Ecole Polytechnique Fédérale de Lausanne

Sciences de l'information

Série 9

Olivier Cloux

9.1

1. Nous savons que $K = m = 451$. Comme le chiffre du milieu est la somme des deux autres, 11 est un diviseur$\rightarrow$ $451 = 11 \cdot 41$, donc $p = 11,\ q = 41$. Depuis là, il est facile de déterminer $k = ppmc(10, 40) = 40$. Comme nous savons que $e = 13$, calculer f devient facile :

$$\begin{aligned} [f]_k &= ([e]_k)^{-1} \\ [f]_{40} &= ([13]_{40})^{-1} \\ 40 &= 3 \cdot 13 + 1 \\ \iff 1 &= 40 - 3 \cdot 13 \\ \iff [f]_{40} &= [-3]_{40} = [37]_{40} \end{aligned}$$

   Donc $\boxed{f = 37 \equiv -3}$

2. Comme $m = 451$, nous allons considérer P et C dans $\mathbb{Z}/451\mathbb{Z}$. Par définition, $C = ([P]_m)^e = ([109]_{451})^{13}$. Depuis là, nous pouvons calculer :

$$\begin{aligned} &\left(109^{13}\right) \mod 451 \\ &= \left((109^2 \mod 451)^6 \cdot 109\right) \mod 451 \end{aligned}$$

   Or, $109^2 = 11881$ et $26 \cdot 451 = 11726 \rightarrow 109^2 \mod 451 = 11881 - 11726 = 155$

$$= \left((155^2 \mod 451)^3 \cdot 109\right) \mod 451$$

   Or, $155^2 = 24025$ et $53 \cdot 451 = 23903 \rightarrow 155^2 \mod 451 = 24025 - 23903 = 122$

$$= \left((122^3 \mod 451) \cdot 109\right) \mod 451$$

   Or, $122^3 = 1815848$ et $4026 \cdot 451 = 1815726 \rightarrow 122^3 \mod 451 = 1815848 - 1815726 = 122$

$$= \left(122 \cdot 109\right) \mod 451$$

Or, $122 \cdot 109 = 13298$ et $29 * 451 = 13079 \rightarrow (122 \cdot 109) \mod 451 = 13296 - 13079 = 219$

$$= (122 \cdot 109) \mod 451 = 219$$

Donc $[109^{13}]_{451} = \boxed{219 = C}$
L'idée ici était de décomposer en plus petits facteurs. Pour ensuite faire les modulos intermédiaire, je prenais le floor de la division par 451. Par exemple, $109^2 = 11881$ et $\lfloor \frac{11881}{451} \rfloor = \lfloor 26.3436... \rfloor = 26$. Depuis la, on prend $26 \cdot 451$, et on prend la différence pour avoir le reste de la division entière.

3. P' s'obtient de la manière inverse : $P' = ([C]_m)^f = ([43]_{451})^{37}$ Vous l'aurez compris avant, la démarche pour trouver le reste d'une telle division entière est long à faire (et à écrire). Je vais donc appliquer la même technique que précédemment, sans justifier les calculs intermédiaires. Ils ont cependant été fait avec la même technique.

$$\begin{aligned} & 43^{37} \mod 451 \\ = & \left(\left((43^4)^3\right)^3 \cdot 43\right) \mod 451 \\ = & \left((221^3)^3 \cdot 43\right) \mod 451 \\ = & \left(78^3 \cdot 43\right) \mod 451 \\ = & (100 \cdot 43) \mod 451 \\ = & 241 \end{aligned}$$

A titre d'exemple : $43^4 = 3418801 \rightarrow \lfloor \frac{3418801}{451} \rfloor = 7580 \rightarrow 7580 \cdot 451 = 3418580 \rightarrow 43^4 - 7580 \cdot 451 = 3418801 - 3418580 = 221 \rightarrow 43^4 \mod 451 = 221$. La suite des résultats (78,100,241) s'est obtenue avec la même méthode. Tout ça à la calculatrice :)

9.2

1. Il lui est facile de le vérifier : comme nous l'avons vu dans les propriétés de RSA et des classes de congruence, en élevant la signature (modulo K), à la puissance e (publique, l'inverse de f), il obtiendra $P(u)$. Il n'a ensuite qu'à recalculer $P(u)$ selon la méthode vue (rien n'est caché à ce stade), pour vérifier que les deux correspondent. S'ils ne correspondent pas, la signature est fausse (faite par la mauvaise personne, ou le message a été modifié).

