Université de Caen Normandie, UFR des Sciences
Licence 3

Module "Protection de données"
TD - Cryptographie ; durée : 5h

1 Quelques ordres de grandeur

Exercice 1 *Avec son supercalculateur Fugaku, le Japon dispose du superordinateur le plus puissant au monde. Cette nouvelle machine atteint une puissance de 415,5 pétaflops, soit* $415,5 \times 10^{15} \approx 2^{58}$ *opérations flottantes par seconde.*

Bob souhaite trouver une collision pour la fonction de hachage SHA-1 (qui retourne des hachés ou empreintes de 160 bits). Avec ce supercalculateur et en supposant que le calcul d'une empreinte ne lui prendra que 2^{10} *opérations flottantes, combien de temps faudra-t-il à Bob pour trouver une collision en s'appuyant sur le principe du paradoxe d'anniversaire ? Même question avec SHA-2 (avec des empreintes/hachés de 256 bits) ?*

- *moins d'un an (soit environ* 2^{25} *secondes)*
- *moins d'un millénaire (soit environ* 2^{35} *secondes)*
- *moins de 15 milliards d'années (soit environ* 2^{59} *secondes)*
- *moins de 1 million de fois l'âge de l'univers (soit environ* 2^{78} *secondes)*
- *moins de 1 milliard de fois l'âge de l'univers (soit environ* 2^{89} *secondes)*
- *plus de 1 milliard de fois l'âge de l'univers*

Exercice 2 *Le poids moyen d'un grain de riz est de* $30mg$*. La production mondiale de riz représentait environ 480 millions de tonnes en 2019. En posant* 1 *grain de riz sur la première case d'un échiquier, puis* 2 *sur la seconde, puis* 4 *sur la troisième et ainsi de suite jusqu'à la 64ème case, combien d'années faudrait-il pour remplir la dernière case ?*

2 Arithmétique

Exercice 3 *En informatique la complexité d'un algorithme se mesure en fonction de la taille pour stocker en machine l'entrée. Étant donné un entier n, quelle est la taille en binaire pour stocker cette entier en machine ?*

Voici un algorithme qui teste si un entier n est premier.

```
booléen est_premier(n) :
    si n < 2 retourner FAUX
    pour i allant de 2 à ⌊√n⌋ :
        si i divise n retourner FAUX
    retourner VRAI
```

Exprimez la complexité de cet algorithme en fonction de n puis de la taille de n (utilisez la notation O ou o). Cet algorithme est-il de complexité sous-linéaire ? Linéaire ? Polynomiale ? sous exponentielle ? Exponentielle ?

Exercice 4 *En utilisant l'algorithme d'Euclide et la factorisation d'entier, calculer de deux manières différentes les pgcd suivants :*

$$pgcd(30030, 5733) =? \qquad pgcd(598455, 295927) =?$$

Vous pouvez utilisez votre calculatrice uniquement pour faire des multiplications, divisions, additions et soustractions.
Quelle méthode vous semble la plus efficace ?

Exercice 5 *1. Soit a et b deux entiers. Montrer que $pgcd(a,b) = pgcd(b,r)$ avec r le reste de la division euclidienne de a par b (relation de base pour l'algorithme d'Euclide).*

2. Soit a et b deux entiers impairs avec $b < a$. On pose $r = (a-b)/2^\mu$ avec 2^μ la plus grande puissance de 2 qui dive $a-b$. Montrer que $pgcd(a,b) = pgcd(b,r)$ avec r le reste de la division euclidienne de a par b (relation de base pour l'algorithme dit binaire).

3. Quelle est l'intérêt informatique de la "division binaire" par rapport à la division euclidienne ?

Exercice 6 *Calculer tous les coefficients de Bezout liés aux couples d'entiers* $(17, 13)$ *et* $(18, 14)$.

Exercice 7 *Trouvez toutes les solutions entières x et y telles que*

$$35x + 49y = 14.$$

Pensez à simplifier et aux coefficients de Bezout.

