Cryptographie – Feuille d'exercices 8

Attaques physiques contre le cryptosystème RSA

M1 Informatique – 2014-2015

1 Exercice 1 : L'age du capitaine

On cherche à connaître l'âge du capitaine. On a uniquement les indices suivants :
- Il y a un an, son âge était un multiple de 3.
- Dans 2 ans, son âge sera un multiple de 5.
- Dans 4 ans, ce sera un multiple de 7.

Énoncé Quel est l'âge du capitaine ?

2 Exercice 2 : Attaque passive contre le cryptosystème RSA

Soit $n = p \times q$ un entier, produit de deux nombres premiers p et q. On considère d un exposant secret RSA de k bits, dont l'écriture binaire est $d = d_{k-1}2^{k-1} + d_{k-2}2^{k-2} + ... + d_1 2 + d_0$ (avec $d_{k-1} = 1$).
La fonction $f : Z/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, définie par $f(x) = x^d \bmod n$, est implémentée dans une carte à puce de la manière suivante (dite "square-and-multiply-always") :

Input: x, d, n
Output: $y_0 = x^d \bmod n$
  $y_0 := x$
  for $i = k - 2$ down to 0 **do**
    $y_0 := y_0^2 \bmod n$
    $y_1 := y_0 \times x \bmod n$
    $y_0 := y_{d_i}$
  end for
  Return y_0

1. Expliquer l'avantage de la méthode "square-and-multiply-always" sur la méthode "naïve" suivante :

   Input: x, d, n
   Output: $y = x^d \bmod n$
     $y := x$
     for $i = k - 2$ down to 0 **do**
       $y := y^2 \bmod n$
       if $d_i = 1$ **then** $y := y \times x \bmod n$
     end for
     Return y

2. On se place maintenant dans l'hypothèse suivante : l'attaquant est capable de détecter (par exemple par observation des courbes de consommation électrique) que la carte effectue deux fois le même calcul. Plus précisément, si la carte calcule $u^2 \bmod n$ (à un instant t_1), puis $v^2 \bmod n$ (à un instant $t_2 > t_1$), l'attaquant n'est pas capable d'en déduire la valeur de u ni celle de v, mais est capable de dire si $u = v$.

   On suppose en outre que l'attaquant peut effectuer le calcul $x^d \bmod n$ avec les valeurs x de son choix. Montrer qu'il peut alors retrouver la valeur de l'exposant secret d, dans le cas de l'algorithme "square-and-multiply-always" (pour cette attaque de type SPA, on pourra considérer la suite des valeurs intermédiaires, successivement pour les valeurs d'entrée x et $x' = x^2 \bmod n$)

3 Exercice 3 : Attaque par injection de faute

Dans la suite, on s'intéresse au cryptosystème RSA. On note :
- $n = p \times q$ le module RSA ;
- e l'exposant public ;
- d l'exposant privé.

1. Rappeler le théorème des restes chinois ;
2. Expliquer comment celui-ci peut être utilisé dans le cadre du déchiffrement ;
3. Donner le facteur d'accélération résultant de l'utilisation du théorème des restes chinois par rapport à une implémentation "classique".

On suppose maintenant que la carte à puce implémente le déchiffrement à l'aide du théorème des restes chinois. Sous l'action d'un laser, il est possible de changer la valeur d'un registre en une valeur complètement aléatoire. Supposons que l'attaquant soit capable de changer la valeur du registre lors de la fin du déchiffrement modulo q ; le résultat du déchiffrement est alors "faux".

5. Montrer comment il peut factoriser le module RSA à l'aide de ce déchiffrement "faux".