Exercices – Crypto / Sécu

Laurent Signac – CC-BY-SA – 07-02-21 1319 5c80794233ad922c609c

1 Cryptographie à clé publique

Pour quelle raison la cryptographie à clé publique a-t-elle fait son apparition ? Justifiez et argumentez.

2 Condensés

Pourquoi une fonction de hachage (SHA1 par exemple) ne peut-elle pas ête utilisée pour chiffrer des mails ou des sessions HTTP ?

3 Bruteforce DES

Supposons que le test d'une clé DES ne prenne qu'une microseconde sur un ordinateur personnel. À quelle durée faut il s'attendre pour retrouver la clé, si on n'a aucune indication dessus ?

4 RSA

Dans le système RSA, la qualité du codage dépend-elle de la clé de celui qui envoie le message ou de la clé de celui qui le reçoit ?

5 Chiffrement asymétrique

Le système de cryptographie asymétrique RSA peut être utilisé pour chiffrer des communications mais aussi pour les authentifier (signature numérique). Dans chacun des quatre cas suivants, indiquez si le but recherché nécessite l'utilisation de la clé privée ou publique de l'expéditeur ou du destinataire.

Action	clé publique/clé privée	de l'expéditeur/du destinataire
Envoyer un document chiffré		
Signer un message à envoyer		
Déchiffrer un document reçu		
Vérifier la signature d'un document reçu		

6 Stockage des mots de passe

1. Pourquoi stocke-t-on le condensé des mots de passe dans la base de données des utilisateurs plutôt que le mot de passe lui-même ?
2. Comment l'utilisateur est-il ensuite authentifié, puisque son mot de passe n'est pas stocké ?
3. La notion de sel consiste à ajouter une chaîne aléatoire au mot de passe, puis à stocker le sel ainsi que le condensé du mot de passe salé. À quoi cela sert-il ?
4. La notion de poivre (…) consiste à choisir une chaîne secrète (le poivre), qui ne **sera pas** stockée dans la base de données, et à poivrer les mots de passe avant hachage. À quoi cela sert-il ?