Examen Final – Cryptographie

jeudi 19 janvier 2006

Toutes les réponses devront être justifiées. En particulier, les diverses étapes de calcul devront être détaillées.

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.

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.

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.

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.

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 ?

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.