CSE546 Applied Cryptography - Project Proposal

Ankit Bisht[1] and Ankit Kumar[2]

[1]ankit21014@iiitd.ac.in
[1]ankit21015@iiitd.ac.in

10 September 2024

1 CryptXpert: Online Encryption and Decryption Platform

CryptXpert is an online cryptography tool designed to allow users to easily encrypt and decrypt data using various cryptographic algorithms. The platform focuses on both symmetric and asymmetric encryption techniques, enabling users to securely protect their data and explore the inner workings of modern cryptographic systems. The primary goal of CryptXpert is to provide a user-friendly interface for users to encrypt and decrypt plaintext, create public private keys or generate hashes.

1.1 Key Features

- **Multiple Cryptographic Algorithms**: Users can choose from a variety of modern algorithms such as AES, RSA for encryption and decryption.
- **Real-Time Key Pair Generation**: Asymmetric encryption algorithms like RSA allow users to generate and manage public-private key pairs directly on the platform.
- **User-Friendly Interface**: Simplified interface for both novices and experienced users to test and visualize encryption processes.
- **Encryption for Text and Files**: Users can input plaintext messages or upload files for encryption and decryption.

2 Motivation

The main motivation behind CryptXpert is to actually understand theoretical cryptographic algorithms and do a practical implementation. Understanding the fundamentals of encryption and decryption requires hands-on experimentation, and CryptXpert will help us to understand various algorithms and we'll build them bottom up without using any packages.

3 Website Sections

CryptXpert will have the following key sections:

- **Home**: Introduction to the platform, including a brief overview of the available cryptographic algorithms.
- **Encrypt/Decrypt**: The main interface for users to input plaintext or upload files, choose encryption algorithms, and view the encrypted or decrypted outputs.
- **Key Management**: A dedicated section for generating, uploading, and managing public and private keys.
- **Hashes**: A section for creating/converting strings to hashes.
- **Documentation**: Detailed documentation on how to use the platform, including usage examples and FAQs.

4 Deliverables

By the end of this project, we aim to deliver:

- A fully functional web platform with encryption and decryption capabilities for multiple cryptographic algorithms, implemented from scratch.
- Key generation and management tools for asymmetric encryption.

5 Supported Algorithms

– Symmetric: AES, DES, 3DES, Blowfish, RC4
– Asymmetric: RSA, ElGamal
– Hashes: SHA-256, SHA-512, MD5

6 References

- Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice.* Pearson.
- Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography.* CRC Press.
- Awesome Cryptography *https://github.com/sobolevn/awesome-cryptography.*