**Exercice 1.** Deux documents $d_1 = 12$ et $d_2 = 13$ sont accompagnés d'une signature numérique, $\sigma_1 = 363$ pour $d_1$ et $\sigma_2 = 227$ pour $d_2$, produites à l'aide d'une clé RSA dont le module est 1 833 et l'exposant public est 3. Les signatures de ces deux documents sont-elles correctes ?

**Exercice 2.** Soit $p = 499$ et $g = 7$ un générateur de $\mathbb{Z}/p\mathbb{Z}^*$ les paramètres d'un schéma de signature ElGamal.

1. Le document $d = 300$ est accompagné de la signature $\sigma = (232, 282)$. La clé publique est $y = 173$. Cette signature est-elle correcte ?
2. La signature du message $m_1 = 400$ est $(r, s) = (95, 197)$. Un adversaire sait que l'aléa $k$ qui a servi à l'élaboration de cette signature est $k = 299$. Quelle est la clé privée du signataire ?
3. Deux messages $m_1 = 100$ et $m_2 = 200$ ont pour signatures respectives $\sigma_1 = (417, 214)$ et $\sigma_2 = (417, 20)$. Un adversaire sait donc que ces signatures ont été élaborées avec le même aléa $k$. Quel est cet aléa ? Quelle est la clé privée du signataire ?

**Exercice 3.** Soient $E$ et $F$ deux ensembles finis. Soient $f_0$ et $f_1$ deux fonctions à sens unique $E \to F$. On dit que $\{f_0, f_1\}$ est une paire de fonctions qui ne *se rencontrent pas* s'il est difficile de trouver un couple $(a, b) \in E \times E$ tel que $f_0(a) = f_1(b)$.

1. Soit $p$ un nombre premier suffisamment grand, $g$ un générateur de $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ et $c$ un élément de $\mathbb{Z}/p\mathbb{Z}$ dont le calcul du logarithme en base $g$ est difficile.
   Démontrer que $f_0 : \begin{array}{ccc} \{1,\dots,p-1\} & \to & \mathbb{Z}/p\mathbb{Z} \\ x & \mapsto & g^x \end{array}$ et $f_1 : \begin{array}{ccc} \{1,\dots,p-1\} & \to & \mathbb{Z}/p\mathbb{Z} \\ x & \mapsto & cg^x \end{array}$ forment une paire de fonctions qui ne se rencontrent pas.
2. Soit $e \in \{1,\dots,p-1\}$ dont un antécédent par $f_0$ ou $f_1$ est difficile à trouver. Démontrer que $F : \begin{array}{ccc} \{0,1\}^* & \to & \mathbb{Z}/p\mathbb{Z} \\ x_1x_2\cdots x_k & \mapsto & f_{x_1} \circ f_{x_2} \circ \cdots \circ f_{x_k}(e) \end{array}$ est résistante aux collisions fortes.

**Exercice 4.** Deux correspondants utilisent le schéma de signature de ElGamal avec la clé publique $(p, g, y = g^x)$ et la clé privée $x$. Un message $m$ est accompagné de la signature $(r, s)$. Un bug dans l'algorithme de vérification de signature fait qu'un message accompagné d'une signature $(r, s)$ avec $r \geq p$ est également acceptée. Montrer comment un adversaire peut faire accepter comme valide un nouveau message $\mu$, premier avec $p - 1$ sans connaître la clé privée $x$ s'il connaît $m$ et sa signature $(r, s)$.

**Exercice 5.** On utilise les même notations que dans l'exercice précédent. On suppose que $p \equiv 1 \pmod 4$. On suppose que $g$ divise $p - 1$, soit $p - 1 = gt$. On note $H$ le sous-groupe de $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ d'ordre $g$ engendré par $g^t$.

1. On suppose que $g$ est assez petit pour qu'un adversaire puisse calculer le logarithme discret dans $H$. Montrer qu'il est possible de trouver $z$ tel que $g^{tz} = y^t \pmod p$.
2. Montrer que $g^{(p-1)/2} \equiv -1 \pmod p$, puis que $t^{(p-3)/2} \equiv g \pmod p$.
3. Un adversaire voulant signer le message $m$ calcule $r = t$ et $s = 1/2(p-3)(m - tz) \bmod (p-1)$. Montrer que cette signature est acceptée comme valide.