2. $(p, q) = (97, 173) \rightarrow k = ppmc(96, 172) = ppmc(2^5 \cdot 3\ ,\ 2^2 \cdot 43) = 2^5 \cdot 3 \cdot 43 = 4128 = k$
$[f]_k = ([e]_k)^{-1} \rightarrow [f]_{4128} = ([17]_{4128})^{-1}$. Pour cela, on utilise l'algorithme d'Euclide et Bézout :
Soit $4128 = a$ et $17 = b$

$$\begin{aligned} 4128 &= 242 \cdot 17 + 14 \\ a &= 242b + 14 \rightarrow 14 = a - 242b \\ b &= 14 + 3 \rightarrow 3 = b - 14 = b - (a - 242b) = -a + 243b \\ 14 &= 4 \cdot 3 + 2 \rightarrow 2 = 14 - 4 \cdot 3 = (a - 242b) - 4 \cdot (-a + 243b) = 5a - 1214b \\ 3 &= 2 + 1 \rightarrow 1 = 3 - 2 = (-a + 243b) - (5a - 1214b) = -6a + 1457b \end{aligned}$$

Donc $[1]_{4128} = [-6 \cdot 4128]_{4128} + [1457 \cdot 17]_{4128} \rightarrow \boxed{f = 1457}$

3. $u = (C, I, A, O) \rightarrow c(u) = (12, 18, 10, 24)$
$\rightarrow P(u) = \sum_{i=1}^{n} c(u_i) \cdot 37^{i-1} = 12 \cdot 1 + 18 \cdot 37 + 10 \cdot 37^2 + 24 \cdot 37^3 = 1'230'040$
Comme $(p, q) = (97, 173)$, alors $K = 97 \cdot 173 = 16'781$

$\rightarrow [P(u)]_K = [1'230'040]_{16'781}$
De plus, $1'230'040 = 73 \cdot 16'781 + 5'027$, donc $[P(u)]_K = [5'027]_{16'781}$
Finalement, $[\sigma(u)]_{16781} = ([5027]_{16781})^f$ avec $f = 1457$. Donc $\boxed{\sigma = 1759}$

4. Calculons la signature de $u = (P, O, I, N, C, A, R, E)$. $c(u) = (25, 24, 18, 23, 12, 10, 27, 14)$
$\rightarrow P(u) = 25 \cdot 1 + 24 \cdot 37 + 18 \cdot 37^2 + \ldots + 14 \cdot 37^7 = 1'399'038'012'981$
$\rightarrow [P(u)]_K = [1'399'038'012'981]_{16'781} = [1'821]_{16'781}$
$\rightarrow [\sigma(u)]_K = ([P(u)]_K)^f = ([1'821]_{16'781})^{1'457} \rightarrow \boxed{\sigma(POINCARE) = 5'313 \neq 14'812}$ Donc la signature est fausse.

5. La signature est facile à trouver. En effet, notons u_1 = BART DOIT LISA CHF 100 et u_2 = BART DOIT LISA CHF 10000000. Nous pouvons affirmer que $P(u_1) = P(u_2)$, car nous avons noté que c(0) = 0. Donc la fin du calcul de $P(u_2)$ sera $[...] + 0 \cdot 37^{21} + 0 \cdot 37^{22} + \ldots$. Nous voyons qu'ajouter des 0 (sans rien mettre d'autre à la suite) ne change rien au calcul. Le message pourrait parler de CHF 1 ou de CHF 1000000000000, cela ne changera pas les $P(u_i)$. Comme les $P(u_i)$ sont identiques, la suite sera la même, donc les signatures seront identiques. Donc $\sigma(u_2) = \sigma(u_1) = S$. Notons cependant que si le message avait un caractère quelconque à la fin (différent de 0), cela changerait tout. Car ce "caractère de contrôle" comme on pourrait l'appeler, passerait de[1] $c(u_{21}) \cdot 37^{21}$ à $c(u_2 1) \cdot 37^{28}$. Le nombre de 0 changerait alors tout.

   Comme nous venons de le voir, la méthode dans son état actuel n'est pas efficace, justement à cause de ce problème ; si le message était intercepté et modifié (de la bonne manière), la signature ne serait pas modifiée, donc la modification serait invisible.

6. Une solution, comme évoquée au dessus, consisterait en l'ajout d'un caractère de contrôle, avec $c(u_{controle}) \neq 0$ a ajouter a la fin de chaque message. De cette manière, le problème des 0 de fin disparaîtrait.

9.3

1. $p = 83 = 2 \cdot 41 + 1,\ q = 59 = 2 \cdot 29 + 1 \rightarrow k = ppmc(82, 58) = 41 \cdot 2 \cdot 29 = 2378$ Comme il n'y a pas de facteur 17 dans ce chiffre, k et e sont premiers entre eux. Donc ces paramètres sont valides.

   Donc $\boxed{K = m = 83 \cdot 59 = 4897}$

   $[f]_m = ([e]_m)^{-1} = ([17]_{4987})^{-1}$
   $4897 = 288 \cdot 17 + 1 \iff 1 = 4897 - 288 \cdot 17$
   $[-288]_{4897} \cdot [17]_{4897} = [1]_{4897}$
   $[f]_{4897} = [-288]_{4897} = [4609]_{4897} \iff \boxed{f = 4609}$

2. $83 = 2 \cdot 41 + 1$, avec 41 premier, et $59 = 2 \cdot 29 + 1$ avec 29 premier. Donc oui, ces chiffres sont sûrs.

