Exercice 1.
$\sigma_1^3 = 12 \pmod{1\,833}$, la signature est correcte. $\sigma_2^3 = 710 \pmod{1\,833}$, la signature n'est pas correcte.

Exercice 2.
1. $g^m = 166$, $y^r r^s = 166$, la signature est correcte.
2. L'adversaire sait que modulo 498, la clé privée x est solution de l'équation $m = xr + ks$, *i.e.* $95x \equiv 400 - 299 \times 197 \pmod{498}$; $x \equiv 261 \times 173 \pmod{498}$; $x = 333$.
3. L'aléa k est solution de $k(s_1 - s_2) = m_1 - m_2 \pmod{498}$; $194k \equiv -100 \pmod{498}$, $194k = -100 + 498u$; $97k = -50 + 249u$; $k = -50 \times 172 \pmod{299}$; $k = 115$. On trouve la clé privée $x = 112$ comme au 1.

Exercice 3.
1. Si f_0 et f_1 se rencontrent, on connaît a et b dans $\{1, \ldots, p-1\}$ tels que $g^a = cg^b$, c-à-d $c = g^{a-b}$. Le logarithme de c en base g serait donc facile.
2. Si F n'était pas résistante aux collisions fortes, on pourrait trouver $x = x_1 \cdots x_k$ et $x' = x'_1 \cdots x'_k$ tels que $F(x) = F(x')$. Si $x_1 \neq x'_1$, on peut supposer que $x_1 = 0$ et $x'_1 = 1$. Alors $a = F(x_2 \cdots x_k)$ et $b = F(x'_2 \cdots x_k)$ vérifient $f_0(a) = f_1(b)$. Si $x_1 = x'_1$, alors $x_2 \ldots x_k$ et $x'_2 \cdots x'_k$ fournissent également une collision pour F. Si x n'est pas préfixe de x'(ou l'inverse), on peut recommencer le raisonnement jusqu'à obtenir une différence sur le premier terme. Si x est préfixe de x', soit $x' = xy$ (ou l'inverse), on trouve $f_1(y) = e$, ce qui fournit un antécédent de e.

Exercice 4
Soit (r, s) une signature valide pour m, *i.e.* $y^r r^s = g^m$. Comme m est inversible modulo $(p-1)$, on peut poser m' l'inverse de m modulo $(p-1)$ et $r' = r + p(r\mu m' - r)$ et $s' = s\mu m' \bmod (p-1)$. On a $r' \equiv r\mu/m \bmod (p-1)$ et $r' \equiv r \bmod p$. Par conséquent, $y^{r'} r'^{s'} = y^{r\mu/m} r^{s\mu/m} = (y^r r^s)^{\mu/m} = (g^m)^{\mu/m} = g^\mu$. La signature est reconnue comme valide.

Exercice 5
1. Soit $\alpha = g^t$. Comme on suppose qu'il est possible de calculer un logarithme en base α, on peut trouver z, qui est le logarithme de y^t en base α.
2. La relation $gt = p-1$ signifie que g est l'inverse de $-t$ modulo p. D'après le petit théorème de Fermat, $g^{p-1} = 1$. Donc $g^{(p-1)/2}$ est une racine carrée de 1. C'est donc ± 1. Comme g est un élément générateur, ce n'est pas 1. C'est donc -1. Comme $p \equiv 1 \pmod 4$, $\frac{p-1}{2}$ est pair. Donc $(gt)^{(p-1)/2} = (-1)^{(p-1)/2} = 1$. D'après $g^{(p-1)/2} = -1$, on a $t^{(p-1)/2} = t \cdot t^{(p-3)/2} = -1$. Le second facteur $t^{(p-3)/2}$ est l'inverse de $-t$ modulo p. D'après la remarque ci-dessus, c'est g.
3. On a $y^t t^s = g^{tz} t^{(p-3)/2 \times (m-tz)} = g^{tz} \times g^{m-tz} = g^m$. La signature est donc considérée comme valide.