

# ENSI BOURGES : MASTER « SÉCURITÉ INFORMATIQUE »

## Systemes cryptographiques : signature électronique

Emmanuel Bresson – ÉNS-DGA

### CORRIGÉS DES EXERCICES DU 28/11/2001

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

[emmanuel@bresson.org](mailto:emmanuel@bresson.org)

#### 1. Signature RSA.

(★)

- 
1. Avec  $p = 17$  et  $q = 23$ , on a  $N = p \times q = 391$  et  $\varphi(N) = (p - 1)(q - 1) = 352$ .
  2.  $e = 11$  n'est pas un exposant de vérification correct car il n'est pas premier avec  $\varphi(N)$  ! En effet on a  $\text{pgcd}(11, 352) = 11$ .  
 $e = 13$  en revanche convient et on peut calculer l'exposant de signature correspondant par l'algorithme d'Euclide étendu :

$$\begin{array}{cccccc|l} 1 & 0 & 352 & 0 & 1 & 13 & \rightarrow 352 = 13 \times \mathbf{27} + 1 \\ 0 & 1 & 13 & 1 & -27 & 1 & \rightarrow 13 = 1 \times \mathbf{13} + 0 \\ 1 & -27 & 1 & -13 & 352 & 0 & \text{On a donc } 1 \times 352 + (-27) \times 13 = 1 \end{array}$$

Donc, modulo  $\varphi(N)$ , i.e. modulo 352, on a  $13(-27) = 1$ .

D'où  $d = -27 = 325 \pmod{352}$ .

3.  $\text{SIGN}(100, 325) = 100^{325} \pmod{391}$ . On a  $325 = 256 + 64 + 4 + 1$  donc on calcule :

$$\begin{aligned} 100^{325} &= 100 \times \left(100 \times (100 \times 100^4)^{16}\right)^4 \pmod{391} \\ &= 100 \times \left(100 \times (100 \times 186)^{16}\right)^4 \pmod{391} \\ &= 100 \times \left(100 \times (223)^{16}\right)^4 \pmod{391} \\ &= 100 \times (100 \times 52)^4 \pmod{391} \\ &= 100 \times (117)^4 = 100 \times 16 = 36 \pmod{391} \end{aligned}$$

4. On calcule  $36^{13} \pmod{391}$ . On a  $13 = 8 + 4 + 1$  donc on calcule :

$$\begin{aligned} 36^{13} &= 36 \times \left(36 \times 36^2\right)^4 = 36 \times (46656)^4 \pmod{391} \\ &= 36 \times (127)^4 = 36 \times 220 = 100 \pmod{391} \end{aligned}$$

---

#### 2. Signature et chiffrement.

(★★)

1. Bob fait successivement  $V_A(c, \sigma) \stackrel{?}{=} \text{OK}$ , puis  $m \leftarrow D_B(c)$ .
2. Charlie remplace  $\sigma$  par  $\sigma'$  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  $(c, \sigma)$ . 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  $p = 467, g = 2, x = 65$

1.  $p = 467$  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 on a  $g^{(p-1)/2} \neq 1$  :  $g$  est donc d'ordre  $p - 1$  (générateur).
2.  $y = g^x = 2^{65} \bmod p$ . Comme  $65 = 64 + 1$ , ça va très vite :

$$2^{65} = 2 \times (2^{16})^4 = 2 \times (65536)^4 = 2 \times 156^4 = 2 \times 369 = 271 \bmod 467$$

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 466,  $100 \neq 65 \times (2^{64} \bmod 467) + 64 \times b$ . Mais il y a d'autres valeurs de  $m$  qui donnerait une égalité. Ainsi  $a = 369 = 2^{64} \bmod 467, b = 42$  et  $m = 111$  vérifient l'égalité :  $111 = 65 \times 369 + 64 \times 42 \bmod 466$ .  
 $k = 213$  est un bon choix car  $\text{pgcd}(213, 466) = 1$ , donc on pourra diviser par  $k$  :

1	0	466	0	1	213	→ 466 = 213 × <b>2</b> + 40
0	1	213	1	-2	40	→ 213 = 40 × <b>5</b> + 13
1	-2	40	-5	11	13	→ 40 = 13 × <b>3</b> + 1
-5	11	13	16	-35	1	→ 13 = 1 × <b>13</b> + 0
16	-35	1	...	...	0	On a donc $16 \times 466 + (-35) \times 213$ = 1 mod 466

L'inverse de 213 est donc  $-35$  qui vaut 431 modulo 466. La signature est  $a = g^k = 2^{213} \bmod 467 = 29$  et  $b = (m - xa) \times k^{-1} = (100 - 65 * 29) \times 431 \bmod 466 = 31$ .

