Introduction à la cryptologie

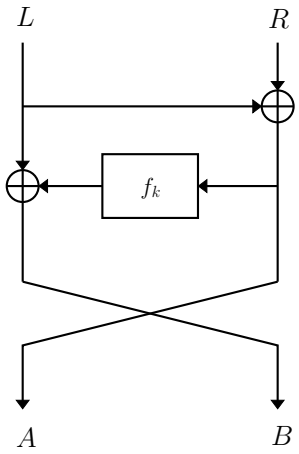
Examen du 15 mai 2009, de 13h30 à 16h30, durée 3h.

Documents et calculatrices interdits.
Rédigez les deux parties sur des feuilles séparées.
Justifiez vos réponses — brièvement mais suffisamment.
Ce sujet comporte 4 pages. Les paragraphes sont indépendants.

Première partie — cours de Laurent Fousse

1. Tour de chiffrement par bloc

On considère le tour suivant pour un algorithme de chiffrement par bloc de taille n bits :



Ici L et R sont les demi-blocs de gauche et de droite respectivement, A et B les demi-blocs de sortie (de gauche et de droite), et f_k est la fonction du tour, dépendant d'une clef k.

1.1. Écrivez les équations liant les sorties A et B aux entrées L et R.

1.2. Montrez que ce tour est inversible pour toute fonction f_k (pas nécessairement inversible elle-même). Écrivez les opérations à réaliser pour calculer L et R à partir de A et B, et dessinez le tour inversé ainsi trouvé.

1.3. Comment un attaquant peut-il distinguer la fonction F_k que réalise ce tour d'une fonction aléatoire $g : \{0,1\}^n \to \{0,1\}^n$? Écrivez la stratégie de l'attaquant, et calculez sa probabilité de réussite (*i. e.* de deviner correctement si l'oracle calcule bien F_k ou s'il a choisi une fonction g quelconque).

2. CHIFFREMENT PAR BLOC DANS $\mathbb{F}_2[X]$

Dans cet exercice les polynômes appartiennent à $\mathbb{F}_2[X]$ où $\mathbb{F}_2 = \{0,1\}$ est le corps à deux éléments.

On définit une fonction de chiffrement E_k sur des blocs de taille 4 bits, vus comme des polynômes : le bloc $b_3b_2b_1b_0$ correspond au polynôme

$$b_3X^3 + b_2X^2 + b_1X + b_0.$$

Par exemple `0100` correspond au polynôme X^2 et le polynôme X^2+1 est représenté par le bloc `0101`. La clef $k = k_3k_2k_1k_0$ est vue aussi comme un polynôme K de degré inférieur ou égal à 3 :

$$K(X) = k_3X^3 + k_2X^2 + k_1X + k_0.$$

On définit d'autre part les polynômes $C(X) = X^3 + X^2 + 1$ et $G(X) = X^4 + 1$.

La fonction de chiffrement E_k est définie par la procédure suivante :

(1) Convertir le bloc d'entrée m en un polynôme $M(X)$.
(2) Calculer $U(X) = M(X) + K(X)$.
(3) Calculer $V(X) = C(X) \times U(X) \mod G(X)$.
(4) Convertir $V(X)$ en un bloc de 4 bits c.
(5) Retourner c.

2.1. Chiffrez `1100` avec la clef `0110`.

2.2. Montrez qu'il est possible de déchiffrer et écrire la fonction de déchiffrement D_k.

2.3. Déchiffrez `1111` avec la clef `1000`.

2.4. Supposons que l'on adapte la fonction de chiffrement pour traiter des blocs et des clefs de taille suffisamment grande pour qu'une attaque *brute-force* ne soit pas possible (en modifiant $C(X)$ et $G(X)$ en conséquence). Le chiffrement serait-il sûr, et sinon quelles attaques pouvez vous envisager ?

3. HACHAGE

On considère la fonction h suivante :

$$\begin{aligned} h : \{0,1\}^{96} &\to \{0,1\}^{32} \\ x_1||x_2||x_3 &\mapsto g(g(x_1||x_2)||x_3), \quad |x_1| = |x_2| = |x_3| = 32 \end{aligned}$$

où $x||y$ représente la concaténation des blocs x et y, et $g : \{0,1\}^{64} \to \{0,1\}^{32}$ est une fonction de compression résistant aux collisions au sens fort, c'est-à-dire qu'il est calculatoirement difficile de trouver $x_1||x_2$ et $x_1'||x_2'$ **distincts** tels que $g(x_1||x_2) = g(x_1'||x_2')$.

