Master CRYPTIS
UE Cartes à puce

2011-2012

Examen

30 janvier 2012
14h-16h

Tout document non électronique autorisé

Q1 : Un objet du JCRE peut il invoquer une méthode sur un objet d'une application Java Card appartenant à un contexte de sécurité applicatif ? Réciproquement est il possible d'appeler une méthode public sur un objet du Run Time ?

Q2 : Le nettoyage des objets sensibles persistants peut il être réalisé dans la méthode *deselect ()* et pourquoi ?

Q3 : Ce code présente-t-il du code mort ? Donnez une explication.

```
public void myMethod (APDU apdu)
{
  byte[] buffer = apdu.getBuffer();
   if (myPin.isValidated ()) {
      //do non sensitive code
      if (!pin.isValidated()) {
      ISOException.throwIt(ISOException.SecurityException);
      // do sensitive actions herre
      } else ISOException.throwIt( (short) ((short) 0x63C0 + (short)
pin.getTriesRemaining()));
  return ;
  }
}
```

Q4 : Cette méthode a elle un comportement prédictible ?

```
private void myMethod (APDU apdu)
{
  byte[] buffer = apdu.getBuffer();
   if (myPin.isValidated ()) {
      JCSystem.BeginTransaction();
      install (apdu, 5, 16);
      JCSystem.commitTransaction ();
  return ;
  }
}
```

Q5 : Quelle différence en terme de taille de code peut on observer entre ces deux définitions:

```
byte[] menu1 = {(byte)'m', (byte)'e',(byte)'n', (byte)'u', (byte)'1' };
static byte[] menu2 = {(byte)'m', (byte)'e', (byte)'n', (byte)'u',
(byte)'2' };
```

Q6 : L'attaque par collision classique (dite BGW) sur l'algorithme COMP128 est-elle une attaque à chiffrés seuls, à clairs connus ou à clairs choisis ? Justifiez votre réponse.

Q7 : A un certain stade d'une variante améliorée de l'attaque BGW sur le COMP128 l'attaquant cherche à provoquer une collision à la sortie de la troisième étape. Il utilise pour cela une pré-collision utile. Expliquez ce qu'est une pré-collision utile et comment fait l'attaquant pour la générer.

Q8 : Dans une DPA sur le DES, combien l'attaquant doit-il générer de courbes de DPA pour retrouver les valeurs de toutes les sous-clés du premier tour ? Justifiez votre réponse.

Q9 : Dans une CPA sur l'AES avec modèle de consommation en poids de Hamming, combien l'attaquant doit-il générer de courbes de CPA pour retrouver la valeur d'un octet de clé ? Combien de courbes de CPA pour retrouver la clé complète ? Justifiez vos réponses.

Q10 : Dans une CPA sur l'AES avec modèle de consommation en distance de Hamming, quelle avantage l'attaquant retire-t-il d'envoyer à la carte uniquement des messages formés de 16 valeurs d'octet identiques ? Pourquoi cette astuce ne s'applique-t-elle pas au DES ?

Q11 : On suppose un attaquant capable de mesurer uniquement le temps d'exécution lors du calcul d'une signature RSA utilisant l'algorithme *square & multiply* binaire classique.
Dans le meilleur des cas, quelle type d'information l'attaquant peut-il apprendre au sujet de l'exposant privé ?

Q12 : Expliquez en détail comment vous vous y prendriez pour adapter la DFA classique sur le DES à l'algorithme Triple-DES.