4. On calcule les deux valeurs suivantes :

$$\begin{aligned}
 g^m &= 2^{100} = \left(2 \times (2^6)^4\right)^4 = (2 \times 64^4)^4 \\
 &= (2 \times 241)^4 = 189 \bmod 467 \\
 y^a a^b &= 271^{29} \times 29^{31} = 322 * 295 = 189 \bmod 467
 \end{aligned}$$

### 4. Attaques sur la signature d'El Gamal. (★★★)

1. Avec  $a = 337, b = 9$  et  $y = 316, p = 467, g = 2, m = 100$  on a :

$$\begin{aligned} g^m &= 2^{100} = 189 \pmod{467} \quad \text{Comme précédemment !.} \\ y^a a^b &= 316^{337} \times 337^9 = 56 * 412 = 189 \pmod{467} \end{aligned}$$

2. Soit  $(r, s, t) = (1, 3, 4)$ . On calcule  $\text{pgcd}(ra - tb, p - 1) = \text{pgcd}(301, 466) :$

$$\begin{array}{r|l} \begin{array}{cccccc} 1 & 0 & 466 & 0 & 1 & 301 \\ 0 & 1 & 301 & 1 & -1 & 165 \\ 1 & -1 & 165 & -1 & 2 & 136 \\ -1 & 2 & 136 & 2 & -3 & 29 \\ 2 & -3 & 29 & -9 & 14 & 20 \\ -9 & 14 & 20 & 11 & -17 & 9 \\ 11 & -17 & 9 & -31 & 48 & 2 \\ -31 & 48 & 2 & 135 & -209 & 1 \\ 135 & -209 & 1 & \dots & \dots & 0 \end{array} & \begin{array}{l} \rightarrow 466 = 301 \times \mathbf{1} + 165 \\ \rightarrow 301 = 165 \times \mathbf{1} + 136 \\ \rightarrow 165 = 136 \times \mathbf{1} + 29 \\ \rightarrow 136 = 29 \times \mathbf{4} + 20 \\ \rightarrow 29 = 20 \times \mathbf{1} + 9 \\ \rightarrow 20 = 9 \times \mathbf{2} + 2 \\ \rightarrow 9 = 2 \times \mathbf{4} + 1 \\ \rightarrow 13 = 1 \times \mathbf{13} + 0 \\ \text{On a donc } 135 \times 466 + (-209) \times 301 \\ = 1 \pmod{466} \end{array} \end{array}$$

Par conséquent l'inverse de  $ra - tb$  est  $u = -209$  modulo 466 soit encore  $u = 466 - 209 = 257$ .

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

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

Donc si on pose  $\mu := \alpha u(rm + sb)$ , le couple  $(\alpha, \beta)$  est bien une signature de  $\mu$  puisqu'il vérifie :  $y^\alpha \alpha^\beta = g^\mu$  ! Avec les valeurs choisies, on  $\mu = 365 \times 257 \times (1 \times 100 + 3 \times 9) = 411 \pmod{466}$ . Sans connaître la clé secrète, et simplement en sachant que  $(337, 9)$  était une signature du message  $m = 100$ , on a donc fabriqué  $(365, 319)$ , qui est la signature d'un message  $\mu = 411$  (qu'on n'a pas choisi!). Note : la valeur commune de cette signature (i.e. la valeur commune de  $g^\mu$  et  $y^\alpha \alpha^\beta$ ) est ici 376.

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.

(\*\*\*)

Pour la question 2, la valeur de  $k$  est 337 (donnée oubliée dans la feuille d'exercices originale.)

