Examen Final – Cryptographie

jeudi 19 janvier 2006

Correction

Exercice 1
Alice change sa clé RSA tous les 25 jours. Bob lui change sa clé tous les 31 jours. Sachant qu'Alice change sa clé aujourd'hui et que Bob a changé sa clé il y a trois jours, déterminer quand sera la prochaine fois qu'Alice et Bob changeront leur clé le même jour.

Solution. Notons d le nombre de jours jusqu'à ce que Alice et Bob changent leur clé le même jour. Puisque Alice change sa clé tous les 25 jours et qu'elle a changé sa clé aujourd'hui, d doit être divisible par 25. Puisque Bob change sa clé tous les 31 jours et qu'il a changé sa clé il y a trois jours, $d + 3$ doit être divisible par 31. Ainsi d doit vérifier le système de congruences :

$$\begin{cases} d & \equiv 0 \pmod{25} \\ d & \equiv -3 \pmod{31}. \end{cases}$$

Par le théorème des restes chinois, ce système équivaut à la congruence

$$d \equiv 400 \pmod{775},$$

et donc Alice et Bob changeront leurs clés le même jour dans 400 jours.

Exercice 2
Bob utilise le protocole RSA et publie sa clé publique $N = 187$ et $e = 3$.

1. Encoder le message $m = 15$ avec la clé publique de Bob.
2. En utilisant le fait que $\varphi(N) = 160$, retrouver la factorisation de N, puis la clé privée de Bob.

Solution.

1. Le message codé est $c = 15^3 \mod 187 = 9$.

2. Ecrivons $N = pq$. On a donc $\varphi(N) = (p-1)(q-1) = pq-p-q+1 = N-(p+q)+1$, et ainsi
$$p + q = N - \varphi(N) + 1 = 187 - 160 + 1 = 28.$$
Les nombres p et q sont racines du polynôme
$$X^2 - (p + q)X + pq = X^2 - 28X + 187.$$
Le discriminant est $28^2 - 4 \times 187 = 36$ et ainsi $p = (28 - 6)/2 = 11$ et $q = (28 + 6)/2 = 17$.

Exercice 3

Soient p et q deux nombres premiers impairs tels que $p \equiv 1 \pmod 3$ et $q \equiv 1 \pmod 3$. On pose $N = pq$.

1. Montrer que
$$\left(\frac{3}{N}\right) = (-1)^{(N-1)/2}.$$
2. On suppose de plus que $N \equiv 3 \pmod 4$. En déduire que : ou bien 3 est un carré modulo p et 3 n'est pas un carré modulo q ; ou bien 3 n'est pas un carré modulo p et 3 est un carré modulo q.

Solution.

1. Par la loi de réciprocité quadratique, on a
$$\left(\frac{3}{N}\right) = (-1)^{(N-1)/2}\left(\frac{pq}{N}\right)$$
et comme $pq \equiv 1 \pmod N$, on trouve que $\left(\frac{pq}{N}\right) = 1$, d'où le résultat.
2. On a $N-1 \equiv 2 \pmod 4$ et ainsi $(N-1)/2 \equiv 1 \pmod 2$. Par la question 1., il suit que $\left(\frac{3}{N}\right) = -1$. Puisque $\left(\frac{3}{N}\right) = \left(\frac{3}{p}\right)\left(\frac{3}{q}\right)$, on trouve que : ou bien $\left(\frac{3}{p}\right) = 1$ et $\left(\frac{3}{q}\right) = -1$ d'où 3 est un carré modulo p, mais pas modulo q ; ou bien $\left(\frac{3}{p}\right) = -1$ et $\left(\frac{3}{q}\right) = 1$ d'où 3 est un carré modulo q, mais pas modulo p.

Exercice 4

Bob_1 et Bob_2 ont pour clé publique RSA respectivement (N, e_1) et (N, e_2) avec e_1 et e_2

premiers entre eux.
Alice envoie le même message m crypté par les clés publiques RSA de Bob_1 et Bob_2 en c_1 et c_2.
Expliquer comment Eve, qui intercepte les deux messages cryptés et qui connait les clés publiques de Bob_1 et Bob_2, peut retrouver le message clair m.

Solution. Puisque e_1 et e_2 sont premiers entre eux, il existe deux entiers u et v tels que $ue_1 + ve_2 = 1$. Eve peut calculer u et v, et finalement retrouve le message en faisant

$$c_1^u c_2^v \equiv m^{ue_1} m^{ve_2} \equiv m^{ue_1+ve_2} \equiv m \pmod N.$$

Exercice 5
On considère un texte de $2n$ lettres dans lequel exactement une lettre sur deux est un 'A'.

