Contrôle final

Cryptographie et sécurité

11 Janvier 2024

1 Consignes

Vous avez 1h20 pour réaliser cette série d'exercices (1h45 pour les étudiants disposant d'un tiers temps). La calculette est interdite. N'hésitez pas à demander des éclaircissements à votre surveillant en cas de doute sur les énoncés.
Les étudiants qui réalisent ce DS sur ordinateur doivent me le transmettre par mail à l'adresse:
mickael.bettinelli@univ-smb.fr
Bonne chance.

2 QCM (5pts)

Le nombre de bonnes réponses est indiqué à chaque question. Entourer toutes les bonnes réponses donne 1 point, trouver au moins une bonne réponse 0.5 point. Sinon, 0 point.

1. **Lesquelles de ses propriétés sont souhaitables pour les méthodes de chiffrement ? (4 bonnes réponses)**

   A. La non-répudiation B. La confidentialité C. La vélocité D. L'authentification E. La sécurité F. L'intégrité des données

2. **Combien d'erreurs peut corriger le CRC dans un message ? (1 bonne réponse)**

   A. 0 B. 1 C. 2 D. 3

3. **Pour des questions de sécurité un utilisateur souhaite chiffrer les données de son disque dur, quel algorithme devrait-il utiliser ? (1 bonne réponse)**

   A. AES B. Diffie-Hellman C. RSA D. Vigénère

4. **Quelles sont les deux méthodes permettant de générer des clés partagées de manière sécurisée entre deux interlocuteurs ? (2 bonnes réponses)**

   A. L'autorité de certification B. La toile de confiance C. Diffie-Hellman D. Key Distribution Center

5. **Quel type de chiffrement symétrique est le plus adapté au streaming ? (1 bonne réponse)**vis

   A. Le chiffrement par bloc B. Le chiffrement par diffusion C. Le chiffrement par flot

3 RSA (4pts)

introduction Bob et Alice souhaitent communiquer de manière sécurisée. Pour cela, il s'apprêtent à utiliser RSA. A l'aide des clés suivantes:

- clef publique: p = 7, q = 3
- exposant: e = 5

aidez les à chiffrer les deux nombres suivants: *10 et 3*

4 Calcul d'inverse (4pts)

Calculez l'inverse de 9 sur Z/110Z avec l'algorithme d'Euclide étendu. Il est attendu que chaque étape du calcul soit compréhensible à la relecture (attention à la forme). Le résultat doit apparaître explicitement ("*L'inverse de 9 sur Z/110Z est ...*").

5 Fonctions de hachage (4pts)

Qu'est-ce qu'une fonction de hachage ? Expliquez leur fonctionnement.

6 L'authentification (3pts)

1. Décrivez comment authentifier un utilisateur avec les clés de RSA lors d'une communication.
2. Décrivez le protocole d'authentification utilisés par des interlocuteurs pour s'authentifier avec une paire de clés partagées.