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.  $p = 467, g = 2, y = 78$ ; premier cas :  $m = 50, a = 416, b = 156$ . 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.  $m = 25, a = 245, b = 292$ . On essaie de trouver  $1/a$  modulo 466. Algorithme d'Euclide (étendu) :

$$\begin{array}{r|l}
 1 & 0 & 466 & 0 & 1 & 245 & \rightarrow 466 = 245 \times \mathbf{1} + 221 \\
 0 & 1 & 245 & 1 & -1 & 221 & \rightarrow 245 = 221 \times \mathbf{1} + 24 \\
 1 & -1 & 221 & -1 & 2 & 24 & \rightarrow 221 = 24 \times \mathbf{9} + 5 \\
 -1 & 2 & 24 & 10 & -19 & 5 & \rightarrow 24 = 5 \times \mathbf{4} + 4 \\
 10 & -19 & 5 & -41 & 78 & 4 & \rightarrow 5 = 4 \times \mathbf{1} + 1 \\
 -41 & 78 & 4 & 51 & -97 & 1 & \rightarrow 4 = 1 \times \mathbf{4} + 0 \\
 51 & -97 & 1 & \dots & \dots & 0 & \text{On a donc } 51 \times 466 + (-97) \times 245 \\
 & & & & & & = 1 \pmod{466}
 \end{array}$$

Par conséquent l'inverse de  $a$  vaut ici  $-97 = 466 - 97 = 369 \pmod{466}$ . Et on trouve pour  $x$  :  $(25 - 337 * 292) * 369 = 15 \pmod{466}$ .

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  $m_1 = 77, b_1 = 341, m_2 = 99, b_2 = 155$ , on a donc  $b_1 - b_2 = 186$ . Donc  $b_1 - b_2$  étant pair, n'est pas inversible modulo  $(p - 1)$ . On ne peut pas calculer  $(m_1 - m_2)/(b_1 - b_2)$ . L'astuce consiste à remarquer que  $m_1 - m_2$  est également pair (il vaut -22). Donc si  $k$  satisfait l'équation  $11 = k * (93)$ , il satisfera aussi l'équation  $-22 = k * 186$  (toujours modulo 466).

On commence donc par l'algorithme d'Euclide étendu pour trouver l'inverse de  $(b_1 - b_2)/2$ , c'est-à-dire de 93 :

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

Par conséquent l'inverse de 93 vaut ici  $-5 = 466 - 5 = 461 \pmod{466}$ . Et on trouve pour  $k$  :  $-11 * (-5) = 55 \pmod{466}$ .

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  $y = 465$ ,  $x = 234$  convient.

## 6. Fonctions de hachage. (★★)

1.  $|M| > 2|E|$  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.

2. 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

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

3. 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.

4. 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  $m_4 = m_2 \pmod{p - 1}$ , 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  $p = 383, g = 2, h = 3, m_1 = 400, m_2 = 100, m_3 = 10, m_4 = 17$ , on a bien une collision :  $2^{400} 3^{100} = 2^{10} 3^{17} = 84 \pmod{383}$ . On calcule le pgcd de  $(17 - 100) = -83 = 299 \pmod{382}$  et de 382 :

$$\begin{array}{r|l} \begin{array}{cccccc} 1 & 0 & 382 & 0 & 1 & 299 \\ 0 & 1 & 299 & 1 & -1 & 83 \\ 1 & -1 & 83 & -3 & 4 & 50 \\ -3 & 4 & 50 & 4 & -5 & 33 \\ 4 & -5 & 33 & -7 & 9 & 17 \\ -7 & 9 & 17 & 11 & -14 & 16 \\ 11 & -14 & 16 & -18 & 23 & 1 \\ -18 & 23 & 1 & \dots & \dots & 0 \end{array} & \begin{array}{l} \rightarrow 382 = 299 \times \mathbf{1} + 83 \\ \rightarrow 299 = 83 \times \mathbf{3} + 50 \\ \rightarrow 83 = 50 \times \mathbf{1} + 33 \\ \rightarrow 50 = 33 \times \mathbf{1} + 17 \\ \rightarrow 33 = 17 \times \mathbf{1} + 16 \\ \rightarrow 17 = 16 \times \mathbf{1} + 1 \\ \rightarrow 16 = 1 \times \mathbf{16} + 0 \\ \text{On a donc } -18 \times 382 + 23 \times 299 \\ \qquad \qquad \qquad = 1 \pmod{382} \end{array} \end{array}$$

Donc on est dans le cas  $d = 1$  et l'inverse de  $m_4 - m_2$  modulo 382 est  $x = 23$ . Et le logarithme discret de  $h$  est  $x(m_1 - m_3) = 184 \pmod{382}$ . C'est-à-dire que l'on a :  $2^{184} = 3 \pmod{383}$ .

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 ».
-