TD5 – Codes d'authentification de message

Exercice 1. *Polynômes et corps finis*

Corps premiers. Pour un nombre premier p, on appelle *corps fini à p éléments* l'ensemble des entiers $\{0, \dots, p-1\}$ muni des opérations *modulo* p. On le note $\mathbb{F}_p$. Par exemple, le corps $\mathbb{F}_7$ est l'ensemble $\{0, 1, 2, 3, 4, 5, 6\}$ avec les opérations *modulo* 7 : $6 + 4 = 3$, $2 - 5 = 4$, $3 \times 5 = 1$, … La notion de *corps* signifie que tout élément non nul de $\mathbb{F}_p$ peut-être inversé : pour tout $x \in \mathbb{F}_p$ non nul, il existe y tel que $x \times y = 1$ (on note $y = 1/x$). On peut donc aussi diviser : x/y est défini par $x \times (1/y)$ si $y \neq 0$.

1. Calculer $9 + 6$, $3 - 8$, 6×4 et $7/2$ dans $\mathbb{F}_{11}$.

Polynômes. Un *polynôme à coefficient dans* $\mathbb{F}_p$ est une expression $P(X) = \sum_{i=0}^{d} c_i X^i$, où $c_i \in \mathbb{F}_p$ est le *coefficient de degré* i de P. On note $\mathbb{F}_p[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{F}_p$. Si $c_d \neq 0$, le *degré de* P est d. On appelle *racine* de P un élément $x \in \mathbb{F}_p$ tel que $F(x) = 0$.

2. Soit $F(X) = 11\,X^3 + 10\,X^2 + 8\,X + 4$ un polynôme à coefficient dans $\mathbb{F}_{13}$.
   - **i.** Calculer $F(4)$.
   - **ii.** Montrer que 9 est racine de F.

Mantra du degré. Le nombre de racines d'un polynôme non nul à coefficients dans un corps fini est au plus égal à son degré.

3. Soit $F(X) = X^3 + 5\,X^2 + 2\,X + 6$ un polynôme à coefficients dans $\mathbb{F}_7$. Vérifier qu'il possède bien ≤ 3 racines.

Corps binaires. Au delà des corps premiers $\mathbb{F}_p$, on peut définir un corps fini à 2^n éléments pour tout entier $n \geq 1$. Pour cela, on choisit un polynôme de degré n sur $\mathbb{F}_2$ *irréductible* et *unitaire*, c'est-à-dire un polynôme φ dont le coefficient de plus grand degré est 1, et qui ne peut pas être écrit comme produit de deux polynômes de degrés plus petits non constants. Ces polynômes jouent un rôle équivalent aux nombres premiers. On peut alors montrer que l'ensemble des polynômes *modulo* φ est un corps [1] : on peut additionner, soustraire, multiplier et surtout diviser dans cet ensemble. On le note $\mathbb{F}_{2^n}$.

4. On considère $\varphi(X) = X^2 + X + 1$. On admet qu'il est irréductible [2].
   - **i.** Soit $\alpha(X) = X + 1$ et $\beta(X) = X$. Calculer $\alpha + \beta$, $\alpha - \beta$ et $\alpha \times \beta$, *modulo* $\varphi(X)$.
   - **ii.** Trouver un inverse de X *modulo* φ.

5. On se place dans le cadre général où φ est un polynôme irréductible de degré n.
   - **i.** Montrer que le corps $\mathbb{F}_{2^n}$ défini par φ possède 2^n éléments distincts.
   - **ii.** Exprimer en terme d'opérations logiques l'addition de deux éléments de ce corps.
   - **iii.** Qu'est-ce qui rend l'utilisation de ce type de corps intéressante ?

Exercice 2. *Fonction de hachage polynomiale*

Soit $\mathbb{F}$ un corps fini (premier ou binaire). On considère l'ensemble des messages $\mathcal{M} = \mathbb{F}^*$, c'est-à-dire qu'un message est un *mot* écrit avec des éléments de $\mathbb{F}$. Plus naturellement, on voit un message $m \in \mathcal{M}$ comme un ℓ-uplet d'éléments de $\mathbb{F}$, où ℓ est la longueur du message. On peut également interpréter un message de longueur ℓ comme un polynôme de degré $< \ell$: un message $m = (m_0, \dots, m_{\ell-1})$ peut être vu comme le polynôme $m(X) = \sum_{i=0}^{\ell-1} m_i X^i$. On note $\mathcal{M}_\ell$ l'ensemble des messages de longueur ℓ.
De même, on définit un espace de clef $\mathcal{K} = \mathbb{F}$ (une clef est un élément de $\mathbb{F}$). On définit alors la fonction de hachage $h : \mathcal{K} \times \mathcal{M} \to \mathbb{F}$ en posant $h_k(m) = m(k)$: pour calculer le haché de m, on interprète m comme un polynôme et on l'évalue sur la clef k.

1. Soit $\mathbb{F} = \mathbb{F}_7$, $m = (3, 4, 0, 1)$ et $k = 4$. Calculer $h_k(m)$.

1. Plus généralement, on peut définir de la même façon un corps à p^n éléments pour tout nombre premier p et tout n. Et on peut montrer réciproquement que tout corps fini possède p^n éléments où p est un nombre premier : il n'existe par exemple aucun corps possédant 6 éléments.
2. Une façon de s'en convaincre est d'essayer toutes les possibilités !

