Corrigé
Cryptographie à clé publique

I. Chiffrement multiplicatif (15 pts)

On considère l'anneau $\mathbb{Z}_{30} = \{0, 1, 2, \ldots, 29\}$ des entiers modulo 30.
Rappelons qu'un élément $a \in \mathbb{Z}_{30}$ est inversible si, et seulement si, $\text{pgcd}(a, 30) = 1$.

1. (2pts) Énumérer tous les éléments de $\mathbb{Z}_{30}^\star$ (les éléments de $\mathbb{Z}_{30}$ inversibles).

   Solution. $30 = 2 \times 15 = 2 \times 3 \times 5$, *donc tous les éléments de* $\mathbb{Z}_{30}$ *non divisibles par* $2, 3$ *et* 5 *sont premiers avec* 30. *Il s'agit donc de* $\mathbb{Z}_{30}^\star = \{1, 7, 11, 13, 17, 19, 23, 29\}$.

2. (3pts) Calculer l'inverse dans $\mathbb{Z}_{30}^\star$ des éléments trouvés à la question précédente.

   Solution. *On appliquera l'algorithme d'Euclide étendu pour trouver* U *tel que* $aU + 30V = 1$ *:*

a	1	7	11	13	17	19	23	29
a^{-1}	1	13	11	7	23	19	17	29

3. On définit le procédé de chiffrement multiplicatif sur $\mathbb{Z}_{30}$ de la façon suivante :

$$E_a(x) = ax \mod 30.$$

   (a) (1pt) Calculer le nombre de clés possibles.

   Solution. *C'est exactement les éléments de* $\mathbb{Z}_{30}^\star$ *: il y en a huit.*

   (b) (1pt) Décrire la fonction de déchiffrement D_a pour $a \in \mathcal{K}$.

   Solution. $D_a(y) = a^{-1}y \mod 30$.

   (c) (4pts) Chiffrer le message suivant avec la clé $a = 13$ (vous donnerez le résultat sous la forme du texte correspondant à la suite de nombres) :

   UN ORNITHORYNQUE TRISTE

   Solution. *On obtient finalement le texte chiffré suivant :*

   UTRCLTOHBCLMT, UWRHLOYHW

lettre	*code*	$E_{13}(code)$	*lettre*
A	0	0	A
B	1	13	N
C	2	26	'
D	3	9	J
E	4	22	W
F	5	5	F
G	6	18	S
H	7	1	B
I	8	14	O
J	9	27	.
K	10	10	K
L	11	23	X
M	12	6	S
N	13	19	T
O	14	2	C
P	15	15	P
Q	16	28	,
R	17	11	L
S	18	24	Y
T	19	7	H
U	20	20	U
V	21	3	D
W	22	16	Q
X	23	29	(espace)
Y	24	12	M
Z	25	25	Z
'	26	8	I
.	27	21	V
,	28	4	E
(espace)	29	17	R

(d) (4pts) Identifier et expliquer quelles sont les vulnerabilités d'un tel cryptosystème.

Solution. *1. Il s'agit d'un chiffrement symétrique, la clé de déchiffrement peut être facilement déduite à partir de la clé de chiffrement (c'est l'inverse modulo 30).*

2. *C'est un chiffrement détérministe, de substitution mono-alphabétique, il peut donc être cassé facilement par une analyse des fréquences des lettres.*
3. *L'espace de clés est de petite taille. Une recherche exhaustive de la clé est possible dans un temps raisonable.*
4. *C'est un chiffrement homomorphe par rapport à l'opération d'addition :*

$$E_a(x+y) = ax + ay = E_a(x) + E_a(y) \mod 30.$$

5. *C'est un chiffrement commutative :*

$$E_b(E_a(x)) = E_a(E_b(x)) = E_{ba}(x).$$

II. Factorisation (3 pts)

1. (1pt) En admettant que l'entier 14803 est le produit de deux nombres premiers, pouvez-vous facilement le factoriser ? Expliquez pourquoi.

