UBE
UFR ST
mars 2025

Examen M2 Sécurité des données

durée 1h30
tous les documents issus du cours sont autorisés

Exercise 1 (3pt.) Expliquez en quelques phrases les propriétés souhaitées d'un protocole de signature numérique.

Exercise 2 (4pt.) Fonction de hachage

1. Expliquez brièvement les bonnes propriétés d'une fonction de hachage cryptographique.
2. Citez quelques exemples d'applications des fonctions de hachage cryptographique.

Exercise 3 (6pt.) Soit $p = 11$ et $q = 3$ deux 'grand' nombres premiers. Pour le protocole RSA, Alice choisit la clef publique $(n, e) = (33, 7)$.

1. Donner d, la clef privée de Alice,
2. Décrire le protocole RSA si le message à chiffrer est $x = 4$.
3. Décrire le protocole de signature électronique RSA avec $p = 11$ et $q = 3$.
4. Sur quoi repose la sécurité du protocole RSA ?

Exercise 4 (Protocole El-Gamal – 6pt.)
On se propose d'utiliser l'algorithme de chiffrement de El-Gamal avec $p = 11$.

1. Donner un générateur g pour $\mathbb{F}_{11}$.
2. Décrire le protocole de chiffrement de ElGamal avec $p = 11$ et g trouvé au point précédent.
3. Pourquoi ce protocole est-il considéré comme sûr ?
4. Adaptez le protocole de chiffrement d'El-Gamal pour la signature numérique.

Exercise 5 (1pt.) Le partage de clé secrète de Shamir (protocole SSS) est un algorithme de cryptographie qui attribue à chaque participant sa propre clé, certaines de ces clés étant nécessaires pour reconstruire un secret. Proposez, en expliquant en quelques phrases, un code détecteur d'erreurs basé sur le protocole SSS.