SynaptikOne

Laboratoire d'Innovation Libre et Open Source

SynaptikOne

À propos de SynaptikOne :

SynaptikOne est un laboratoire d'innovation libre et open source, *totalement indépendant*. Nous ne sommes rattachés à aucune organisation ou institution. Notre mission est d'accompagner et d'aider tous les étudiants, qu'ils soient inscrits dans une université ou autodidactes. Nous offrons un environnement ouvert et collaboratif, afin que chacun puisse apprendre, expérimenter et innover librement.

Nous sommes également ouverts à toute collaboration, partenariat ou opportunité de projet. N'hésitez pas à nous contacter pour explorer ensemble de nouvelles idées et initiatives.

Rédigé par : Rakotondravelo Tahina Mickaël

Fondateur du Laboratoire SynaptikOne

Site web : `https://synaptikone.pages.dev/`

Facebook : Page Facebook SynaptikOne

Énoncé du sujet - Théorie des nombres et Cryptographie(Master 1, Parcours Informatique)

Université CNTEMAD — Session 2024–2025

1. Définir la cryptographie. Quels sont ses objectifs ?
2. Citer les quatre fonctions de la cryptographie. Expliquer.
3. La méthode de chiffrement classique est basée sur la combinaison de deux techniques. Lesquelles ? Citer quelques exemples. Quels inconvénients représentent ces chiffrements classiques ?
4. Expliquer le principe du chiffrement à clé secrète (symétrique). Quels sont les deux modèles de base d'algorithmes à clé secrète ? Citer des exemples de cryptosystèmes à clé secrète. Quels inconvénients représentent ces chiffrements à clé secrète ?
5. Expliquer le principe du chiffrement à clé publique (asymétrique). Sur quel principe se base l'algorithme de chiffrement à clé publique ? Citer des exemples de cryptosystèmes à clé publique. Quels inconvénients représentent ce type de chiffrement ?
6. Qu'est-ce qu'un cryptosystème hybride ?

Corrigé détaillé

Question 1 – Définir la cryptographie et ses objectifs

La **cryptographie** est la science et l'art de protéger l'information en la transformant de manière à ce qu'elle ne soit compréhensible que par les destinataires autorisés.
Objectifs :

— Confidentialité : empêcher l'accès non autorisé à l'information.
— Intégrité : garantir que l'information n'a pas été modifiée.
— Authenticité : permettre de vérifier l'identité de l'émetteur.
— Non-répudiation : empêcher un émetteur de nier avoir envoyé l'information.

Question 2 – Les quatre fonctions de la cryptographie

1. **Chiffrement** : transformer le message clair en message codé illisible pour les non-autorisés.
2. **Authentification** : vérifier l'identité des utilisateurs et des systèmes.
3. **Intégrité** : s'assurer que les données n'ont pas été altérées.
4. **Non-répudiation** : empêcher la dénégation d'un message ou d'une transaction.

Question 3 – Méthodes de chiffrement classiques

La méthode classique combine :

— **Chiffrement par substitution** : remplacer chaque symbole du message par un autre (ex. : chiffre de César, chiffre de Vigenère).

— **Chiffrement par permutation/transposition** : réorganiser les symboles du message (ex. : carré de Polybe, grille de Cardan).

Inconvénients :

— Facilement cassables par analyse statistique.

— Peu sûrs face aux attaques modernes.

— Gestion de clés peu pratique.

Question 4 – Chiffrement à clé secrète (symétrique)

Principe : le même secret (clé) est utilisé pour chiffrer et déchiffrer le message. **Modèles de base :**

— Algorithmes par bloc (ex. : AES, DES)

— Algorithmes par flux (ex. : RC4, Salsa20)

Inconvénients :

— Partage sécurisé de la clé difficile.

— Ne permet pas l'authentification directe.

— Risque si la clé est compromise.

Question 5 – Chiffrement à clé publique (asymétrique)

Principe : deux clés distinctes : clé publique pour chiffrer et clé privée pour déchiffrer. **Algorithme basé sur :** problèmes mathématiques difficiles (ex. : factorisation, logarithme discret). **Exemples de cryptosystèmes :** RSA, Diffie-Hellman, ECC. **Inconvénients :**

— Plus lent que les systèmes symétriques.

— Gestion des clés plus complexe.

— Susceptible aux attaques si les clés sont mal générées.

Question 6 – Cryptosystème hybride

Un **cryptosystème hybride** combine le chiffrement symétrique et asymétrique :

— Chiffrement asymétrique pour l'échange sécurisé de la clé symétrique.

— Chiffrement symétrique pour le traitement rapide des données.

Avantages : rapide, sécurisé et pratique pour les communications modernes (ex. : HTTPS, TLS).

Licence

Remarque

Les corrigés proposés par le Laboratoire SynaptikOne sont élaborés avec soin et rigueur. Cependant, en raison du nombre important de sujets, projets et documents traités quotidiennement, il est possible que certains corrigés comportent des erreurs ou des imprécisions. Nous invitons chaque lecteur à nous signaler toute correction ou suggestion d'amélioration, afin de contribuer ensemble à l'enrichissement et à la fiabilité de nos ressources pédagogiques.