1 TD 1 : Structure de $(\mathbb{Z}/n\mathbb{Z})^*$, un protocole simple et probabilités

Groupe des éléments inversibles

1. Soit G un groupe et $g \in G$. Montrer que $g^n = 1$ ssi n est un multiple de l'ordre de g.

2. Soit G un groupe et $g \in G$. Montrer que si $g^n = 1$ et que pour tout p premier divisant n, $g^{n/p} \neq 1$ alors n est l'ordre de g.

3. Soient p et q deux nombres premiers distincts. A-t-on

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}?$$

4. Montrer que si $n = \prod_{i=1}^{k} p_i^{e(p_i)}$ (p_i premiers distincts) est impair, le nombre de solutions de $x^2 \equiv 1 \pmod{n}$ est 2^k.

5. Montrer le théorème suivant: p est premier si et seulement si

$$(p-1)! \equiv -1 \pmod{p}.$$

Un protocole d'échange

Alice veut envoyer à Bob le message $x \in \{0,1\}^n$. Alice (resp. Bob) possède une clé secrète a (resp. b) de même longueur que x. Ils effectuent le protocole suivant :

1. Alice envoie $A_1 = x \oplus a$ à Bob.

2. Bob envoie $B_1 = A_1 \oplus b$ à Alice.

3. Alice envoie $A_2 = B_1 \oplus a$ à Bob.

Montrer que Bob peut retrouver le message x. Montrer que si Oscar a intercepté tous les échanges, il peut également retrouver x.

Probabilités

Nous allons étudier la sécurité de Shannon pour les systèmes symétriques. On suppose que les ensembles $\mathcal{P}$ et $\mathcal{K}$ sont donnés avec des lois de probabilité notées respectivement $Pr_{\mathcal{P}}$ et $Pr_{\mathcal{K}}$. On note alors Pr la loi de probabilité produit sur $\mathcal{P} \times \mathcal{K}$ (i.e. $Pr(A \times B) = Pr_{\mathcal{P}}(A) \times Pr_{\mathcal{K}}(B)$). Pour simplifier les notations, on pourra aussi écrire $Pr(x)$ pour $x \in \mathcal{P}$ en identifiant $\{x\}$ avec $\{x\} \times \mathcal{K}$ (ainsi $Pr(\{x\} \times \mathcal{K}) = Pr_{\mathcal{P}}(\{x\})$ et de même pour $k \in K$. Enfin si $y \in \mathcal{C}$, on note $Pr(y)$ la probabilité de l'évènement $\{(x,k),\ \mathcal{E}_k(x) = y\}$.

1. On dit qu'un tel système symétrique est *parfaitement sûr* si

$$\forall x \in \mathcal{P}, \forall y \in \mathcal{C}, Pr(x|y) = Pr(x).$$

   Justifier la dénomination.

2. Montrer que si $\forall y \in \mathcal{C},\ Pr(y) > 0$ et que si le système est parfaitement sûr alors

$$\#\mathcal{K} \geq \#\mathcal{C} \geq \#\mathcal{P}.$$

   On pourra utiliser la formule de Bayes et interpréter $Pr(y|x) > 0$.

3. Montrer que pour $y \in \mathcal{C}$ fixé,

$$\{(x,k),\ \mathcal{E}_k(x) = y\} = \bigcup_{\substack{k \in \mathcal{K} \\ y \in \mathcal{E}_k(\mathcal{P})}} \{(\mathcal{D}_k(y), k)\}$$

   et qu'ainsi

$$Pr(y) = \sum_{\substack{k \in \mathcal{K} \\ y \in \mathcal{E}_k(\mathcal{P})}} Pr(k) Pr(\mathcal{D}_k(y)).$$

4. On suppose maintenant que $\#\mathcal{K} = \#\mathcal{C} = \#\mathcal{P}$ et que $\forall y \in \mathcal{C},\ Pr(y) > 0$. Montrer que le système est parfaitement sûr si et seulement si

   - toutes les clés ont la même probabilité ;
   - $\forall x \in \mathcal{P}$ et $\forall y \in \mathcal{C}$ il existe une unique clé k satisfaisant $\mathcal{E}_k(x) = y$.

   Pour montrer la sécurité parfaite, on pourra utiliser la formule de la question précédente.

