ENSEIRB - 2eAnnée Filière Informatique Année 2003-20004

Cryptologie

Durée : 2h.
Notes de cours et de TD autorisées.

Exercice 1 Deux siècles avant JC, le philosophe Polybe proposa le cryptosystème suivant. L'alphabet retenu était l'alphabet latin débarassé de la lettre `W` : soit un total de 25 lettres. La clef de chiffrement était n'importe quel mot. Ce mot fixé, on le débarassait des lettres doublons, on l'augmentait par le restant des caractères non utilisés et ce dans l'ordre alphabétique puis on le plaçait dans une grille 5 lignes 5 colonnes. Chaque lettre étant ainsi chiffré par un nombre de deux chiffres : le premier étant le numéro de la ligne, le second celui de la colonne.

Exemple 1 Ainsi la clef est le mot `clefsecrete`, la lettre `b` est chiffré par le nombre 24.

```
  1 2 3 4 5
1 c l e f s
2 r t a b d
3 g h i j k
4 m n o p q
5 u v x y z
```

Est-ce que ce cryptosystème s'apparente à d'autres cryptosystèmes ? Peut-on cryptanalyser un tel cryptosystème ?

Exercice 2

1. Rappeler le protocole de chiffrement et de déchiffrement `RSA`.
2. Définir le cassage complet de ce protocole (2 lignes) et comparer ce problème avec d'autres problèmes élèmentaires (Nous vous demandons jute de rappeler ces comparaisons sans en fournir la preuve).

Exercice 3 L'utilisateur *DuSchmoll* décide de dévier du protocole `RSA` en choisissant non pas deux grands nombres premiers aléatoires p et q mais deux grands nombres premiers très proches p et q avec $p > q$. Ce nouveau protocole sera appelé `RSADuSchmoll`.

1. En posant $n := p \cdot q$, $s := \frac{p-q}{2}$ et $t := \frac{p+q}{2}$, démontrer les assertions suivantes :
   (a) $n = t^2 - s^2$.
   (b) t est proche par valeur supèrieure de la racine carrée de n.
   (c) s est un petit entier.
2. Déduire de la question suivante une attaque de `RSADuSchmoll`. Vous définirez précisément le problème résolu, l'algorithme le résolvant et sa complexité en temps.

Exercice 4 Considérons le chiffrement RSA. L'objectif de cet exercice est de comparer la sécurité de ce système au problème du calcul du bit de poids faible du message en clair :

Parité
E: clef publique (n, e), un message chiffré $y = e_K(x)$
S: le bit de poids faible de x noté parité(x)

Pour les notations futures, nous considérons que la clef privée K est fixée ainsi que sa sous-clef publique (n, e). Soit $|n|$ la taille de n, c'est à dire le nombre de bits nécessaires pour représenter n en binaire (on a : $|n| = \lceil \log_2(n+1) \rceil$). Pour tout mot w de longueur $l \leq |n|$, nous notons $I(w)$ l'intervalle $[\frac{\overline{w}}{2^l} \cdot n, \frac{\overline{w}+1}{2^l} \cdot n[$ où $\overline{w}$ désigne l'entier représenté par w. À titre d'exemple voici quelques intervalles : $I(0) = [0, \frac{1}{2} \cdot n[$, $I(1) = [\frac{1}{2} \cdot n, 1 \cdot n[$, $I(00) = [0, \frac{1}{4} \cdot n[$, $I(01) = [\frac{1}{4} \cdot n, \frac{2}{4} \cdot n[$, $I(10) = [\frac{2}{4} \cdot n, \frac{3}{4} \cdot n[$, $I(11) = [\frac{3}{4} \cdot n, \frac{4}{4} \cdot n[$.

1. Démontrer que si l'on sait décider rapidement de l'appartenance du mot chiffré à tout intervalle de la forme $I(w)$ on sait décrypter en temps polynomial ce mot chiffré. C'est à dire plus formellement, démontrer que le problème du décryptage de x est aussi facile que :

   E: clef publique (n, e), $y = e_K(x)$, un mot $w \in \{0,1\}^l$ avec $l \leq |n|$.
   S: le booléen $x \in I(w)$

2. Démontrer que le booléen $x \in I(0)$ est égal à parité$(2 \cdot x)$. De façon plus générale démontrer que pour tout mot $w = w_1 w_2 \ldots w_l$, on a $x \in I(w)$ si et seulement si pour tout indice $i \in [1, l]$ le booléen parité$((2^i \cdot x) \bmod n)$ est w_i.

3. Conclure.