Examen de Cartes à Puce 2

Session 2 – 30 septembre 2014

Durée : 1 heure

<u>Aucun document autorisé</u>

1) Analyse de fautes

Expliquez ce qu'est une analyse de faute : par quel moyen est-il possible de provoquer une faute ?, quel effet un faute peut-il avoir sur les données, les instructions exécutées ?, comment peut-on exploiter une faute et dans quel but ?, ...

2) Analyse de courant

Dites ce que vous savez sur la DPA et la CPA. Puis vous comparerez ces deux techniques d'attaque : similarités/différences, avantages/inconvénients.

3) Algorithme

```
Input : m, d et n des entiers,  ( d = (d_{k-1}...d_0) en base 2 )
Output :

1.  s = 1
2.  Pour i de k-1 à 0
      2.1.  s = s x s modulo n
      2.2.  si (d_i == 1) alors s = s x m modulo n
3.  Retourner s
```

a) Expliquez ce que sert à calculer l'algorithme ci-dessus.

b) Comment appelle-t-on cet algoritme ?

c) À quel type d'attaque en courant cet algorithme est-il vulnérable ? Expliquez comment fonctionne cette attaque.