[Cryptographie Appliquée] Correction de l'annale 2012-2013

Exercice 1

1. **Correction par Jad <3**

   > La sécurité des mots de passe dépend de la taille du hash jusqu'à un certain point(128/256 bits largement suffisant).
   >
   > - Pour une attaque par force brute : *2^(128/256)* essais pour une pré-image jusqu'à 2^80.
   > - 128 bits suffisent pour une attaque par force brute.
   >   - Pour trouver des collisions *2^(N/2)*. Pour atteindre *2^80 (Infaisable à l'heure actuelle)* il nous faut 160 bits. Cependant les collisions sont peu interessantes pour les mots de passe.
   > - Pour une attaque par dictionnaire, supposons qu'on a un hash de 128 bits
   >   - Supposons que l'on veuille stocker au moins 2^48 hash de mot de passe
   >   - 2^48 x 128bits = *64TBytes* !
   >
   > **Conclusion :** La sécurité du mot de passe dépend surtout du mot de passe (*Notion d'entropie*)

2. **Correction par Jad <3**

   > Le serveur stocke les mots de passe crypté (3-DES *à éviter pour des mots de passe de moins de 8 octets*, AES). Pour envoyer le mot de passe, il sera crypté avec le même algortihme et comparé avec celui stocké dans le serveur.
   > Le MAC est généralement envoyé en complément avec un différente clé du chiffré afin de vérifier l'intégrité des données.

3. Le principe des tables arc-en-ciel est quasiment le même que le compromis temps/mémoire. On va alterner une fonction de hachage et une fonction de réduction (qui elle produit un mot de passe à partir d'un haché). On va donc stocker beaucoup moins de mots de passe. En pratique on utilise t fonctions de réduction différentes pour réduite les fusions. En somme, les tables arc-en-ciel sont simplement un type de stockage optimisé dérivié du compromis temps/mémoire.

Exercice 2

1. Les modes opératoires standards (*or CBC*) ne sont pas adaptés car il ne permettent pas de modifier une section du mot chiffré. Si on chiffre un fichier de 2Go, on devra rechiffrer ce dernier dans son intégralité même si on ne change qu'un seul bit.

2. Il est plus adapté car son mode de chiffrement permet de délimiter des "secteurs" afin de pouvoir recrypter qu'une partie du fichier si on modifie ce dernier.

3. On va itérer sur les différents secteurs et appliquer la fonction de déchiffrement sur chacun d'eux.

Exercice 3

1.
   - Version du certificat
   - Numéro de série
   - Emetteur
   - Période de validité
   - Nom et informations au sujet de la clé publique du sujet
   - Nom de l'algorithme utilisant cette clé publique
2. Dans ce cas, l'utilisation d'un certificat va servir à identifier une carte, être sûr que c'est bien la bonne et réaliser l'authentification en étant sûr du demandeur.
3. L'autorité de certification.
4. Il garantit la confidentialité et l'intégrité des échanges.

Exercice 4 Correction par Quentin <3

1.
    - La machine de PIN Mailing
    - Le Back Office
    - La machine de PIN Mailing
2.
    - SAA
    - SAE
    - L'interface bancaire du réseau e-RSB
3.
    - Transhiffrement du PIN
4.
    - Vérification du PIN
5.
    - Génération du PIN
6.
    - Calcul de l'ARPC
    - Vérification de l'IDN
7.
    - Dérivation des clés maître Emetteur EMV
8.
    - Calcul de l'IDN
9.
    - Générer des clés
    - Effectuer des calculs cryptographiques
    - Permettre l'échange de clés symétriques tirées dynamiquement
10.
    - Trois
11.
    - Clé KTK