2. **i.** Soit $P \in \mathbb{F}[X]$ un polynôme de degré au plus d. Montrer que si on tire uniformément $\alpha \in \mathbb{F}$, $\Pr[P(\alpha) = 0] \leq d/|\mathbb{F}|$.
   ii. Soit $m^0, m^1 \in \mathcal{M}_\ell$ deux messages de longueur ℓ, et $\Delta \in \mathbb{F}$. Montrer que si on tire aléatoirement une clef $k \in \mathcal{K}$, alors $\Pr\left[h_k(m^0) - h_k(m^1) = \Delta\right] < \ell/|\mathbb{F}|$.
3. Compter *précisément* le nombre d'additions et de multiplications dans $\mathbb{F}$ nécessaires pour calculer $h_k(m)$ si $m \in \mathcal{M}_\ell$.

Exercice 3. *GMAC et Poly1305*

Les deux codes d'authentification de messages standardisés GMAC et Poly1305 sont basés sur la même construction[3], en utilisant des fonctions de hachage polynomiales sur un *grand* corps fini $\mathbb{F}$.
Étant donné une fonction de hachage polynomiale h sur un corps binaire $\mathbb{F}_{2^n}$ et une fonction pseudo-aléatoire $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, on définit un MAC de la manière suivante :

- $\mathsf{Gen}(1^n)$: tire $k_h \in \mathcal{K} = \mathbb{F}_{2^n}$ et $k_F \in \{0,1\}^n$, uniformément ;
- $\mathsf{Mac}_{k_h,k_F}(m)$ où $m \in \mathcal{M}_n$: tire $r \in \{0,1\}^n$ uniformément et renvoie $t = (r, h_{k_h}(m) + F_{k_F}(r))$;
- $\mathsf{Vrfy}_{k_h,k_F}(m,(r,s))$: renvoie 1 si et seulement si $s = h_{k_h}(m) + F_{k_F}(r)$.

1. **i.** Dans le cas de GMAC, on utilise le corps binaire $\mathbb{F}_{2^{128}}$. Comment peut-on représenter les éléments du corps $\mathbb{F}_{2^{128}}$, et que peut-on utiliser en pratique comme fonction pseudo-aléatoire ?
   ii. Dans le cas de Poly1305, on utilise le corps premier $\mathbb{F}_{2^{130}-5}$ et on doit donc légèrement modifier la construction. Proposer une solution qui utilise pour F un chiffre par bloc dont la taille de block est 128 (par ex. AES).

On va montrer que ce MAC est *fortement sûr*. Pour définir cette sécurité renforcée, on modifie légèrement l'expérience de sécurité des MAC. Après avoir fait autant d'appels à Mac_k qu'il souhaite, l'attaquant doit toujours produire un couple (m,t) tel que $\mathsf{Vrfy}_k(m,t) = 1$. Mais on autorise maintenant l'attaquant à demander une étiquette pour m : tout ce qu'il doit être capable de faire est de produire une *autre* étiquette valide. Précisément, si l'attaquant a appelé Mac_k sur les messages $m_1, \ldots, m_q$ et obtenu les étiquettes $t_1, \ldots, t_q$, il doit maintenant produire un couple (m,t) tel que si $m = m_i$, t doit être différent de t_i.
On note $\mathsf{Macforge}$ l'expérience de l'attaquant : $\mathsf{Macforge}(n) = 1$ si l'attaquant réussit son attaque, et $\mathsf{Macforge}(n) = 0$ sinon. On désigne par Mac^* l'algorithme Mac modifié dans lequel on utilise une *vraie* fonction aléatoire h à la place de F_k, et $\mathsf{Macforge}^*$ l'expérience correspondante.

2. On peut montrer que pour tout attaquant polynomial probabiliste, les deux expériences sont indiscernables, c'est-à-dire $|\Pr[\mathsf{Macforge}(n) = 1] - \Pr[\mathsf{Macforge}^*(n) = 1]| \leq \mathsf{negl}(n)$. De manière informelle, quelle technique de preuve peut-on utiliser pour prouver l'affirmation précédente ?

On s'intéresse maintenant à $\Pr[\mathsf{Macforge}^*(n) = 1]$. On note $m_1, \ldots, m_q$ l'ensemble des requêtes faites par l'attaquant à Mac^*, et $(r_1, s_1), \ldots, (r_q, s_q)$ les réponses correspondantes. On note $(m,(r,s))$ le couple produit *in fine* par l'attaquant.

3. À chaque appel à Mac^*, la valeur r_i est tirée aléatoirement. On note R l'évènement « les r_i ne sont pas toutes distinctes ». Encadrer la probabilité de R.
4. Soit N l'évènement « la valeur de r dans le couple $(m,(r,s))$ renvoyé par l'attaquant est différente de tous les r_i ».
   i. Montrer que
   $$\Pr[\mathsf{Macforge}^*(n) = 1] \leq \Pr[R] + \Pr[\mathsf{Macforge}^*(n) = 1 \wedge N] + \Pr[\mathsf{Macforge}^*(n) = 1 \wedge \neg R \wedge \neg N].$$
   ii. Montrer que $\Pr[\mathsf{Macforge}^*(n) = 1 \wedge N] \leq \mathsf{negl}(n)$.
5. On borne maintenant $\Pr[\mathsf{Macforge}^*(n) = 1 \wedge \neg R \wedge \neg N]$.
   i. Traduire les évènements $\neg R$ et $\neg N$ en une condition sur les r_i et r.
   ii. Montrer que l'attaquant ne peut avoir aucune information sur la clef k_h pendant l'expérience.
   iii. Montrer qu'il existe i tel que $(m,(r,s))$ est valide si et seulement si $h_{k_h}(m) - h_{k_h}(m_i) = s - s_i$.
   iv. En déduire que $\Pr[\mathsf{Macforge}^*(n) = 1 \wedge \neg R \wedge \neg N] \leq n/|\mathbb{F}|$.
6. Conclure.

3. En réalité, on ignore quelques détails ici.