

ENSI BOURGES : MASTER « SÉCURITÉ INFORMATIQUE »

Systemes cryptographiques : signature électronique

Emmanuel Bresson – ÉNS-DGA

CORRIGÉS DES EXERCICES DU 19/03/2002

N'hésitez pas à me contacter si vous avez des questions ou si vous apercevez des erreurs.

emmanuel@bresson.org

1. Signature RSA.

(★)

1. Avec $p = 19$ et $q = 23$, on a $N = p \times q = 437$ et $\varphi(N) = (p - 1)(q - 1) = 396$.
2. $e = 9$ n'est pas un exposant de vérification correct car il divise $p - 1$. De même, $e = 14$ ne convient pas car on a $\text{pgcd}(e, \varphi(N)) = \text{pgcd}(14, 396) = 2$.
 $e = 17$ en revanche convient et on peut calculer l'exposant de signature correspondant par l'algorithme d'Euclide étendu :

$$\begin{array}{cccccc|l} 1 & 0 & 396 & 0 & 1 & 17 & \rightarrow 396 = 17 \times \mathbf{23} + 5 \\ 0 & 1 & 17 & 1 & -23 & 5 & \rightarrow 17 = 5 \times \mathbf{3} + 2 \\ 1 & -23 & 5 & -3 & 70 & 2 & \rightarrow 5 = 2 \times \mathbf{2} + 1 \\ -3 & 70 & 2 & 7 & -163 & 1 & \rightarrow 2 = 1 \times \mathbf{2} + 0 \\ 7 & -163 & 1 & -17 & 396 & 0 & \text{On a donc } 7 \times 396 + (-163) \times 17 = 1 \end{array}$$

Donc, modulo $\varphi(N)$, i.e. modulo 396, on a $17(-163) = 1$.

D'où $d = -163 = 233 \pmod{396}$.

3. $\text{SIGN}(100, 233) = 100^{233} \pmod{437}$. On a $233 = 128 + 64 + 32 + 8 + 1$ donc on calcule :

$$\begin{aligned} 100^{233} &= 100 \times \left(100 \times \left(100 \times \left(100 \times 100^2 \right)^2 \right)^4 \right)^8 \pmod{437} \\ &= 100 \times \left(100 \times \left(100 \times 144^2 \right)^4 \right)^8 \pmod{437} \\ &= 100 \times \left(100 \times (35)^4 \right)^8 \pmod{437} \\ &= 100 \times 196^8 \pmod{437} \\ &= 100 \times 289^2 \pmod{437} \\ &= 156 \end{aligned}$$

4. On calcule $156^{17} \pmod{437}$. On a $17 = 16 + 1$ donc on calcule :

$$\begin{aligned} 156^{17} &= 157 \times (156^4)^4 = 156 \times (142)^4 \pmod{437} \\ &= 156 \times 348 = 100 \pmod{437} \end{aligned}$$

2. Signature et chiffrement.

(**)

-
1. Bob fait succesivement $V_A(c, \sigma) \stackrel{?}{=} \text{OK}$, puis $m \leftarrow D_B(c)$.
 2. Charlie remplace σ par σ' et pretend que c'est lui qui a donné sa réponse en premier, avant Alice.
 3. Il vaut mieux faire $\sigma \leftarrow S_A(m)$, puis $c \leftarrow E_B(m, \sigma)$ et envoyer le couple (c, σ) . Bob fera $(m, \sigma) \leftarrow D_B(c)$, puis $V_A(m, \sigma) \stackrel{?}{=} \text{OK}$.
-

3. Signature El Gamal.

(*)

On considère la méthode de signature d'El Gamal, avec $p = 499, g = 2, x = 129$

1. $p = 499$ est un nombre premier (il suffit de tenter une division par 2,3,5,7,11,13,17 ou 19 pour s'en apercevoir) et $g^{(p-1)/2} \neq 1$ donc g est d'ordre $p - 1$ (générateur).
2. $y = g^x = 2^{129} \bmod p$. Comme $129 = 128 + 1$, ça va très vite :

$$2^{129} = 2 \times (2^{16})^8 = 2 \times (65536)^8 = 2 \times 444^4 = 2 \times 462 = 425 \bmod 499$$

3. $k = 64$ est un mauvais choix de nombre aléatoire, car on ne pourrait peut-etre pas trouver b tel que $m = xa + kb \bmod (p - 1)$. On peut verifier que pour tous les b allant de 1 à 498, $100 \neq 129 \times (2^{64} \bmod 499) + 64 \times b$. Mais il y a d'autres valeurs de m qui donnerait une égalité. Ainsi $a = 31 = 2^{64} \bmod 499$, $b = 111$ et $m = 147$ vérifient l'égalité : $147 = 129 \times 31 + 64 \times 111 \bmod 498$.

