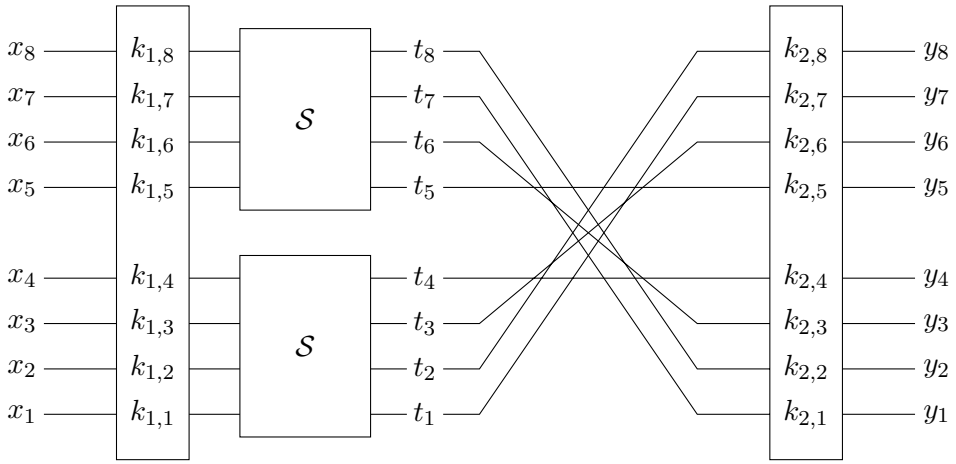
Examen Final – Cryptographie

jeudi 17 janvier – Amphi G3

Toutes les réponses devront être soigneusement justifiées
Notes de cours et TD autorisées – calculatrice interdite

On considère le cryptosystème E sur 8 bits donné par le diagramme suivant :



où les blocs verticaux correspondent à l'addition des sous-clés et la S-boîte $\mathcal{S}$ envoie le mot d'entrée A sur le mot de sortie B suivant le diagramme ci-dessous.

A	0000	0001	0010	0011	0100	0101	0110	0111
B	0111	1000	0000	0010	0110	1010	0001	1011
A	1000	1001	1010	1011	1100	1101	1110	1111
B	0100	0101	1100	0011	1111	1001	1110	1101

On note respectivement X, K_1, T, K_2 et Y le mots de 8 bits dont les bits sont respectivement $x_1, \ldots, x_8$, $k_{1,1}, \ldots, k_{1,8}$, $t_1, \ldots, t_8$, $k_{2,1}, \ldots, k_{2,8}$ et $y_1, \ldots, y_8$.

On note $A = a_1a_2a_3a_4$ les bits du mot A et $B = b_1b_2b_3b_4$ les bits du mot B.

1. (a) Calculer le biais de la relation linéaire $a_2 \oplus a_3 = b_2$.
   (b) Calculer le biais de la relation linéaire $a_1 \oplus a_2 \oplus a_3 \oplus a_4 = b_1 \oplus b_2$.
   (c) Calculer le biais de la relation binaire $a_1 \oplus a_4 = b_1$.
   (d) Que peut-on conclure des questions (1a-c) sur la résistance linéaire de $\mathcal{S}$?

(e) Que peut-on conclure des questions (1a-c) sur l'indépendance des bits $a_1, a_2, a_3, a_4, b_1, b_2$?

2. (a) Trouver l'image du mot $X = 1001\,0011$ par le cryptosystème E en prenant pour sous-clés $K_1 = 0001\,1101$ et $K_2 = 1101\,1000$.

   (b) Trouver un mot de 8 bits dont l'image par le cryptosystème E est le mot $1111\,1111$ en sachant que les sous-clés K_1 et K_2 sont égales à $1001\,1001$.

   (c) Trouver une sous-clé K_2 telle que l'image par le cryptosystème E du mot $0101\,1010$ est le mot $1010\,0101$ avec $K_1 = 1100\,0011$.

3. On suppose à présent qu'un attaquant, qui connaît la sous-clé $K_1 = 1011\,1010$, cherche à obtenir de l'information sur la sous-clé K_2.

   (a) Montrer que $P(x_1 \oplus x_4 = t_1) = P(x_1 \oplus x_4 = k_{2,7} \oplus y_7) = 3/4$.
   (Indication : utiliser la question (1c).)

   (b) On considère la variable aléatoire T qui compte parmi 20 couples (X, Y), où X est un mot de 8 bits pris au hasard et Y est le cryptage de X par le cryptosystème E, le nombre de couples pour lesquels $x_1 \oplus x_4 = y_7$.
   Calculer l'espérance et la variance de T.
   (Indication : séparer les cas $k_{2,7} = 0$ et $k_{2,7} = 1$.)

   (c) L'attaquant dispose de 20 couples (X, Y), avec Y cryptage de X par le cryptosystème E, et trouve qu'on a $x_1 \oplus x_4 = y_7$ pour 13 couples.
   En utilisant l'inégalité de Chebyshev, majorer la probabilité de cet événement quand $k_{2,7} = 1$.

   (d) Que peut conclure l'attaquant sur la valeur de $k_{2,7}$?