Exercice 8 *Soit $n = p \cdot q$ avec p, q deux nombres premiers différents. Montrez que connaitre n et $\varphi(n) = (p-1)(q-1)$ est équivalent à connaitre p et q (c'est pourquoi il faut garder $\varphi(n)$ secret dans le protocole RSA).*

3 Arithmétique modulaire

Exercice 9 *On se place dans l'anneau $\mathbb{Z}/18\mathbb{Z}$.*

1. Effectuez les additions suivantes :

$$12 + 13, \qquad 19 + 11, \qquad 134 + 177, \qquad 1345 + 1809$$

2. Effectuez les multiplications suivantes

$$10 \times 11, \qquad 22 \times 9, \qquad 130 \times 107, \qquad 1201 \times 108$$

Exercice 10 *Calculer $\varphi(n)$ pour les valeurs de n suivantes :* 231, 144, 10!.

Exercice 11 *1. Combien d'éléments inversibles contiennent les ensembles $\mathbb{Z}/1024\mathbb{Z}$, $\mathbb{Z}/245\mathbb{Z}$?*

2. Donnez les éléments inversibles de $\mathbb{Z}/20\mathbb{Z}$ et $\mathbb{Z}/21\mathbb{Z}$.

Exercice 12 *Donnez l'inverse modulaire de :*
- *45 modulo 13,*
- *48 modulo 17,*
- *53 modulo 101.*

Exercice 13 *Calculez les puissances modulaires suivantes (sans calculatrice et en allant le pus loin possible) :*

$$2^5 \mod 5, \qquad 2^{234} \mod 7, \qquad 57^{234} \mod 11, \qquad 1432^{2034} \mod 13.$$

$$2^5 \mod 35, \qquad 7^{234} \mod 16, \qquad 35^{234} \mod 12, \qquad 81^{2034} \mod 50.$$

4 Protocoles cryptographiques

Exercice 14 *Annie dispose de la clé publique RSA* $(N, e) = (187, 3)$.

1. *Retrouvez la clé de déchiffrement* d.
2. *Thibault, en utilisant la clé publique d'Annie obtient le chiffré* $c = 64$ $(= 2^6)$. *Déchiffrez le message.*

Exercice 15 (RSA avec une porte dérobée) *Lorsque l'on est novice en sécurité, il est naturel d'utiliser des bibliothèques cryptographiques en* boîte noire. *Dans ce contexte, un attaquant peut concevoir des boîtes noires qui fournissent des clés cryptographiques ayant toutes les apparences (statistiques en particulier) de clés aléatoires mais qui en pratique ont une porte dérobée (backdoor). Cette porte dérobée peut ensuite être utilisée pour déchiffrer tous les messages.*

Un peu de lecture grand publique *et* scientifique *à ce sujet :*
[lien: article de numerama.com]
[lien sur ResearchGate: The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone?, A. Young and M. Yung, Crypto'96]

Principe de l'attaque :

- *l'attaquant génère des clés RSA* N_{att} *(k bits),* p_{att} *(k/2 bits),* q_{att} *(k/2 bits),* e_{att} *et* d_{att} *(avec les notations du cours) qu'il conserve pour son usage.*
- *Lors d'une demande de clés par un usager, l'attaquant effectue les étapes suivantes :*
  1. *Il génère aléatoirement un nombre premier* p *de* k *bits exactement avec* $p < N_{att}$, *un nombre aléatoire* r_2 *de* k *bits exactement et calcule* $r_1 = p^{e_{att}} \mod N_{att}$.
  2. *Il calcule* q *le quotient de la division euclidienne de* $r_1||r_2$ *(concaténation de* r_1 *et* r_2*) et* p. *Si* q *n'est pas premier, on recommence à l'étape* 1.
  3. *Soit* $N = pq$, e *un exposant publique,* $d = e^{-1} \mod \varphi(N)$. *Retourner la clé publique* (N, e) *et la clé privée* (p, q, d).