$k = 211$ est un bon choix car $\text{pgcd}(211, 498) = 1$, donc on pourra diviser par k :

1	0	498	0	1	211	→ 498 = 211 × 2 + 76
0	1	211	1	-2	76	→ 211 = 76 × 2 + 59
1	-2	76	-2	5	59	→ 76 = 59 × 1 + 17
-2	5	59	3	-7	17	→ 59 = 17 × 3 + 8
3	-7	17	-11	26	8	→ 17 = 8 × 2 + 1
-11	26	8	25	-59	1	→ 8 = 1 × 8 + 0
25	-59	1	0	On a donc 25 × 498 + (-59) × 211 = 1 mod 498

L'inverse de 211 est donc -59 qui vaut 439 modulo 498. La signature est $a = g^k = 2^{211} \bmod 498 = 37$ et $b = (m - xa) \times k^{-1} = (100 - 129 * 37) \times 439 \bmod 498 = 313$.

4. On calcule les deux valeurs suivantes :

$$\begin{aligned} g^m &= 2^{100} = \left(2 \times (2^6)^4\right)^4 = (2 \times 64^4)^4 \\ &= (2 \times 241)^4 = 165 \bmod 499 \\ y^a a^b &= 425^{37} \times 37^{313} = 432 * 288 = 165 \bmod 499 \end{aligned}$$

4. Attaques sur la signature d'El Gamal.

(***)

1. Avec $a = 83, b = 102$ et $y = 77, p = 499, g = 2, m = 100$ on a :

$$\begin{aligned} g^m &= 2^{100} = 165 \pmod{499} \quad \text{Comme précédemment !} \\ y^a a^b &= 77^{83} \times 83^{102} = 1 * 165 = 165 \pmod{499} \end{aligned}$$

2. Soit $(r, s, t) = (1, 2, 3)$. On calcule $\text{pgcd}(ra - tb, p - 1) = \text{pgcd}(-223, 498)$:

1	0	498	0	1	-223	→ 498 = -223 × -2 + 52
0	1	-223	1	2	52	→ -223 = 52 × -5 + 37
1	2	52	5	11	37	→ 52 = 37 × 1 + 15
5	11	37	-4	-9	15	→ 37 = 15 × 2 + 7
-4	-9	15	13	29	7	→ 15 = 7 × 2 + 1
13	29	7	-30	-67	1	→ 7 = 1 × 7 + 0
-30	-67	1	0	On a donc -30 × 498 + (-67) × (-223) = 1 mod 498

Par conséquent l'inverse de $ra - tb$ est $u = -67$ modulo 498 soit encore $u = 498 - 67 = 431$.

3. Si $\alpha = a^r g^s y^t \pmod{p}$ et $\beta = \alpha b u \pmod{p-1}$ constituent la signature d'un message μ , alors on doit avoir $y^\alpha \times \alpha^\beta = g^\mu \pmod{p}$. Calculons :