   Solution. *La factorisation est un problème connu comme difficile. La méthode naïve pour factoriser un entier n est en $\mathcal{O}(n^{1/2})$ opérations : on divise n par tous les entiers inférieurs à $\sqrt{n}$. Dans notre cas on a besoin de faire au maximum 121 divisions.*

2. (2pts) Si en outre, on révèle que $\varphi(14803) = 14560$, la factorisation est-elle possible ? Donnez les deux facteurs.

   Solution. *Ecrivons $n = pq$. On a donc $\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$, et ainsi $p + q = n - \varphi(n) + 1 = 14803 - 14560 + 1 = 244$. Les nombres p et q sont racines du polynome*

$$P(X) = X^2 - (p+q)X + pq = X^2 - 244X + 14803.$$

   Le discriminant est $\Delta = 244^2 - 4 \times 14803 = 324 = 18^2$ et ainsi $p = (244 - 18)/2 = 113$ et $q = (244 + 18)/2 = 131$.

III. Fonctions de hachage (7 pts)

Le but de l'exercice est de montrer les liens d'implication ou de non-implication parmi les propriétés des fonctions de hachage :

Propriétés

- **Résistance à la préimage** : étant donné h, on ne peut pas trouver en un temps raisonnable de x tels que $h = H(x)$
- **Résistance à la seconde préimage** : étant donné x, on ne peut pas trouver en un temps raisonnable de $y \neq x$ tels que $H(y) = H(x)$
- **Résistance aux collisions** : on ne peut pas trouver en un temps raisonnable de couples x et y tels que $H(x) = H(y)$

1. (2pts) Montrer une relation entre la résistance à la seconde préimage et la résistance aux collisions d'une fonction de hachage.

   Solution. *La résistance aux collisions implique la résistance à la seconde préimage.*
   Pour la résistance à la seconde préimage, l'attaquant reçoit un x fixé et il doit trouver un y different de x tel qu'ils ont la même empreinte $H(y) = H(x)$. Pour la résistance aux collisions, l'adversaire est libre à choisir les deux messages x et y tels que leurs empreintes coincident.
   S'il existe un attaque pour trouver une seconde péimage, on peut facilement l'utiliser pour trouver une collision : On veux trouver de $y \neq x$ tels que $H(y) = H(x)$. Fixons un x au hasard. D'après notre hypothèse on peut facilement trouver un $y \neq x$ tel que $H(y) = H(x)$, d'où la collision.

2. Considérons la fonction $f : \mathbb{Z} \to \mathbb{Z}_n$ définie par $f(x) = x^2 \mod n$ pour n un module RSA.

   (a) (1pt) Justifier que la fonction f est résistante à la préimage.
   Solution. *Lorsque n est un module RSA (le produit de deux grands nombres premiers), l'extraction d'une racine carrée modulo n est un problème réputé difficile, la fonction f est donc résistante à la préimage.*

   (b) (1pt) Justifier que la fonction n'est pas résistance à la seconde préimage.
   Solution. *Puisque $f(x) = f(-x)$, cette fonction n'est pas résistante à la seconde préimage.*

   Ainsi, la résistance à la préimage n'entraîne pas la résistance à la seconde préimage.

3. Considérons une fonction de hachage $g : \{0,1\}^* \to \{0,1\}^n$ résistante à la collision. Considérons ensuite la fonction de hachage h qui calcule des empreintes de longueur $n+1$ construites de la façon suivante :

$$h : \{0,1\}^* \to \{0,1\}^{n+1}$$

$$h(x) = \begin{cases} 1|x & \text{si } x \text{ est de longueur } n \\ 0|g(x) & \text{sinon} \end{cases}$$

   où $|$ désigne l'opération de concaténation.

