



---

Documents papiers autorisés

---

**Exercice 1.** a) Calculer  $S_i(110101)$  où  $S_i$  est la  $i^{eme}$  S-Box du DES et  $i = 5, 8$ .  
b) Calculer  $S(88)$ ,  $S(54)$  où  $S$  est la S-Box de l'AES.

**Exercice 2.** Montrer que l'inverse du polynôme  $a(x) = 03_H X^3 + 01_H X^2 + 01_H X + 02_H \text{ mod}(X^4 + 1)$  considéré comme un polynôme à coefficients dans  $\mathbb{F}_{2^8}$  est  $b(x) = 0B_H X^3 + 0D_H X^2 + 09_H X + 0E_H$

**Exercice 3.** Dans le corps  $\mathbb{F}_{2^8}$  on pose  $RC[1] = 1$  et pour  $j \geq 2$ ,  $RC[j] = 2RC[j - 1]$ . Calculer  $RC[j]$  pour  $j = 1, 2, \dots, 12$ .

**Exercice 4.** Soit la clé  $K = 11\ 00\ 00\ 00\ 11\ 00\ 00\ 00\ 11\ 00\ 00\ 00\ 11\ 00\ 00\ 00$  qu'on veut utiliser pour chiffrer des blocs de taille 128 bits avec l'AES. Calculer  $k_i$  pour  $i = 0, 1, \dots, 7$

**Exercice 5.** a) On suppose que Alice et Bob utilisent l'entier  $n$  et RSA avec deux clés publiques  $e_A$  et  $e_B$  premières entre elles. On suppose que *Caroline* envoie le même message chiffré  $m^{e_A}$  et  $m^{e_B}$  à Alice et à Bob. Montrer que Eve qui écoute les communications peut retrouver facilement le message  $m$ .

b) À fin d'améliorer la sécurité des messages Bob choisit deux exposants  $e_1$  et  $e_2$  et demande à Alice de chiffrer d'abord son message par  $e_1$ , pour obtenir  $c_1 = m^{e_1}$  puis de re-chiffrer par  $e_2$  pour obtenir  $c_2 = c_1^{e_2}$  et d'envoyer  $c_2$ . Est-ce que ce double chiffrement améliore la sécurité. Si oui pourquoi, si non pourquoi.

**Exercice 6.** Soit  $p = 1 + 2q$  un grand nombre premier tel que  $q$  soit aussi premier. Soit  $\alpha$  et  $\beta$  deux éléments primitifs de  $\mathbb{Z}_p^*$ . La valeur de  $\log_\alpha \beta$  n'est pas publique et l'on suppose qu'elle est calculatoirement difficile à obtenir.

a) Montrer que la fonction de hachage

$$h : \mathbb{Z}_q \times \mathbb{Z}_q \longrightarrow \mathbb{Z}_p^* \\ (x_1, x_2) \longrightarrow \alpha^{x_1} \beta^{x_2}$$

résiste aux collisions si le calcul de  $\log_\alpha \beta$  est difficile.

b) Que pensez vous de cette fonction de hachage ?