, 6, 20, 14, 2, 28, 11, 5, 8
K_2	4, 24, 23, 12, 22, 21, 31, 15, 29, 1, 0, 26, 17, 24, 16, 5, 31, 0, 20, 21, 26, 30, 15, 11, 16, 23, 18, 30, 30, 19, 28, 23

This mean for example that the first bit of K_0 is the 17-th bit of K, the second is the 31-th bit of K (we enumerate the positions from 0 to 31).

Find the secret key K.

10. (Extension to B32 **with three turns).** We now suppose that B32 is doing three turns. How to choose (A, B) to make minimal the number of active boxes at the end of the second turn ? What is the corresponding $P_{A,B}$ probability ? Write this attack with 3 turns and test it by choosing random keys K_0, K_1, K_2, K_3 and by constructing enough corresponding couples plaintext/ ciphertext.