Examen de Cartes à Puce 2

Février 2017

Durée : 1h30

Les supports de cours de l'UE Cartes à Puce 2
sont les seuls documents autorisés pour la composition de cet examen.

L'usage d'une calculatrice est autorisé.

Quizz (10 points)

1. Expliquez en détail comment vous vous y prendriez pour adapter la DFA classique sur le DES à l'algorithme Triple-DES.

2. Un développeur de RSA embarqué sur carte à puce sait très bien que l'algorithme « Square and Multiply » classique est vulnérable à une analyse simple du courant qui permet de retrouver successivement les différents bits de l'exposant secret d manipulé.
   Souhaitant malgré tout utiliser cet algorithme d'exponentiation pour des raisons de performance, il décide de protéger son implémentation en utilisant la panoplie complète des masquages (masquages d'exposant, de message et de module).

   Donnez votre avis argumenté sur la pertinence de ce choix de contre-mesures dans ce cas précis.

3. Lorsqu'on calcule une trace de DPA pour la bonne hypothèse de clé, il arrive que le pic de DPA obtenu soit négatif. Quelle explication pouvez-vous donner à ce phénomène ?

4. Du point de vue de la vulnérabilité aux attaques physiques, quel(s) parallèle(s) faites-vous entre l'exponentiation modulaire (RSA) et la multiplication scalaire d'un point d'une courbe elliptique (ECC) ?

5. La représentation signée de la clé privée x peut-elle avoir un intérêt dans le cas suivant ? Justifiez vos réponses.

   a) Exponentiation de type $m^x \bmod n$

   b) Exponentiation de type $g^x \bmod p$

   c) Multiplication scalaire du type $x.P$

6. Est-il possible de retrouver de l'information sur la clé d'un DES ou d'un AES en exploitant par DPA ou CPA les traces de consommation relatives à l'exécution du key schedule ? Justifiez votre réponse.

Exercice 1 (2,5 points)

Parmi les différents algorithmes d'exponentiation modulaire, certains sont dits « réguliers ».

1. Quels algorithmes réguliers connaissez-vous ?

2. De quels types d'attaques un algorithme régulier protège-t-il ? De quels types d'attaques ne protège-t-il pas ?

Exercice 2 (4 points)

1. Qu'est-ce que la « doubling attack » ?

2. À quel(s) algorithme(s) s'applique-t-elle ?

3. Expliquez en détails comment un attaquant retrouverait la valeur de la clé lorsque celle-ci est égale à 105.

Exercice 3 (3,5 points)

On suppose qu'il possible de distinguer les différentes étapes d'un calcul en observant une trace de consommation de courant.

Dessinez de manière schématique ce qu'observerait un attaquant sur une trace de courant dans les cas suivants :

1. Exponentiation modulaire par la méthode Square & Multiply de droite à gauche avec un exposant égal à 53.

2. Exponentiation modulaire par la méthode Square & Multiply always de gauche à droite avec un exposant égal à 53.

3. Exponentiation modulaire par la méthode Joye Ladder avec un exposant égal à 53.

4. Génération de premier par la méthode naïve simple.

5. Génération de premier par la méthode naïve incrémentale.

6. Génération de premier par la méthode du crible simple.

7. Génération de premier par la méthode du crible optimisée.