3.1. La fonction h est-elle une fonction de hachage ou une fonction de compression ?

3.2. Montrer qu'il est calculatoirement difficile de trouver une collision pour la fonction h.

Seconde partie — cours de Michael Eisermann

4. Polynômes sur un corps

Soit $\mathbb{K}[X]$ l'anneau des polynômes sur un corps $\mathbb{K}$. On se propose d'étudier l'ensemble V des polynômes $P \in \mathbb{K}[X]$ vérifiant $P(x) = 0$ pour tout $x \in \mathbb{K}$.

4.1. (a) Quelle est la structure d'un idéal quelconque de $\mathbb{K}[X]$?

(b) L'ensemble V est-il un idéal de l'anneau $\mathbb{K}[X]$?

(c) Expliciter V dans le cas où le corps $\mathbb{K}$ est de cardinal infini.

4.2. Supposons que $\mathbb{K}$ est un corps fini à q éléments.

(a) Existe-t-il un polynôme $P \in V$ tel que $0 \leq \deg(P) < q$?

(b) Expliciter sous forme développée un polynôme $Q \in V$ de degré q. Justifier.

(c) En déduire une description explicite de V.

4.3. Supposons toujours que $\mathbb{K}$ est un corps fini.

(a) Déterminer les éléments $u \in \mathbb{K}^\times$ vérifiant $u = u^{-1}$.

(b) En déduire le produit $\prod_{u \in \mathbb{K}^\times} u$ de tous les éléments non nuls dans $\mathbb{K}$.

(c) On pose $P_a = -\prod_{b \neq a}(X - b)$. Que vaut $P_a(x)$ en fonction de $x \in \mathbb{K}$?

On note $\mathbb{K}^\mathbb{K}$ l'anneau des fonctions $f, g \colon \mathbb{K} \to \mathbb{K}$ muni de l'addition et la multiplication point par point, $(f+g)(x) := f(x) + g(x)$ et $(f \cdot g)(x) := f(x) \cdot g(x)$ pour tout $x \in \mathbb{K}$.

4.4. On considère le morphisme naturel $\mathbb{K}[X] \to \mathbb{K}^\mathbb{K}$:

(a) Quel est son noyau ?

(b) Quelle est son image ?

En déduire un isomorphisme d'anneaux par passage au quotient.

Tournez, s'il vous plaît.

5. Corps finis et polynômes irréductibles

5.1. Énoncer (sans preuve) la classification des corps finis.

5.2. Donner, en la justifiant, une description d'un corps à 49 éléments.

5.3. Expliciter tous les polynômes irréductibles de degré ≤ 3 sur $\mathbb{F}_2$.

Soit $p \geq 2$ un nombre premier et soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps à p éléments.

5.4. Énoncer (sans preuve) la décomposition du polynôme $X^{p^n} - X$, où $n \in \mathbb{N}$, en facteurs irréductibles unitaires dans $\mathbb{F}_p[X]$.

5.5. En déduire une formule récursive pour le nombre a_n des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p$.

5.6. Quel est le comportement asymptotique de a_n pour $n \to \infty$?

5.7. Calculer les nombres $a_1, a_2, \ldots, a_8$ dans le cas $p = 2$.

L'algorithme suivant n'est pas correct :

Algorithme 1 Tester l'irréductibilité de $P \in \mathbb{F}_p[X]$

Entrée: un polynôme $P \in \mathbb{F}_p[X]$ de degré $n \geq 2$.
Sortie: « irréductible » si P est irréductible, « composé » sinon.

pour k **de** 1 **à** n **faire**
  $Q \leftarrow X^{p^k} - X$
  $R \leftarrow \mathrm{pgcd}(P, Q)$
  si $R \neq 1$ **alors retourner** « composé » **fin si**
fin pour
retourner « irréductible »

5.8. Expliciter un exemple où cet algorithme donne la mauvaise réponse.

5.9. Rectifier (légèrement) la méthode pour qu'elle donne toujours la bonne réponse.

5.10. Telle qu'elle est écrite, la méthode est inefficace. Expliquer pourquoi.

5.11. Améliorer la méthode pour qu'elle soit efficace (tout en restant correcte).

Fin.