5. On imagine le système de chiffrement suivant : soit $n > 1$ un entier et $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$. On suppose que $Pr_{\mathcal{P}}$ est telle que $Pr_{\mathcal{P}}(x) > 0$ pour tout x. Pour tout $x \in \mathcal{P}$ on tire aléatoirement (avec une distribution uniforme) une clé $k \in \mathcal{K}$ et on envoie $\mathcal{E}_k(x) = x \oplus k$. Montrer qu'un tel système est parfaitement sûr. Quels sont ses inconvénients ?

2 TD2 : RSA

Questions simples

1. Peut-on avoir un exposant de chiffrement e pair pour RSA ?

2. Soit la clé publique $n = 55, e = 13$ pour RSA. Calculer la clé secrète d puis déchiffrer $y = 4$. Pour indication $4^{2^i} \equiv 16, 36, 31, 26, 16 \pmod{55}$ pour $i = 1, 2, 3, 4, 5$.

Une attaque cyclique sur RSA

Soit (n, e) une clé publique pour RSA. Soit $x \in (\mathbb{Z}/n\mathbb{Z})^*$ un texte clair et y son chiffré. Montrer qu'il existe un entier k tel que

$$x^{e^k} \equiv x \pmod{n}$$

et que

$$y^{e^{k-1}} \equiv x \pmod{n}.$$

Pensez-vous qu'une telle attaque est dangereuse pour RSA ? Justifiez.

Une attaque sur les bits de plus haut poids

Soit p, q deux grands nombres premiers tels que $p < q < 2p$ et $n = pq$. Soit (d, e) un couple de clé privée/publique pour RSA tel que $e < \phi(n)$ et $d < \phi(n)$.

1. Montrer que $p + q \leq 3\sqrt{n}$.
2. Montrer que si on note $k = (ed - 1)/\phi(n)$
$$\left| \frac{kn + 1}{e} - d \right| < 3\sqrt{n}.$$
3. On suppose jusqu'à la fin que $e = 3$. Montrer qu'alors $k = 2$.
4. Soit $d' = \lfloor \frac{kn+1}{e} \rfloor$. Comparer d' et d. En conclure qu'environ la première moitié des bits de d ne sont pas des hard-core bits.

Une méthode de factorisation

On rappelle qu'un témoin de non-primalité d'un entier n impair pour le test de Miller-Rabin est un entier a premier à n tel que, si on écrit $n - 1 = 2^s d$ avec d impair, alors $a^d \not\equiv 1 \pmod{n}$ et quelque soit $r \in \{0, \ldots, s-1\}$ on a $a^{2^r d} \not\equiv -1 \pmod{n}$.

Montrer que s'il existe un entier a témoin de non-primalité pour n tel que $a^{n-1} \equiv 1 \pmod{n}$ *alors on peut trouver un facteur de n* (On pourra commencer par montrer qu'il existe $r \in \{0, \ldots, s-1\}$ tel que $a^{2^r d} \not\equiv 1 \pmod{n}$ et $(a^{2^r d})^2 \equiv 1 \pmod{n}$).

3 TD 3 : Un protocole de signature

Nous étudions ici une variante du protocole de signature, utile par exemple dans le cas de figure suivant. Un client veut accéder à un coffre dans une banque. Celle-ci demande au client de signer un document daté avant que l'autorisation soit accordée. Cependant, le client ne veut pas que la banque puisse révéler à quiconque quand il a eu accès au coffre. Par conséquent, il ne veut pas que la vérification de sa signature puisse se faire sans sa participation. Dans ce protocole, il faut donc rajouter un système de contrôle pour qu'Alice ne puisse signer un document puis déclarer que ce n'est pas le cas. On propose le protocole suivant :

1. Choix de la clé. La signataire A choisit un groupe cyclique G fini d'ordre premier q, un générateur g et un élément $a \in (\mathbb{Z}/q\mathbb{Z})^*$, secret. Elle calcule alors $b = g^a$. Elle choisit également une fonction de hachage $h : \{0,1\}^* \to G$ et publie (G, g, q, b, h). *Donner un exemple de choix de groupe et de paramètre résistant pour DLP.*

2. Signature. Etant donné un document $m \in \{0,1\}^*$, A calcule $s = h(m)^a$. *Quelles propriétés cette signature possède-t-elle pour l'instant?*

3. Vérification. A va convaincre Victor (V) que s est bien la puissance a-ième of $h(m)$ sans révéler sa clé secrète a.

   (a) V a le document m, la signature s et b. Il choisit aléatoirement $u, v \in \mathbb{Z}/q\mathbb{Z}$ et calculer $z = s^u b^v$. Il envoit le challenge z à A.

