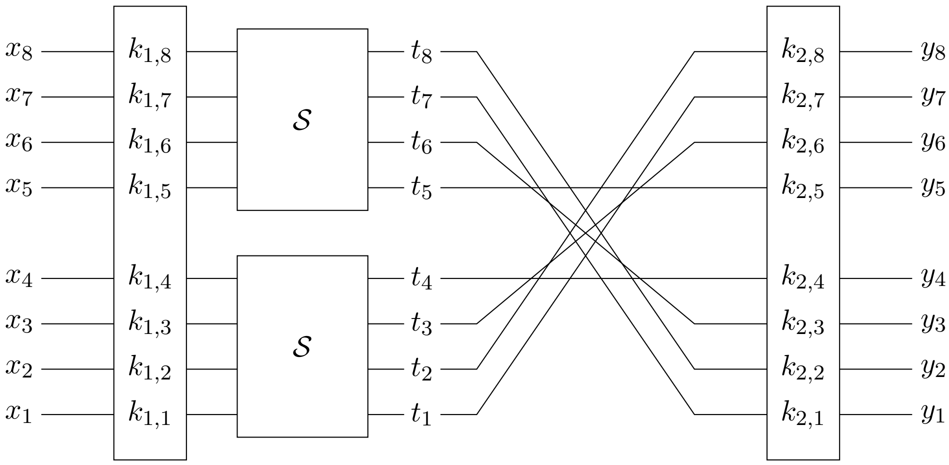
# Solutions de l'examen final – Cryptographie

**jeudi 17 janvier – Amphi G3**

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 $a_2 \oplus a_3 = b_2$.
   *Solution. L'équation est vérifiée pour* $A =$ 0001, 0100, 0110, 0111, 1010, 1100, *et donc avec une probabilité de* $6/16 = 3/8$. *Ainsi le biais de cette relation est* $3/8 - 1/2 = -1/8$.

   (b) Calculer le biais de la relation linéaire $a_1 \oplus a_2 \oplus a_3 \oplus a_4 = b_1 \oplus b_2$.
   *Solution. L'équation est vérifiée pour* $A =$ 0001, 0011, 0100, 0110, 0111, 1000, 1010, 1100, 1101, 1111 *et donc avec une probabilité de* $10/16 = 5/8$. *Ainsi le biais de cette relation est* $5/8 - 1/2 = 1/8$.

   (c) Calculer le biais de la relation binaire $a_1 \oplus a_4 = b_1$.
   *Solution. L'équation est vérifiée pour* $A =$ 0000, 0001, 0010, 0100, 0101, 0110, 0111, 1001, 1010, 1011, 1100, *et* 1110 *donc avec une probabilité de* $12/16 = 3/4$. *Ainsi le biais de cette relation est* $3/4 - 1/2 = 1/4$.

   (d) Que peut-on conclure des questions (1a-c) sur la résistance linéaire de $\mathcal{S}$ ?
   *Solution. La résistance linéaire est au plus de* 4.

(e) Que peut-on conclure des questions (1a-c) sur l'indépendance des bits $a_1, a_2, a_3, a_4, b_1, b_2$ ?
*Solution. Puisque la relation* $a_1 \oplus a_4 = b_1$ *est la somme des relations* $a_2 \oplus a_3 = b_2$ *et* $a_1 \oplus a_2 \oplus a_3 \oplus a_4 = b_1 \oplus b_2$*, si les variables étaient indépendantes, le lemme d'empilement donnerait comme valeur pour son biais*

$$2(1/8)(-1/8) = -1/32.$$

*Ce qui est inexact, donc les variables* $a_1, a_2, a_3, a_4, b_1, b_2$ *sont dépendantes.*

2. (a) Trouver l'image du mot $X = 1001\,0011$ par le cryptosystème $E$ en prenant pour les sous-clés $K_1 = 0001\,1101$ et $K_2 = 1101\,1000$.
*Solution. On a* $X \oplus K_1 = 1000\,1110$ *et donc* $T = 0100\,1110$. *Ainsi* $Y = K_2 \oplus 1010\,1001 = 0111\,0001$.

   (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 $1001\,1001$.
*Solution. On a* $Y \oplus K_2 = 0110\,0110$ *et donc on doit avoir* $T = 1010\,0101$ *et donc* $X = 1100\,0000$.

   (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 $K_1 = 1100\,0011$.
*Solution. On a* $T = 0101\,0101$ *et donc* $Y = 1010\,0101 = 0111\,0001 \oplus K_2$, *d'où* $K_2 = 1101\,0100$.

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).)
*Solution. On a, par la question* (1c), *en prenant* $a_1 = x_1 \oplus k_{1,1}$ *et* $a_4 = x_4 \oplus k_{1,4}$

$$P((x_1 \oplus 1) \oplus (x_4 \oplus 1) = t_1) = P(x_1 \oplus x_4 = t_1) = 3/4.$$

   (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 $k_{2,7} = 1$.)
*Solution. Si* $k_{2,7} = 0$, *alors* $P(x_1 \oplus x_4 = y_7) = 3/4$ *et donc l'espérance est* $E(T) = (3/4) \times 20 = 15$ *et la variance est* $V(T) = (3/4) \times (1 - 3/4) \times 20 = 15/4$.
*Si* $k_{2,7} = 1$, *alors* $P(x_1 \oplus x_4 = y_7) = 1/4$ *et donc l'espérance est* $E(T) = (1/4) \times 20 = 5$ *et la variance est* $V(T) = (3/4) \times (1 - 3/4) \times 20 = 15/4$.

   (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 $k_{2,7} = 1$.
*Solution. Si* $k_{2,7} = 1$ *alors* $E(T) = 1/4$ *et* $V(T) = 15/4$. *L'inégalité de Chebyshev donne*

$$P(T - E(T) = 8) \leq P\big(|T - E(T)| = 8\big) \leq P\big(|T - E(T)| \geq 8\big) \leq V(T)/8^2 \approx 0,23$$

   (d) Que peut conclure l'attaquant sur la valeur de $k_{2,7}$ ?
*Solution. Il y a donc plus de* 75% *de chances que* $k_{2,7} = 0$.