Question : comment l'attaquant peut-il retrouver la clé privée uniquement à partir de la clé publique ?

Exercice 16 (Cryptosystème de Pailler) Génération des clés :

- *Choisir deux nombres premiers* p *et* q.
- *La clé publique est* $N = p \cdot q$ *et la clé privée est* $\varphi = (p-1)(q-1)$.

Chiffrement :
Si m *est le message à chiffrer, choisir* r *un entier aléatoire tel que* $0 < r < N$. *Le chiffré est :*

$$c = (1+N)^m \cdot r^N \mod N^2.$$

Questions :

1. *L'objectif des questions suivantes est de trouver la procédure de déchiffrement.*
   - *Que vaut* $c \mod N$ *?*
   - *On pose* $u = N^{-1} \mod \varphi(N)$. *Pour tout* x *premier avec* N, *que vaut* $x^{Nu} \mod N$ *?*
   - *En déduire une méthode pour retrouver* r *à partir du chiffré* c *et de la clé secrète* $\varphi(N)$.
   - *En déduire la procédure de déchiffrement.*
2. *Soit* c_1 *et* c_2 *les chiffrés de* m_1 *et* m_2. *Donner un chiffré de* $m_1 + m_2$ *?*
3. *Donner une application possible de cette propriété (on parle d'un protocole homomorphe pour l'addition).*

Exercice 17 (Cryptosystème de Boneh-Franklin (2001))

Définition d'un couplage :

Soit $(G_1, +)$ et $(G_2, \times)$ deux groupes. Un couplage sur G_1 et G_2 est une application $e : G_1 \times G_1 \to G_2$ telle que

$$\forall k \in \mathbb{Z}, \forall (x, y) \in G_1^2, \qquad e(kx, y) = e(x, ky) = e(x, y)^k.$$

Private Key Generator :

Le générateur de clés privées (cela pourrait être un fournisseur d'accès) dispose :

- *d'un groupe $(G_1, +)$ cyclique, d'ordre $p + 1$ (p premier) et de générateur g,*
- *d'un autre groupe $(G_2, \times)$ d'ordre q premier divisant $p + 1$,*
- *d'un couplage e sur G_1 et G_2,*
- *d'une clé privée maitre s dans $\mathbb{Z}/q\mathbb{Z}$,*
- *d'une clé publique $K_p = sg$,*
- *d'une fonction de hachage $H_1 : \{0,1\}^\star \to \{0,1\}^n$ (n fixé),*
- *d'une fonction de hachage $H_2 : G_2 \to \{0,1\}^n$,*
- *L'ensemble des messages clairs est $\{0,1\}^n$,*
- *L'ensemble des messages chiffrés est $G_1 \times \{0,1\}^n$.*

Génération des clés pour l'utilisateur :

L'utilisateur possède l'identifiant $Id \in \{0,1\}^\star$ (l'adresse MAC de sa box par exemple). Le PKG calcule

- *$Q_{Id} = H_1(Id) \in G_1^\star$ (public)*
- *$d_{Id} = sQ_{Id}$ (donnée à l'utilisateur qui la garde secrête)*

Chiffrement :

Si m est le message en clair, le chiffré c est :

1. *Récupérer Id et calculer $Q_{Id} = H_1(Id) \in G_1^\star$*
2. *Choisir aléatoirement r dans $\mathbb{Z}/q\mathbb{Z}^\star$*
3. *Calculer $g_{Id} = e(Q_{Id}, K_{pub}) \in G_2$*
4. *retourner $c = (rg, m \oplus H_2(g_{Id}^r))$.*

Question

Donner la procédure de déchiffrement.