$$\begin{aligned} y^\alpha \alpha^\beta &= y^\alpha (a^r g^s y^t)^\beta = y^\alpha \left((g^k)^r g^s y^t \right)^\beta \quad \text{puisque } a \text{ est de la forme } g^k \\ &= y^\alpha g^{kr\beta} g^{s\beta} y^{t\beta} = y^\alpha g^{krabu} g^{sabu} y^{tabu} \quad \text{en développant} \\ &= y^\alpha g^{r\alpha u(m-xa)} g^{sabu} y^{tabu} \quad \text{en utilisant le fait que } m = xa + kb \\ &= (g^x)^\alpha g^{r\alpha u(m-xa)} g^{sabu} (g^x)^{tabu} \quad \text{en remplaçant } y \text{ par } g^x \\ &= g^{x\alpha} g^{r\alpha u m} g^{-x\alpha u r a} g^{sabu} g^{x\alpha u t b} \quad \text{on met un peu d'ordre...} \\ &= g^{x\alpha} g^{r\alpha u m} g^{x\alpha u (tb-ra)} g^{sabu} \quad \text{en groupant le dernier et l'avant-avant-dernier} \\ &= g^{x\alpha} g^{r\alpha u m} g^{-x\alpha} g^{sabu} \quad \text{en utilisant } u(tb - ra) = -1 \pmod{p-1}. \\ &= g^{x\alpha - x\alpha} g^{r\alpha u m} g^{sabu} \quad \text{en regroupant, les } x\alpha \text{ vont disparaître} \\ &= g^{\alpha u (rm+sb)} \quad \text{qui est de la forme } g^{\text{quelque chose}} \end{aligned}$$

Donc si on pose $\mu := \alpha u (rm + sb)$, le couple (α, β) est bien une signature de μ puisqu'il vérifie : $y^\alpha \alpha^\beta = g^\mu$! Avec les valeurs choisies, on $\mu = 201 \times 348 \times (1 \times 100 + 2 \times 102) = 90 \pmod{498}$. Sans connaître la clé secrète, et simplement en sachant que $(83, 102)$ était une signature du message $m = 100$, on a donc fabriqué $(201, 348)$, qui est la signature d'un message $\mu = 90$ (qu'on n'a pas choisi !). Note : la valeur commune de cette signature (i.e. la valeur commune de g^μ et $y^\alpha \alpha^\beta$) est ici 371.

4. Que dire de la valeur aléatoire k sous-jacente à cette contrefaçon ? On ne la connaît pas ! On a fabriqué une contrefaçon sans connaître le nombre aléatoire k associé.

5. Attaques sur la signature d'El Gamal.

(***)

1. En connaissant k , Charlie retrouve la clé secrète x à partir de la signature (a, b) d'un message m en calculant $(m - kb)/a \pmod{p-1}$ (c'est x !).
2. $p = 499, g = 2, y = 127$; premier cas : $m = 50, a = 148, b = 10, k = 47$. On voit que a n'est pas premier avec $p-1$ car ils sont tous les deux pairs. Donc il ne peut pas y avoir deux nombres u et v tels que $au + (p-1)v = 1$. Autrement dit, a n'a pas d'inverse modulo $p-1$. L'attaque est inopérante ici !
Deuxième cas. $m = 25, a = 149, b = 79, k = 109$. On essaie de trouver $1/a$ modulo 498. Algorithme d'Euclide (étendu) :

$$\begin{array}{r|l}
 1 & 0 & 498 & 0 & 1 & 149 & \rightarrow 498 = 149 \times \mathbf{3} + 51 \\
 0 & 1 & 149 & 1 & -3 & 51 & \rightarrow 149 = 51 \times \mathbf{2} + 47 \\
 1 & -3 & 51 & -2 & 7 & 47 & \rightarrow 51 = 47 \times \mathbf{1} + 4 \\
 -2 & 7 & 47 & 3 & -10 & 4 & \rightarrow 47 = 4 \times \mathbf{11} + 3 \\
 3 & -10 & 4 & -35 & 117 & 3 & \rightarrow 4 = 3 \times \mathbf{1} + 1 \\
 -35 & 117 & 3 & 38 & -127 & 1 & \rightarrow 3 = 1 \times \mathbf{3} + 0 \\
 -38 & -127 & 1 & \dots & \dots & 0 & \text{On a donc } 38 \times 498 + (-127) \times 149 \\
 & & & & & & = 1 \pmod{498}
 \end{array}$$

Par conséquent l'inverse de a vaut ici $-127 = 498 - 127 = 371 \pmod{498}$. Et on trouve pour x : $(25 - 109 * 79) * 371 = 300 \pmod{498}$.