1. Quelle est la contribution de la lettre 'A' dans l'indice de coïncidence de ce texte ?
2. En déduire que si $n \geq 2$, alors l'indice de coïncidence est $\geq 1/6$.
3. Supposons à présent que toute les lettres autres que 'A' sont des 'B'. Vers quelle valeur l'indice de coïncidence du texte tend quand n tend vers l'infini ? Pourquoi cette réponse est-elle bien celle que l'on attend ?

Solution.

1. Puisque le nombre de 'A' dans le texte est n, la contribution c_A de A est
$$c_A = \frac{n(n-1)}{2n(2n-1)} = \frac{n-1}{2(2n-1)}.$$
2. On a $(n-1)/(4n-2) \geq 1/6$ si et seulement $6n-6 \geq 4n-2$ si et seulement $2n \geq 4$ si et seulement si $n \geq 2$, d'où le résultat.
3. Notons c_B la contribution de 'B'. Puisqu'une lettre sur deux est un 'B', on a donc par la question 1. que $c_B = (n-1)/(4n-2)$. La contribution des autres lettres est nulle et donc l'indice de coïncidence du texte est
$$c_A + c_B = \frac{n-1}{2n-1}.$$
Il suit que la limite de l'indice de coïncidence quand n tend vers $+\infty$ est $1/2$.

   On explique pourquoi cette réponse est conforme à ce qu'on attend. En effet, si on prend une lettre au hasard, elle peut être un 'A' ou un 'B' avec la même probabilité. Ainsi, si on prend deux lettres au hasard, on a les quatre possibilités suivantes avec la même probabilité : AA, AB, BA, BB. Donc la probabilité que deux lettres choisit au hasard soient égales est bien $1/2$.

Exercice 6
On considère un diagramme de Feistel à deux rondes sur des chaînes de 8 bits avec deux fonctions f_1 et f_2.

1. On pose
$$f_1(a) := a \oplus 1011 \quad \text{et} \quad f_2(a) := \bar{a} \oplus 0101$$
pour toute chaîne a de 4 bits.
   (a) Calculer l'image de la chaîne 11010011 par ce diagramme.
   (b) Déterminer une chaîne de 8 bits dont l'image par le diagramme est elle-même.
2. La propriété précédente, à savoir il existe une chaîne dont l'image par le diagramme de Feistel est elle-même, est-elle vraie pour toutes les fonctions f_1 et f_2 ? Justifier votre réponse par une démonstration ou un contre-exemple.

Solution.

1. (a) On calcule les formules donnant le mot de sortie $w'_1 \cdot w'_2$ en fonction du mot d'entrée $w_1 \cdot w_2$:
$$\begin{aligned} w'_1 = f_2(f_1(w_1) \oplus w_2) \oplus w_1 &= \overline{w_1 \oplus 1011 \oplus w_2} \oplus 0101 \\ &= w_1 \oplus w_2 \oplus 1111 \oplus 0101 = w_1 \oplus w_2 \oplus 1010, \end{aligned}$$
$$w'_2 = f_1(w_1) \oplus w_2 = w_1 \oplus w_2 \oplus 1011.$$
Ainsi pour $w_1 = 1101$ et $w_2 = 0011$, on obtient $w'_1 = 1101 \oplus 0011 \oplus 1010 = 0100$ et $w'_2 = 1101 \oplus 0011 \oplus 1011 = 0101$. Donc finalement l'image de 11010011 par ce diagramme est 01000101.
   (b) On veut que $w'_1 = w_1$ et $w'_2 = w_2$. En remplaçant dans les formules ci-dessus, on obtient
$$\begin{cases} w_1 & = w_1 \oplus w_2 \oplus 1010, \\ w_2 & = w_1 \oplus w_2 \oplus 1011. \end{cases}$$
et donc $w_1 \oplus 1010 = 0000$ et $w_1 = 0101$, $w_2 \oplus 1011 = 0000$ d'où $w_2 = 0100$.
En conclusion, le mot 01010100 est invariant par le diagramme.
2. On considère l'équation $w'_2 = f_1(w_1) \oplus w_2$. Si on prend f_1 telle que $f_1(w_1) \neq 0000$ pour tout w_1, alors on ne peut jamais avoir $w'_2 = w_2$ et donc, pour ce choix de f_1, il n'existe pas de mot invariant.