Exercice 18 (Monnaie électronique) *Une banque souhaite mettre à la disposition de ses clients de la monnaie électronique. Pour cela, elle dispose d'un groupe (commutatif) G public, d'une fonction à sens unique $f : E \to G$ avec un ensemble E public et d'une fonction à sens unique avec trappe $\varphi : G \to G$. La trappe est gardée secrête par la banque. On suppose de plus que φ est un isomorphisme de groupe, c'est-à-dire, φ est bijective et*

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \qquad \forall (x, y) \in G^2.$$

Cela implique que φ^{-1} est aussi un isomorphisme.

Un client qui souhaite obtenir x unités de monnaie électronique ($x \in E$) doit effectuer les étapes suivantes :

- *il choisit aléatoirement un élément r de G, calcule $y = f(x)\varphi(r)$ et envoie y à la banque.*
- *La banque calcule $z = \varphi^{-1}(y)$ et envoie z au client.*
- *Le client calcule $X = z \cdot r^{-1}$*

Lorsque le client souhaite payer avec sa monnaie électronique, il donne au vendeur le couple (x, X).

1. *Exprimez X en fonction de x.*
2. *Que doit faire un vendeur pour vérifier la validité d'un couple (x', X') ?*
3. *Montrez que la contrefaçon de monnaie électronique est possible si l'on sait inverser φ.*
4. *Montrez que la contrefaçon de monnaie électronique est possible si l'on sait inverser f.*

5 Courbes elliptiques (uniquement pour ceux qui s'ennuient)

Rappels sur les courbes elliptiques : Soit $p > 3$ un nombre premier et $\mathbf{F}_p$ le corps fini à p éléments. Les points d'une courbe elliptique sont le point à l'infini 0_∞ et les couples (X, Y) d'éléments de $\mathbf{F}_p$ qui vérifient l'équation $Y^2 = X^3 + AX + B$, où $A, B \in \mathbf{F}_p$.

Soit $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points d'une courbe elliptique. La loi de groupe est définie de la manière suivante (les calculs se font dans $\mathbf{F}_p$) :

- Pour tout point P, $P + 0_\infty = 0_\infty + P = P$.
- $0_\infty + 0_\infty = 0_\infty$.
- Pour $P = (x, y)$, $-P = (x, -y)$.
- Si $x_1 \neq x_2$, alors $P_1 + P_2 = (x_3, y_3)$ avec

$$(x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1), \quad \lambda = (y_2 - y_1)(x_2 - x_1)^{-1}.$$

- Si $x_1 = x_2$ et $y_1 = -y_2$, alors $P_1 = -P_2$ et $P_1 + P_2 = 0_\infty$.
- Si $x_1 = x_2$ et $y_1 = y_2$, alors $P_1 + P_2 = 2P_1 = (x_3, y_3)$ avec

$$(x_3, y_3) = (\lambda^2 - 2x_1, \lambda(x_1 - x_3) - y_1), \quad \lambda = (3x_1^2 + A)(2y_1)^{-1}.$$

Exercice 19 (Chiffrement Elgamal avec une courbe elliptique)
Génération des clés : *Bob choisit comme courbe elliptique* $E : y^2 = x^3 + 3x + 5 \mod 23$*, un point* $P = (7, 22)$ *et un entier* $s = 11$*.*

1. *Calculez* $2P$*,* $4P$*,* $8P$ *puis* $10P$ *puis* $B = 11P$*.*

La clé secrète de Bob est 11 *et la clé publique est* (E, P, B)*.*

Chiffrement d'un message : *Alice souhaite chiffrer un message. Pour cela, elle dispose d'une procédure qui à une suite de bits, fait correspondre un point de la courbe* E*. Supposons que le message d'Alice correspond au point* $M = (6, 3)$*. Elle tire ensuite au hasard un entier* k*. Nous supposons ici* $k = 2$*.*

2. *Calculer* $C_1 = kP$ *et* $C_2 = M + kB$*.*

Le message chiffré de Alice est le couple (C_1, C_2)*.*
Déchiffrement d'un message : *Bob reçoit* (C_1, C_2) *d'Alice.*

3. *Calculer* $C_2 - sC_1$*. Que constatez-vous ?*