   (a) (1pt) Montrer que cette fonction est résistante à la collision
   Solution. *Cette fonction est résistante à la collision notamment car g l'est : Si $h(x) = h(y)$ alors le premier bit ne peut etre égal à 1 car sinon on aurait $h(x) = 1|x = h(y) = 1|y$ donc $x = y$ (ce ne serait plus une collision). Donc le premier bit est 0 et on a nécessairement $g(x) = g(y)$, ce qui veut dire que x et y forment une collision sur g. Par hypothèse, g est résistante aux collisions, donc x et y sont difficiles à trouver, et donc h est résistante aux collisions.*

   (b) (1pt) Montrer que cette fonction n'est pas résistante à la préimage
   Solution. *Cette fonction n'est pas résistante à la préimage car il est facile de déterminer un antécédent pour la moitié des images (celles qui commencent par 1). L'antécédent de la valeur $h = 1|x$ est juste la suite binaire x.*

   Ainsi, la résistance à la collision n'entraîne pas la résistante à la préimage.

4. (1pt) Donner un exemple de fonction résistante aux collisions et à la seconde préimage, mais pas à la préimage. Est-ce une fonction de hachage ?

   Solution. *La fonction identité est résistante (infiniment) aux collisions et aux secondes préimages. Par contre, ce n'est pas une fonction de hachage car elle ne condense pas le message.*

IV. Signature RSA (3 pts)

Alice a mis à la disposition du public les clés publiques RSA ($e = 17, n = 437$). Elle garde secret l'exposant d.

Algorithmes

- **Génération des clés**
  $\mathsf{pk} : \mathsf{n},\ \mathsf{e}\ (\mathsf{mod}\varphi(\mathsf{n}))$
  $\mathsf{sk} : \mathsf{d}\ (\mathsf{mod}\varphi(\mathsf{n}))$
- **Signature**
  $\mathcal{S}(\mathsf{d}, \mathsf{m}) = \sigma$
  $\sigma = m^{d}\ (\mathsf{mod}\ \mathsf{n})$
- **Vérification**
  $\mathcal{V}(\mathsf{e}, \mathsf{m}, \sigma) = \mathsf{oui/non}$
  $m \stackrel{?}{=} \sigma^{e}\ (\mathsf{mod}\ \mathsf{n})$

1. (1pt) Générer une signature valide σ (sans contrôle sur le message m signé).
2. (1pt) Soient $(m_1, \sigma_1) = (100, 156)$ et $(m_2, \sigma_2) = (2, 257)$ deux documents signés par Alice. Montrer qu'il est facile de fabriquer une signature valide pour le message $m = 200$.
3. (1pt) Montrer une attaque à clairs choisis qui permet de signer n'importe quel message m. (Falsification Universelle)

Solution. *1. Falsification Existentielle : On peut choisir une valeur σ au hasard et calculer le message m pour lequel σ est une signature valide de la manière suivante : $m = \sigma^e \mod n$.*

2. En utilisant la propriété de homomorphisme par rapport à la multiplication de la signature RSA on obtient une signature valide pour le message $m_1 m_2 = 200$ en faisant le produit de deux signatures $\sigma_1 \sigma_2 = 325 \mod 437$.

3. Falsification Universelle : On peut signer n'importe quel message m en demandant deux signatures σ_1, σ_2 pour les messages clairs $m_1 = m/2$ et $m_2 = 2$. Pour obtenir la signature valide du message m on n'a que à multiplier les signatures σ_1 et σ_2.

V. Preuves de connaisance sans divulgation (6 pts)

Le but de l'exercice est de s'identifier en tant que le possesseur d'une clé publique El Gamal.
On rappelle l'algorithme de génération de clés ElGamal :

Clés ElGamal

- Soit un premier p et le groupe cyclique $\mathbb{Z}_{\mathsf{p}}^{\star}$
- Soit q un diviseur premier de $(\mathsf{p} - 1)$.
- Soit $\mathsf{g} \in \mathbb{Z}_{\mathsf{p}}^{\star}$ un élément d'ordre q.
- Soit une clé secrète $\mathsf{sk} : \mathsf{x}\ (\mathsf{mod}\ \mathsf{q})$.
- Soit la clé publique $\mathsf{pk} : \mathsf{y} = \mathsf{g}^{\mathsf{x}}\ (\mathsf{mod}\ \mathsf{p})$.