   (b) *Montrer que Alice peut calculer w tel que $w = h(m)^u g^v$.* Elle envoie w à Victor.

   (c) Victor compare w et $h(m)^u g^v$ et accepte la signature s'ils sont égaux.

   Nous allons montrer que ceci permet de vérifier que la signature est correcte.

   (a) Montrer que pour tout $z \in G$ il y a q couples (u, v) tels que $s^u b^v = z$.

   (b) Montrer que si $s \neq h(m)^a$ et si $z \in G$ alors pour tout $w \in G$ il y a exactement un couple (u, v) tel que $h(m)^u g^v = w$ et $s^u b^v = z$ pour un w et un z donnés.

   (c) Montrer que si s n'est pas correcte, la probabilité qu'elle soit acceptée est inférieure à $1/q$.

4. Non répudiation. Supposons maintenant que durant la vérification $z = s^u b^v$ et w aient été échangés et que la vérification échoue. Alice déclare que s n'est pas correcte. *Pourquoi doit-elle être en mesure de prouver ce fait ?* Pour le montrer, on réalise alors le protocole suivant.

   (a) Victor effectue une seconde vérification avec un challenge $z' = s^{u'} b^{v'}$.

   (b) La réponse w' lui est renvoyée.

   (c) Victor vérifie alors si
   $$(wg^{-v})^{u'} = (w'g^{-v'})^u \tag{1}$$
   et si l'égalité est vérifiée, il accepte que la signature est incorrecte.

   Nous allons montrer que ce protocole est correct.

   (a) Montrer que si A réalise correctement les calculs de vérification alors (1) est vraie.

   (b) Supposons maitenant que s est valide mais que A veut convaincre V que ce n'est pas le cas. Alors $w \neq h(m)^u g^v$. Montrer alors que pour tout challenge z' et réponse w' il existe un unique couple (u', v') tel que (1) soit vraie.

   (c) Montrer que lorsque s est valide, A peut faire échouer le test de vérification tout en préservant l'égalité (1) avec une probabilité inférieure à $1/q$.

   (d) En déduire que ce protocole permet la non-répudiation.

4 TD 4 : La signature Elgamal

Soit p un grand nombre premier et h une fonction de hachage à valeurs entières dans $[0, p-2]$. Soit g un élément primitif de $G = (\mathbb{Z}/p\mathbb{Z})^*$. On considère le protocole de signature suivant pour Alice :

Clé publique : (p, g, b) avec $b \equiv g^a \pmod{p}$;
Clé secrète : $a \in [0, p-2]$;
Signature : $y \to (y, r, s)$ avec $r \equiv g^k \pmod{p}$, $s \equiv k^{-1}(m - ra) \pmod{p-1}$ avec $m = h(y)$ et $k \in [1, p-2]$ différent à chaque signature;
Vérification : on vérifie que $0 \leq r \leq p-1$. Si non, rejeter la signature ; calculer $m = h(y)$; calculer $v \equiv g^m \pmod{p}$ et $w \equiv b^r r^s \pmod{p}$; vérifier que $v = w$.

1. *Rappeler les critères que doit remplir une signature.*
2. *Montrer que si la signature est correcte, on a bien $v = w$.*
3. *Quel élément un attaquant devrait-il calculer à priori pour signer des textes à la place d'Alice ?*
4. *Quel est la taille du paramètre de sécurité p pour qu'une telle attaque soit impossible de nos jours ?*
5. *Peut-on alors effectivement (i.e. en terme de temps de calcul) utiliser ce protocole ?*

Dans la suite, nous allons voir certaines attaques contre ce protocole de signature lorsqu'on oublie certaines des recommandations.

L'importance de k

Montrer que si Alice se sert deux fois du même k pour signer deux messages y_1 et y_2 différents, alors Oscar peut en général retrouver le secret a (On regardera l'expression s).

