Projet de Cryptographie : AES, DES RSA

Mohamed Taha Aboumehdi Hassani, Wadie Kadiri

Décembre 2024

Résumé

Ce rapport présente un projet de cryptographie implémentant trois algorithmes majeurs : AES (Advanced Encryption Standard), DES (Data Encryption Standard), et RSA (Rivest-Shamir-Adleman). L'objectif est de permettre une démonstration pratique et une compréhension approfondie de ces algorithmes de cryptographie avec des exemples concrets.

Table des matières

1 Introduction

La cryptographie est une composante essentielle de la sécurité de l'information. Le présent projet vise à implémenter trois algorithmes cryptographiques classiques : AES, DES, et RSA. Ces algorithmes sont étudiés pour permettre une compréhension pratique de leurs principes fondamentaux et de leur mise en œuvre.

2 Présentation du Projet

2.1 Objectifs

L'objectif principal de ce projet est de démontrer l'utilisation des algorithmes de cryptographie symétriques et asymétriques suivants :

- **AES (Advanced Encryption Standard)** : Utilisé pour le chiffrement avec une clé symétrique (128, 192 ou 256 bits).
- **DES (Data Encryption Standard)** : Un algorithme basé sur une structure de Feistel avec 16 tours de chiffrement.
- **RSA (Rivest-Shamir-Adleman)** : Un algorithme asymétrique utilisant une clé publique/privée pour sécuriser les échanges.

2.2 Algorithmes Implémentés

- **AES :** Cet algorithme est implémenté avec les fonctionnalités suivantes :
  - Génération de sous-clés
  - Chiffrement et déchiffrement de données
- **DES :** Fonctionne avec la structure de Feistel sur 16 tours, et inclut :
  - Le chiffrement par blocs
  - Le déchiffrement par blocs
- **RSA :** Un algorithme asymétrique avec les fonctionnalités suivantes :
  - Génération de clés publiques et privées
  - Chiffrement de messages
  - Déchiffrement de messages

3 Structure des Fichiers

Le projet est organisé comme suit :

— **aes.h / aes.c :** Implémentation complète de l'algorithme AES avec ses fonctionnalités.

— **des.h / des.c :** Implémentation de l'algorithme DES avec chiffrement et déchiffrement par blocs.

— **rsa.h / rsa.c :** Implémentation de l'algorithme RSA avec chiffrement/déchiffrement et génération de clés.

— **main.c :** Exemple pratique démontrant le fonctionnement des algorithmes AES, DES et RSA.

— **Makefile :** Permet la compilation rapide du projet.

4 Instructions

4.1 Compilation

Assurez-vous que tous les fichiers du projet sont dans le même répertoire. Utilisez la commande suivante pour compiler le projet :

```
make
```

4.2 Exécution

Une fois la compilation terminée, exécutez le programme avec la commande suivante :

```
./rsa_des_aes
```

4.3 Nettoyage

Pour supprimer les fichiers intermédiaires, utilisez la commande suivante :

```
make clean
```

5 Exemple de Résultat

5.1 AES

— Texte clair : 101010...
— Texte chiffré : 111000...

5.2 DES

— Texte clair : 01010101...
— Texte chiffré : 11001100...

5.3 RSA

— Clé publique : (e = 17, n = 3233)
— Clé privée : (d = 413, n = 3233)
— Message original : 65
— Message chiffré : 2790
— Message déchiffré : 65

6 Prochaines Étapes

— Ajouter un support pour des tailles de clés RSA plus grandes.
— Implémenter le mode CBC pour l'algorithme DES.
— Développer un ensemble de tests automatisés pour valider l'ensemble des fonctions implémentées.

7 Conclusion

Ce projet a permis la mise en pratique de concepts cryptographiques fondamentaux, en explorant l'implémentation de trois algorithmes majeurs : AES, DES et RSA. Ces démonstrations offrent une meilleure compréhension de la cryptographie moderne.