Grand Oral

16, Mai 2024

Lucas Duchet-Annez

Problématique

Comment sécurisons-nous nos conversations ?

Plan

1. Contexte et Introduction

- Présentation du contexte : les communications électroniques sont de plus en plus courantes dans notre vie quotidienne, mais cela pose des risques de sécurité
- Présentation du sujet : les mathématiques permettent de sécuriser nos conversations en utilisant des algorithmes de cryptographie basés sur des principes mathématiques solides
- But de l'exposé : montrer comment les mathématiques permettent de sécuriser nos conversations en utilisant des exemples concrets
- Choix du sujet : expliquer les raisons

2. Les clés asymétriques et symétriques

- Définition des clés asymétriques : une paire de clés, l'une publique et l'autre privée, utilisées pour chiffrer et déchiffrer les messages
- Explication du principe des clés asymétriques : utilisation de la théorie des nombres, notamment le petit théorème de Fermat
- Définition des clés symétriques : une seule clé utilisée à la fois pour chiffrer et déchiffrer les messages

Explication du principe des clés symétriques : utilisation de l'algorithme AES (Advanced Encryption Standard)

3. Exemples d'utilisation concrète

- Exemple 1 : le protocole SSL/TLS (Secure Sockets Layer/Transport Layer Security) qui utilise des clés asymétriques pour sécuriser les communications sur internet
- Exemple 2 : le chiffrement des données avec l'algorithme AES (Gestionnaire de mot de passe)
- Exemple 3 : la signature numérique RSA (Rivest-Shamir-Adleman) qui utilise des clés asymétriques pour authentifier et vérifier l'intégrité des données (Authentification)

4. Conclusion

Reprendre les idées principales

Elements mathématiques

Petit théorème de Fermat: $a^p \equiv a \pmod{p}$ si p est premier (RSA) Fonction indicatrice d'Euler $C \equiv M^e \pmod{n}$ Chiffrement $M \equiv C^d \pmod{n}$ Déchiffrement Congruence (RSA) Nombre premier

Matrice (AES)

Sources

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf
- https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf
- https://fr.wikipedia.org/wiki/Cryptographie
- https://fr.wikipedia.org/wiki/Advanced_Encryption_Standard
- https://fr.wikipedia.org/wiki/Chiffrement_RSA
- https://www.di.ens.fr/~nitulesc/files/crypto3.pdf
- https://www.youtube.com/playlist?list=PLBlnK6fEyqRgj06MEnp2VebJ8DgMpF0Zj

IA

Je me suis aidé d'une IA pour faciliter les itérations du plan et me donner des pistes pour commencer les recherches