L'importance de la condition $0 \leq r \leq p-1$

Supposons que notre protocole ne vérifie pas cette condition. On va montrer que Oscar peut alors créer des falsifications sélectives, i.e. des signatures de nouveaux messages ayant un sens à partir d'une ancienne signature. Soit donc (y, r, s) une signature valide produite par Alice. Oscar souhaite signer un message y' avec la signature d'Alice. Oscar calcule :

$$u \equiv h(y')h(y)^{-1} \pmod{p-1}.$$

Il calcule ensuite

$$s' \equiv su \pmod{p-1}.$$

Il trouve r' tel que

$$r' \equiv ru \pmod{p-1}, \quad r' \equiv r \pmod{p}.$$

1. *Montrer comment et sous quelles conditions il peut réaliser tous ces calculs.*
2. *Vérifier que (y', r', s') est une signature valide.*
3. *Montrer que si h est sans collision alors la condition $0 \leq r \leq p-1$ empêche la falsification.*

L'importance de la fonction h

Supposons que Alice n'utilise pas de fonction de hachage, i.e. $m = y$ dans notre protocole. Oscar peut alors réaliser une autre falsification comme suit :

1. Soit i, j des entiers tels que $0 \leq i, j \leq p-2$. On cherche r sous la forme $r \equiv g^i b^j \pmod{p}$.
2. *Montrer que la relation $v = w$ est équivalente à*

$$g^{y-is} \equiv b^{r+js} \pmod{p}.$$

3. Ceci est le cas en particulier si

$$\begin{cases} y - is & \equiv 0 \pmod{p-1} \\ r + js & \equiv 0 \pmod{p-1} \end{cases}.$$

4. *Donner la condition pour que ce système admette une solution puis déterminer (r, s, y) en fonction de i, j.*
5. *Pourquoi cette falsification est moins puissante que la précédente ?*

5 TD 5 : Partage d'un secret et vote électronique

Partage

Le protocole de partage d'un secret de Shamir est basé sur le lemme suivant

Lemma 5.1. *Soient $l \leq t$ deux entiers positifs, p un nombre premier et $(x_i, y_i) \in \mathbb{Z}/p\mathbb{Z}$, $1 \leq i \leq l$ des couples tels que les x_i sont distincts. Alors il y a exactement p^{t-l} polynômes $P \in \mathbb{Z}/p\mathbb{Z}[X]$ de degré au plus $t-1$ tel que $P(x_i) = y_i$.*

Nous présentons maintenant un protocole de partage d'un secret $s \in \mathbb{Z}/p\mathbb{Z}$ entre n personnes de telle sorte que t d'entre elles (mais pas moins) peuvent reconstituer le secret initial.

1. Initialisation : soit p premier plus grand que $n+1$ et $x_i \in (Z/p\mathbb{Z})^*$, n éléments distincts. Le distributeur D publie les x_i.

2. Le partage :

   (a) D choisit secrètement $a_j \in Z/p\mathbb{Z}$, $1 \leq j \leq t-1$ et construit le polynôme

   $$a(X) = s + \sum_{j=1}^{t-1} a_j X^j.$$

   (b) D calcule les parts $y_i = a(x_i)$ et distribue secrètement à chaque i-ème membre du groupe le couple (x_i, y_i).

3. La reconstruction du secret : *montrer que si t membres du groupe collaborent ils peuvent retrouver le secret.*

4. Sécurité : supposons que $m < t$ membres du groupe collaborent. *Montrer que pour tout $s' \in \mathbb{Z}/p\mathbb{Z}$ il existe exactement p^{t-m-1} polynômes $a'(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ de degré $\leq t-1$ tel que $a'(0) = s'$ et $a'(x_i) = y_i$, $1 \leq i \leq m$. En déduire que ces membres ne peuvent pas obtenir d'information sur le secret s.*

Vote électronique

Le vote est une procédure complexe puisqu'on veut obtenir (au moins !) les sept propriétés suivantes:

1. Seules les personnes autorisées peuvent voter;
2. Personne ne peut voter plus d'une fois;
3. Aucune partie ne peut déterminer le vote d'un tiers;
4. Aucune partie ne peut dupliquer un vote;
5. Le compte total doit être correct;
6. Toutes les parties peuvent vérifier que le résultat a été correctement calculé;
7. Le protocole fonctionne même en présence d'erreurs.