3. Comme nous savons que $K = 4897 = 59 \cdot 83 = p \cdot q$, le théorème des restes chinois, nous permet de poser que $P^e = P \mod K \iff \begin{cases} P^e = P \mod p \\ P^e = P \mod q \end{cases}$. Nous sommes exactement dans le cas du théorème 10.4 (aussi car $e - 1 = 17 - 1$ est une puissance de 2). Ce théorème dit qu'il y a exactement 9 solutions, qui sont les combinaisons de $[0]_p, [1]_p, [-1]_p$ avec $[0]_q, [1]_q, [-1]_q$. Si certaines combinaisons sont triviales ($[0]_p, [0]_q$ par exemple), d'autre le sont moins. Je montrerai ici la manière d'en trouver une, les autres se feront exactement de la même manière. La combinaisons que nous allons considérer est $[1]_{59}, [82]_{83}$.

[1] chiffres indicatifs

Pour que notre résultat dans $\mathbb{Z}/pq\mathbb{Z}$ soit valable, nous devons poser

$$x = 59q + 1 \text{ et } x = 83k + 82,\ \forall k, q \in \mathbb{Z} \tag{1}$$

, puis les égaler. Nous cherchons donc un k et un q tels que

$$59q - 83k = 81 \tag{2}$$

Pour cela, nous appliquons l'égalité de Bézout sur 59 et 83. Il doit exister un couple u, v tels que $59u + 83v = pgcd(83, 59) = 1$. Comme fait plus haut :

$$\begin{aligned}
83 = 59 + 24 &\rightarrow 24 = 83 - 59 \\
59 = 2 \cdot 24 + 11 &\rightarrow 11 = 59 - 2 \cdot 24 = 59 - 2 \cdot (83 - 59) = 3 \cdot 59 + 5 \cdot 83 \\
24 = 2 \cdot 11 + 2 &\rightarrow 2 = 24 - 2 \cdot 11 = (83 - 59) - 2 \cdot (3 \cdot 59 - 2 \cdot 83) = 5 \cdot 83 - 7 \cdot 59 \\
11 = 5 \cdot 2 + 1 &\rightarrow 1 = 11 - 5 \cdot 2 = (3 \cdot 59 - 2 \cdot 83) - 5 \cdot (5 \cdot 83 - 7 \cdot 59) = 38 \cdot 59 - 27 \cdot 83
\end{aligned}$$

Donc, nous savons que

$$\begin{aligned}
1 &= 38 \cdot 59 - 27 \cdot 83 \\
\rightarrow 81 &= 3078 \cdot 59 - 2187 \cdot 83 \\
\rightarrow u &= 3078,\ v = 2187
\end{aligned}$$

Ces chiffres correspondent a notre équation. Cependant, afin de les simplifier, nous pouvons appliquer sur u, respectivement v, un modulo 83, respectivement 59. Cela nous donne les résultats $q = 7,\ k = 4$. Nous pouvons bien vérifier que ces chiffres sont valides en les remplaçant dans (2). Ensuite, nous pouvons remplacer nos valeurs dans (1), afin de trouver $x = 414$. Une des 9 solutions est donc $[414]_{4897}$

En appliquant cette méthode, nous trouvons toutes les autres solutions :

$$P = \{0,\ 1,\ 414,\ 2241,\ 2242,\ 2655,\ 2656,\ 4483,\ 4896\}$$

(bien entendu, dans $\mathbb{Z}/4897\mathbb{Z}$)

4. a) $p = 17 = 2^4 + 1 = 2 \cdot 8 + 1$, mais 8 n'est pas premier. Donc 17 n'est pas sûr.

   b) Cela ressemble très fortement au petit théorème de Fermat.... Celui-ci énonce que, si p est un nombre premier, pour tout entier a

   $$([a]_p)^p = [a]_p \iff a^p = a \pmod p$$

   que nous ne prouverons pas, car il s'agit là de l'objet d'unes série précédente.
   Cela nous permet d'affirmer que $x^{17} = x \pmod{17}\ \forall x \in \mathbb{Z}/17\mathbb{Z}$. Les solutions sont donc $\boxed{x = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}}$

   c) Selon le théorème des restes chinois, cela revient à chercher ne nombre de solutions dans $\begin{cases} P^{17} = P \mod 17 \\ P^{17} = P \mod 59 \end{cases}$. Comme 59 est sûr $(2 \cdot 29 + 1)$, la seconde équation admettra 3 solutions[2] : $[-1]_{59}, [1]_{59}, [0]_{59}$. L'équation en 17, nous l'avons vu auparavant, admet 17 solutions. Il y aura donc autant de solutions que de combinaisons, à savoir $3 \cdot 17 =$ $\boxed{51 \text{ messages distincts}}$

[2] comme prouvé dans le théorème 10.4, et utilisé dans l'exercice 9.3.3