3. Si les deux signatures utilisant une même valeur pour k (et donc pour a) sont valides, on a :

$$g^{m_1} = y^a a^{b_1} \quad \text{et} \quad g^{m_2} = y^a a^{b_2} \pmod{p}$$

En divisant membre à membre les égalités, les termes y^a vont se simplifier, et on obtient :

$$g^{m_1 - m_2} = a^{b_1 - b_2} = g^{k(b_1 - b_2)} \quad (\text{car même valeur pour } k!)$$

Dès lors, puisque les puissances sont égales modulo p , les exposants sont égaux modulo $(p-1)$, donc :

$$m_1 - m_2 = k(b_1 - b_2) \pmod{p-1}$$

4. Si on suppose que $\text{pgcd}(b_1 - b_2, p-1) = 1$, il est facile de calculer $k = \frac{m_1 - m_2}{b_1 - b_2} \pmod{p-1}$.

5. Avec $m_1 = 62, b_1 = 208, m_2 = 99, b_2 = 21$, on a donc $b_1 - b_2 = 187$. On commence donc par l'algorithme d'Euclide étendu pour trouver l'inverse de $(b_1 - b_2)$, c'est-à-dire de 187 :

$$\begin{array}{r|l}
 1 & 0 & 498 & 0 & 1 & 187 & \rightarrow 498 = 187 \times \mathbf{2} + 124 \\
 0 & 1 & 187 & 1 & -2 & 124 & \rightarrow 187 = 124 \times \mathbf{1} + 63 \\
 1 & -2 & 124 & -1 & 3 & 63 & \rightarrow 124 = 63 \times \mathbf{1} + 61 \\
 -1 & 3 & 63 & 2 & -5 & 61 & \rightarrow 63 = 61 \times \mathbf{1} + 2 \\
 2 & -5 & 61 & -3 & 8 & 2 & \rightarrow 61 = 2 \times \mathbf{30} + 1 \\
 -3 & 8 & 2 & 92 & -245 & 1 & \rightarrow 2 = 1 \times \mathbf{2} + 0 \\
 92 & -245 & 1 & \dots & \dots & 0 & \text{On a donc } 92 \times 466 + (-245) \times 187 \\
 & & & & & & = 1 \pmod{498}
 \end{array}$$

Par conséquent l'inverse de 187 vaut ici $-245 \pmod{498}$. Et on trouve pour k : $-37 * (-245) = 101 \pmod{498}$.

Remarque : On n'a besoin ni de y ni de a pour effectuer ce calcul.

Remarque : Avec la première partie de l'exercice, connaissant k , on peut maintenant retrouver x ; on vérifiera que pour $y = 166, x = 264$ convient.

6. Fonctions de hachage.

(**)

- $|M| > 2|E|$ signifie que les messages font au moins un bit de plus que les empreintes (par ex. 2^{129} et 2^{128}). Cela correspond bien à l'utilisation courante d'une fonction de hachage.
- Soit **Procédure** $P(e \in E) \rightarrow m \in M$ tel que $H(m) = e$.
On suppose qu'on dispose de la procédure P . On utilise l'algorithme suivant :

Entrée : rien

Sortie : "Échec" ou une collision

- Choisir un message m au hasard dans M .
- Calculer son empreinte $e := H(m)$
- Calculer $m' := P(e)$. (NB : on a donc $H(m') = e = H(m)$)
- If $m = m'$ Then Return "Échec"
Else Return (m', m) (une collision)

- En moyenne chaque empreinte correspond à $x = |M|/|E|$ messages, ce qui est supérieur à deux d'après la question 1. L'idée est que m' a $x - 1$ chances sur x d'être différents de m , ce qui est supérieur à une chance sur deux.
- Si le fait de disposer d'un *inverseur* permet de trouver des collisions, le fait d'être à collisions difficiles montre que, justement, on ne dispose pas d'un tel inverseur. C'est-à-dire que la fonction est à sens unique.

7. Fonction de hachage de Chaum-van Heijst-Pfitzmann.

(***)

1. Une empreinte $H(m)$ est un élément de \mathbb{Z}_p^* .
2. Si $H(m_1, m_2) = H(m_3, m_4)$ est une collision, alors on a $g^{m_1 - m_3} = h^{m_4 - m_2} \pmod p$. Le pgcd $d = \text{pgcd}(m_2 - m_4, p - 1)$ est par définition un diviseur de $p - 1$. Ses valeurs peuvent être 1, 2, q ou $p - 1$: ce sont les seuls diviseurs de $p - 1$.

