Fondements de la cryptographie: TD 5

Exercice 1. (Attaques par canaux cachés) Soit n un entier. On considère d un exposant secret (RSA, Diffie-Hellman) 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, définie par $f(x) = x^d \bmod n$, est implémentée dans une carte à puce de la manière suivante (dite "square-and-multiply") :

Require: x, d, n
Ensure: $y = x^d \bmod n$
  $y := x$
  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

1. Expliquer l'avantage de la méthode "square-and-multiply" sur la méthode "naïve" d'exponentiation. Calculer $2^7 \pmod{15}$ et $3^{11} \pmod 6$.

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 une multiplication ou un carré. Montrer qu'il peut alors retrouver la valeur de l'exposant secret d, dans le cas de l'algorithme "square-and-multiply".

Exercice 2.

1. Soit $N = 7 \cdot 13$ un module RSA et $e = 11$ la clé publique d'un utilisateur. Calculer la clé secrète correspondante et chiffrez le message $m = 2$. Décrivez l'algorithme de déchiffrement.

2. On suppose ici qu'un module RSA N est commun à tous les utilisateurs d'un réseau. Nous avons deux utilisateurs avec les clés publiques e_1 et e_2 tel que $(e_1, e_2) = 1$. Un message m chiffré avec ces clés leur est envoyé et les messages chiffrés sont interceptés. Montrer que l'attaquant peut retrouver le message m en temps polynomial. Nous rappelons ici que l'algorithme d'Euclid etendu permettant de calculer u et v tel que $ue_1 + ve_2 = 1$ a une complexité polynomiale.