Cahier des Charges
Projet de Cryptographie : AES, DES RSA

Mohamed Taha Aboumehdi Hassani, Wadie Kadiri

Décembre 2024

Table des matières

1 Contexte

La cryptographie est une discipline fondamentale pour la sécurité des systèmes d'information et la protection des communications sur les réseaux. Le projet de cryptographie présenté dans ce cahier a pour objectif la mise en place d'algorithmes de chiffrement modernes. Ces algorithmes incluent AES, DES, et RSA, afin de permettre leur étude pratique et leur démonstration.

2 Objectifs du Projet

- Implémenter et étudier trois algorithmes de cryptographie majeurs :
  - AES (Advanced Encryption Standard), un algorithme symétrique basé sur des clés de taille 128, 192 ou 256 bits.
  - DES (Data Encryption Standard), basé sur la structure de Feistel avec 16 tours de chiffrement.
  - RSA (Rivest-Shamir-Adleman), un algorithme de cryptographie asymétrique basé sur la cryptographie à clé publique.
- Démontrer le fonctionnement pratique de ces algorithmes avec des exemples concrets.
- Faciliter la comparaison des algorithmes symétriques et asymétriques dans leurs usages pratiques.
- Préparer une documentation complète expliquant les fonctionnalités de chaque algorithme implémenté.

3 Description des Fonctionnalités

3.1 AES - Advanced Encryption Standard

— Génération de sous-clés nécessaires pour le chiffrement.
— Chiffrement et déchiffrement de données avec une clé symétrique de 128, 192 ou 256 bits.

3.2 DES - Data Encryption Standard

— Chiffrement par blocs avec une structure de Feistel sur 16 tours.
— Déchiffrement correspondant aux blocs chiffrés avec la même clé.

3.3 RSA - Rivest-Shamir-Adleman

— Génération de clés publiques et privées pour la cryptographie asymétrique.
— Chiffrement de messages avec la clé publique.
— Déchiffrement avec la clé privée correspondante.

4 Exigences Fonctionnelles

Les fonctionnalités attendues pour ce projet sont les suivantes :

1. Implémentation correcte de l'algorithme AES avec une démonstration sur plusieurs tailles de clés (128, 192, 256 bits).
2. Implémentation correcte de l'algorithme DES avec les opérations de chiffrement et déchiffrement par blocs.
3. Implémentation correcte de l'algorithme RSA avec la génération de clés, chiffrement, et déchiffrement.
4. Intégration de toutes ces fonctionnalités dans un programme principal unique pour la démonstration.
5. Génération de sous-clés dynamiques pour AES et DES.
6. Simulation d'échanges sécurisés avec RSA pour montrer l'importance de la cryptographie asymétrique.

5 Exigences Techniques

5.1 Environnement de Développement

— Langage de programmation : C
— Outils : `gcc`, `make`, `pdflatex` pour la documentation.
— Système d'exploitation : Multiplateforme (Linux, Windows, macOS).

5.2 Dépendances

Le projet utilise uniquement la bibliothèque standard C :
— `stdio.h`
— `stdlib.h`
— `string.h`

5.3 Structure des Fichiers

Les algorithmes doivent être organisés selon la structure suivante :
— **aes.h / aes.c** : Implémentation de l'algorithme AES.
— **des.h / des.c** : Implémentation de l'algorithme DES.
— **rsa.h / rsa.c** : Implémentation de l'algorithme RSA.
— **main.c** : Programme principal démontrant les trois algorithmes avec des exemples pratiques.
— **Makefile** : Permet la compilation avec la commande `make`.

6 Contraintes

6.1 Contraintes Fonctionnelles

— Toutes les fonctionnalités doivent être complétées pour le bon fonctionnement des algorithmes AES, DES, et RSA.
— Chaque module doit être bien testé pour valider les résultats des opérations cryptographiques.

6.2 Contraintes Techniques

— Utiliser uniquement les fonctions standards en C.
— Le code doit être portable sur les systèmes Linux, Windows, et macOS.

7 Planification

7.1 Phases du Projet

— **Phase 1 : Analyse et conception** (2 semaines)
— **Phase 2 : Développement des fonctionnalités AES, DES et RSA** (4 semaines)
— **Phase 3 : Tests et validation** (2 semaines)
— **Phase 4 : Rédaction de la documentation et du rapport final** (2 semaines)

8 Livrables

Les livrables attendus pour ce projet sont :

— Le code source complet avec les algorithmes AES, DES, et RSA.
— Le Makefile pour faciliter la compilation.
— Un rapport détaillé (rédigé en LaTeX) incluant l'analyse, le processus de conception, et les résultats.
— Une démonstration avec des exemples concrets pour illustrer le fonctionnement des algorithmes.

9 Conclusion

Le présent cahier des charges vise à définir clairement les objectifs, les fonctionnalités, les contraintes, et la planification nécessaires pour la réalisation du projet. La réussite de ce projet permettra une meilleure compréhension pratique des algorithmes cryptographiques symétriques (AES, DES) et asymétriques (RSA).