

Contrôle : Sécurité et intégrité cryptographique des données

Janvier 2026

Durée 2h, tous documents non électroniques autorisés.

Le barème est donné à titre indicatif.

1. (3 points) Quelle est la différence entre une fonction de hachage pour les tables de hachage et une fonction de hachage cryptographique ?
2. (3 points) Comment peut-on utiliser la cryptographie asymétrique afin d'assurer l'authenticité de l'expéditeur ?
3. (4 points) La clé publique RSA est $(e, n) = (3, 15)$. Chiffrez le message $m = 8$.
4. (4 points) Calculez le couple p, q de nombres premiers à partir de la clé publique $(e, n) = (7, 143)$.
5. (6 points) Dans l'algorithme de génération de clés RSA, peut-on utiliser $e = 3$ si $p = 7$ and $q = 5$? Expliquer pourquoi.