3. On examine les 4 cas un par un :

- Cas $d = 1$. Celà signifie donc que $(m_4 - m_2)$ est inversible modulo $p - 1$. Notons $x = 1/(m_4 - m_2) \pmod{p - 1}$. On a alors $x(m_4 - m_2) = 1 \pmod{p - 1}$ et on peut écrire :

$$h = h^1 = h^{x(m_4 - m_2)} = (h^{m_4 - m_2})^x = (g^{m_1 - m_3})^x = g^{x(m_1 - m_3)} \pmod p$$

Dans ce cas, le logarithme discret de h en base g vaut $x(m_1 - m_3)$.

- Cas $d = 2$. $m_4 - m_2$ n'a pas d'autre facteurs communs avec $p - 1$ que 2 (sinon, 2 ne serait pas le pgcd). Donc $m_4 - m_2$ n'a pas de facteur premier commun avec q : ils sont premiers entre eux. On a donc $\text{pgcd}(m_4 - m_2, q) = 1$; $m_4 - m_2$ est inversible modulo q . On appelle x son inverse : $x(m_4 - m_2) = 1 \pmod q$, i.e. $x(m_4 - m_2) = 1 + kq$. Alors :

$$h^{x(m_4 - m_2)} = h^{1 + kq} = h \times (h^q)^k = h \pmod p$$

car $h^q = 1 \pmod p$ (h est d'ordre q). On a alors :

$$g^{x m_1 - m_3} = (g^{m_1 - m_3})^x = (h^{m_4 - m_2})^x = h^{x(m_4 - m_2)} = h \pmod p$$

Donc, encore une fois, on a $\log_g h = x(m_1 - m_3)$.

- Cas $d = q$. Puisque m_2 et m_4 sont tous deux compris entre 0 et $q - 1$, on a $-(q - 1) \leq (m_4 - m_2) \leq (q - 1)$. La valeur du pgcd d entre $m_4 - m_2$ et un autre nombre ne peut pas être supérieure à $m_4 - m_2$, donc ce cas est impossible. d n'est jamais égal à q .
- Cas $d = p - 1$. ce cas ne peut se produire que si $m_4 = m_2$ modulo $(p - 1)$, c'est-à-dire si $m_4 = m_2$. Mais alors $H(m_1, m_2) = H(m_3, m_4)$ entrainerait :

$$g^{m_1} h^{m_2} = g^{m_3} h^{m_4} \text{ et donc } g^{m_1} = g^{m_3} \pmod p \text{ car } m_2 = m_4$$

Ceci entrainerait $m_1 = m_3$, ce qui ne correspond plus à la définition d'une collision. Ce cas est donc également impossible.

Dans tous les cas, on a $\log_h g = (\log_g h)^{-1} \pmod{p - 1}$

4. Avec $p = 467, g = 2, h = 3, m_1 = 10, m_2 = 35, m_3 = 100, m_4 = 128$, on a bien une collision : $2^{10} 3^{35} = 2^{100} 3^{128} = 453 \pmod{467}$. On calcule le pgcd de $(128 - 35) = 93$ et de 466 : ce pgcd est égal à 1 (les seuls valeurs possibles sont 1, 3, 31 et 93). Donc on est dans le cas $d = 1$ et on calcule l'inverse de $m_4 - m_2$ modulo 466 :

$$\begin{array}{cccccc|l} 1 & 0 & 466 & 0 & 1 & 93 & \rightarrow 466 = 93 \times \mathbf{5} + 1 \\ 0 & 1 & 93 & 1 & -5 & 1 & \rightarrow 93 = 1 \times \mathbf{93} + 0 \\ 1 & -5 & 1 & \dots & \dots & 0 & \text{On a donc } 1 \times 466 + (-5) \times 93 = 1 \pmod{466} \end{array}$$

Donc l'inverse de $m_4 - m_2$ est $x = -5 = 461$. Et le logarithme discret de h est $x(m_1 - m_3) = 450 \pmod{466}$. C'est-à-dire que l'on a : $2^{450} = 3 \pmod{467}$.

5. On a montré que, connaissant une collision, on pouvait calculer un logarithme discret. Cela signifie que trouver une collision pour H est plus difficile que calculer un logarithme discret. Cf le bon vieil adage : « Qui peut le plus, peut le moins ».