Introduction à la cryptologie

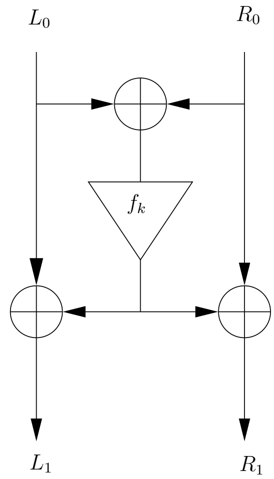
Examen du 4 septembre 2009, de 14h à 17h, durée 3h.

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. Chiffrement par bloc à la Feistel

On considère une fonction F de chiffrement par bloc constituée de 16 fois le tour suivant :



où f_k est une fonction dépendant de la sous-clef secrète de ronde S_k et du numéro de tour k, et les demi-blocs d'entrée L_0, R_0 et de sortie L_1, R_1 ont pour longueur n bits.

1.1. Écrire les sorties L_1 et R_1 en fonction des entrées L_0, R_0 et de la fonction f_k.

1.2. Montrer comment inverser un tel tour, sans hypothèse sur la fonction f_k. Dessiner le diagramme correspondant au déchiffrement.

1.3. En supposant que $n = 3$, calculer tous les chiffrés possibles pour $(L_0, R_0) = (\texttt{000}, \texttt{111})$.

1.4. En supposant que $n = 5$, le chiffré de $(\texttt{00000}, \texttt{01010})$ peut-il être $(\texttt{11111}, \texttt{00000})$?

1.5. En déduire une attaque à clairs et chiffrés connus permettant de distinguer la fonction F de chiffrement (utilisant 16 tours) d'une fonction aléatoire.

2. HACHAGE

On considère la fonction h suivante :

$$\begin{array}{rcl} h : \{0,1\}^{128} & \rightarrow & \{0,1\}^{32} \\ x_1||x_2||x_3||x_4 & \mapsto & x_1 \oplus g(x_2||g(x_3||x_4)) \\ |x_1| = |x_2| = |x_3| = |x_4| = 32 & & \end{array}$$

où $x||y$ représente la concaténation des blocs x et y, et $g : \{0,1\}^{64} \rightarrow \{0,1\}^{32}$ 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 $g(x_1||x_2) = g(x'_1||x'_2)$).

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

2.2. Étant donné un message $x = x_1||x_2||x_3||x_4$, est-il facile de trouver un message $x' = x'_1||x'_2||x'_3||x'_4 \neq x$ tel que $h(x) = h(x')$?

2.3. Est-il facile d'inverser la fonction h ? Si oui, proposer un algorithme qui calcule un message x pour une entrée y avec $h(x) = y$.

3. CHIFFREMENT PAR BLOC À LA AES

On considère le chiffrement par bloc « *NonAES* » opérant sur des blocs de 9 bits (l'état) que l'on dispose en un carré de 3 sur 3 :

a_{00}	a_{01}	a_{02}
a_{10}	a_{11}	a_{12}
a_{20}	a_{21}	a_{22}

Les opérations d'une ronde sont les suivantes :

– *ShiftRows* : la deuxième ligne est décalée cycliquement d'une position vers la droite, et la troisième ligne d'une position vers la gauche.

– *MixColumns* : chaque colonne est vue comme un polynôme de degré 2 dans $\mathbb{F}_2$, les coefficients faibles à forts de haut en bas, et multiplié par X^2 modulo $X^3 + X + 1$. Le polynôme obtenu est écrit dans la colonne correspondante.

– *AddRoundKey* : la clef de ronde, de taille 9 bits, est ajouté case par case.

3.1. On choisit comme message clair $m = (\texttt{001010100})$ et comme clef de ronde $k = (\texttt{110001011})$. Calculer le bloc chiffré correspondant après une ronde (on lit le tableau ligne par ligne, de gauche à droite).

3.2. Montrer qu'il est possible de déchiffrer en connaissant la clef, et décrire une ronde du déchiffrement.

3.3. On essaie de mesurer les propriétés de diffusion du chiffrement. Pour cela on simule le chiffrement de deux messages, avec la même clef, ne différant que du premier bit. À partir de combien de rondes complètes est-ce que la différence initiale se sera potentiellement propagée à tout l'état ? Détailler.

3.4. Par rapport au vrai AES, et en plus de calculer dans un corps plus petit et sur un état de seulement 3 sur 3 éléments, le chiffrement NonAES n'a pas d'opération *SubBytes*. Quelle vulnérabilité ce manque introduit-il, et comment l'exploiter sur AES ?

Seconde partie — cours de Michael Eisermann

4. Racines de X^2+1

Rappelons que le polynôme X^2+1 est irréductible sur $\mathbb{R}$ alors que sur $\mathbb{C}$ il se décompose en $X^2+1=(X-i)(X+i)$ où $i^2=-1$. L'objectif de cet exercice est d'étudier la décomposition de X^2+1 sur un corps fini $\mathbb{F}_q$ à éléments.

4.1. Décomposer X^2+1 en facteurs irréductibles dans $\mathbb{F}_2[X]$.

4.2. Énoncer l'ordre et la structure du groupe $\mathbb{F}_q^\times$.

4.3. Supposons qu'il existe $x \in \mathbb{F}_q$ tel que $x^2+1=0$.
Quel est l'ordre de x dans le groupe $\mathbb{F}_q^\times$?
Que conclure pour la valeur de q modulo 4 ?
Énoncer avec précision le théorème qui sert ici.

4.4. Réciproquement, sous quelle condition sur q modulo 4 le polynôme X^2+1 admet-il une racine dans $\mathbb{F}_q$? Justifiez votre réponse. Quel résultat sert ici ?

Pour conclure, expliciter (tant que possible) la décomposition de X^2+1 en facteurs irréductibles dans $\mathbb{F}_q[X]$ en fonction de q.

5. Isomorphismes entre corps finis

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

Dans la suite on travaille sur le corps $\mathbb{F}_7=\mathbb{Z}/7\mathbb{Z}$ à 7 éléments.

5.2. Les anneaux quotients

$$F=\mathbb{F}_7[X]/(X^2+1) \quad \text{et} \quad G=\mathbb{F}_7[X]/(X^2-1)$$

sont-ils isomorphes ? Justifiez votre réponse.

5.3. Les anneaux quotients

$$E=\mathbb{F}_7[X]/(X^2+X-1) \quad \text{et} \quad F=\mathbb{F}_7[X]/(X^2+1)$$

sont-ils isomorphes ? Justifiez votre réponse.

Soit x l'image de X dans le quotient E et soit $y=ax+b$ où $a,b\in\mathbb{F}_7$.

5.4. Dans E calculer y^2 sous la forme $cx+d$ où $c,d\in\mathbb{F}_7$.

5.5. Trouver $a,b\in\mathbb{F}_7$ de sorte que $y^2=-1$ dans E.

5.6. En quoi ce calcul permet-il d'expliciter la réponse à la question 5.3 ?

6. Corps finis et polynômes irréductibles

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

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

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

6.3. Quel est le comportement asymptotique de a_n pour $n \to \infty$? (sans preuve)

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 ← X^(p^k) − X
    R ← pgcd(P,Q)
    si R ≠ 1 alors retourner « composé » fin si
fin pour
retourner « irréductible »
```

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

6.5. Rectifier (légèrement) la méthode pour qu'elle donne toujours la bonne réponse. Justifier ensuite la validité de votre algorithme rectifié.

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

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

Fin.