Alice prétend être en possession de la clé secrète x associée à la clé publique y.

1. (2pts) Comment Alice, peut-elle prouver la validité de sa clé publique y sans révéler sa clé secrète x.

   Solution. *Le protocole de Schnorr est un protocole de divulgation nulle de connaissance pour le secret x associé à une clé publique $y = g^x \mod p$. Le protocole est illustré dans la figure 1.*

2. (2pts) Montrer deux moyens differents qui permetent à Alice de tricher dans le protocole précédent.

Alice		Bob
$r \leftarrow \$ \mod q$		
$t = g^r \mod p$	$\xrightarrow{t}$	
	$\xleftarrow{e}$	$e \in \{0,1\}$
$s = r - ex \mod q$	$\xrightarrow{s}$	$t \stackrel{?}{=} g^s y^e \mod p$

FIGURE 1 – Protocole de Schnorr

Solution. *Alice ne connaissant pas x a deux choix :*

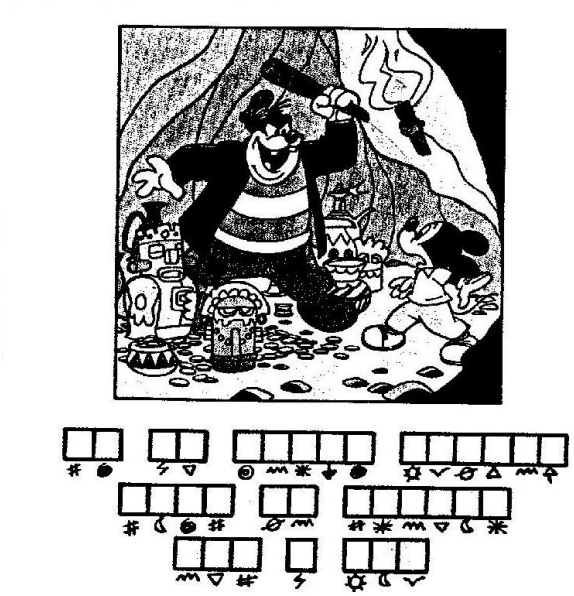
(a) Alice ne triche pas lors de la première étape :
(calcul et envoi de $t = g^r$)
— *Si $e = 0$ elle pourra répondre toujours correctement à la question du Bob avec $s = r$.*
— *Si $e = 1$, elle devra choisir un nombre au hasard s, et il n'a pas plus d'une chance sur $q - 1$ de tomber sur $r - ex$.*

(b) Alice triche lors de l'envoi de t. Dans ce cas, elle peut parier dès le départ sur le bit e que Bob enverra :
— *Si elle parie $e = 0$, elle envoie effectivement $t = g^r$, puis ensuite $s = r$.*
— *Si elle parie $e = 1$, elle envoie alors $t = g^r y \mod p$, puis ensuite $s = r$ qui vérifie bien $t = g^s y$.*

3. (2pts) Avec quelle probabilité aura-t-elle la chance de nous faire croire qu'elle posède le secret x après 20 executions du protocole ?

Solution. *Alice a une chance sur deux de gagner dans chacun des deux cas.*
Avec un tour de ce protocole, Alice a une probabilité p de faire le bon choix (avec $p \approx 1/2$ si q est grand). En répétant ce protocole 20 fois, Bob pourra s'assurer de la honnêteté d'Alice : la probabilité qu'elle lui faire croire qu'elle posède le secret sans le connaître en réalité est $\approx \frac{1}{2^{20}}$.

• Question bonus (1 pt)



Que dit Pat à Mickey ?
(Source : Le Journal de Mickey, n 2119, p. 46)

Solution. *"Tu as perdu Mickey tout ce tresor est à moi"*