Initialisation : On suppose que les n centres de vote C_i ont chacun un chiffrement à clé public avec une fonction de chiffrement $\mathcal{E}_i$ *(en proposer un exemple)* et qu'au plus $t-1 < n/2$ d'entre eux peuvent être malhonnêtes. On suppose aussi fixé un groupe cyclique $(G, \times)$ d'ordre q premier et deux éléments $g, h \in G$ tel que $h = g^x$. On suppose que ce problème du logarithme discret est difficile, i.e. personne (pas même les centres de vote) ne connaît x. *Proposer un exemple de tel groupe.*

Vote : On suppose que chacun des m votants a le choix entre deux candidats $\{\pm 1\}$. Chaque votant choisit une valeur $v_j \in \{\pm 1\}$ et une valeur aléatoire $a_j \in \mathbb{Z}/q\mathbb{Z}$ et publie le vote $B_j = g^{a_j} h^{v_j}$. *Montrer que la propriété (3) est satisfaite de manière inconditionnelle. Quel protocole ajouter pour assurer les propriétés (1) et (2) ?.*
Pour la suite, il va être important de s'assurer que $v_j = \pm 1$. On propose le schéma de mise en gage suivant:

1. Le votant V_j choisit aléatoirement $r, w \in \mathbb{Z}/q\mathbb{Z}$ et $d \in (Z/q\mathbb{Z})^*$.

2. si $v_j = 1$ alors il publie
$$\alpha_1 = g^r (B_j h)^{-d},\ \alpha_2 = g^w.$$
Sinon il publie
$$\alpha_1 = g^w,\ \alpha_2 = g^r (B_j h)^{-d}.$$

3. Un des centres de vote C_i au hasard lui envoie un challenge aléatoire $c \in \mathbb{Z}/q\mathbb{Z}$.

4. Si $v_j = 1$, V_j calcule $d' = c - d$ et $r' = w + a_j d'$ et poste $(d_1, d_2, r_1, r_2) = (d, d', r, r')$. Sinon il poste $(d_1, d_2, r_1, r_2) = (d', d, r', r)$.

5. C_i vérifie si
$$\begin{aligned} d_1 d_2 &\neq 0 \\ d_1 + d_2 &= c \\ g^{r_1} &= \alpha_1 (B_j h)^{d_1} \\ g^{r_2} &= \alpha_2 (B_j / h)^{d_2}. \end{aligned}$$

Montrer que la vérification est correcte avec une probabilité $> 1/q$ si et seulement si $v_j \in \{\pm 1\}$. Montrer ensuite que C_i n'a aucune information sur le vote.

Distribution du vote : chaque votant V_j utilise le protocole de Shamir pour partager les secrets v_j, a_j entre les n centres de vote de telle manière qu'il faut au moins $t < m$ d'entre eux pour récupérer les secrets. On note
$$R_j = v_j + r_{1j} X + \ldots + r_{tj} X^t,\ S_j = a_j + s_{1j} X + \ldots + s_{tj} X^t,$$
les polynômes utilisés avec des valeurs aléatoires r_{lj}, s_{lj} et
$$(u_{ij}, w_{ij}) = (R_j(i), S_j(i)),\ 1 \leq i \leq m$$
les valeurs envoyées à chaque C_i chiffrées avec la fonction $\mathcal{E}_i$. *Montrer que la propriété (4) est maintenant complètement satisfaite.*
Le votant V_j se lie au polynôme R_j en publiant
$$B_{lj} = g^{s_{lj}} h^{r_{lj}},\ 1 \leq l \leq t.$$

Chaque centre C_i vérifie si

$$B_j \prod_{l=1}^{t} B_{lj}^{i^l} = h^{u_{ij}} g^{w_{ij}}.$$

Montrer que si V_j a bien choisi R_j et S_j pour ses calculs, la vérification réussit. A quoi sert-elle ?

Décompte : Chaque centre de vote C_i publie

$$T_i = \sum_{j=1}^{m} u_{ij},\ A_i = \sum_{j=1}^{m} w_{ij}.$$

Montrer que toutes les autres parties peuvent vérifier que T_i et A_i sont corrects en calculant

$$\prod_{j=1}^{m} \left(B_j \prod_{l=1}^{t} B_{lj}^{j^l} \right) = h^{T_i} g^{A_i}.$$

Montrer que les conditions (6), (7) sont vérifiées en interpolant au moins $t+1$ des valeurs T_i.