Université Mohammed V Agdal
Faculté des Sciences
Rabat

Année 2012-13
Master C2SI
Intro à la crypto
Contrôle continu

Aucun document n'est autorisé.

Exercice 1. Rappeler le protocole de Delffie-Helman. Donner un exemple de son application.

Exercice 2. Décrire le procédé de signature électronique en utilisant un algorithme de chiffrement asymétrique.

Peut-on utiliser un un algorithme de chiffrement symétrique pour construire un procédé de signature électronique ? Justifier votre réponse.

Exercice 3. Soit une fonction de hachage $h : \{0,1\}^* \longrightarrow \{0,1\}^m$.
Montrer que la recherche exhaustive de collisions a plus d'une chance sur deux d'aboutir après seulement $\mathcal{O}(2^{\frac{m}{2}})$.

Exercice 4. a) Rappeler le principe de Kerckhoffs.
b) Pourquoi doit-on absolument l'appliquer à tout algorithme de chiffrement ?

Exercice 5. Comment faire pour prouver que l'on connaît un secret mais sans avoir besoin de le révéler dans l'immédiat.

Exercice 6. Rappeler la construction de Merkele-Damgard.

Exercice 7. Expliquer comment utiliser une fonction de hachage h pour l'authentification.