CIS 628 Introduction to Cryptography

Syracuse University

Fall 2023

Advanced Encryption Standard (AES) Encryption and Decryption Tool

List of the team members in the group.

Mandar Angchekar – 386916341
Paras Suri - 5643363582

What is the project about?

The project endeavours to enhance a cryptographic tool leveraging the Advanced Encryption Standard (AES) to bolster the security of file encryption and decryption operations. AES is globally acknowledged as a steadfast symmetric encryption algorithm, praised for its robustness and speed. The central objective of this project is to engineer a comprehensive AES-based encryption system using Python, aiming to simplify the process of securing files for transmission or archival purposes. By crafting a tool that combines the reliability of AES with an intuitive user interface, the project seeks to demystify encryption for non-experts, thereby fostering widespread adoption of strong cryptographic practices. It will bridge the gap between complex encryption technologies and everyday users, ensuring that sensitive information remains confidential and impervious to unauthorized access. This initiative is a stride towards integrating advanced security measures with ease of use, intending to promote a safer digital environment for personal and professional data management.

How is it done today and the limits of the current practice?

Current implementations of AES encryption require users to have a certain level of technical expertise, particularly in the areas of key management and operational procedures. This complexity often cerate’s a barrier to entry, deterring individuals who are not well-versed in cryptographic concepts from utilizing encryption tools. Such a scenario not only undermines the security of data but also hampers the widespread adoption of encryption technologies. Furthermore, the intricacies involved in the secure generation, storage, and exchange of encryption keys are not always adequately addressed by existing software, posing significant risks to the confidentiality and integrity of sensitive information.

Mandar Angchekar
Research paper: “ANALYSIS AND DESIGN OF FILE SECURITY SYSTEM AES (ADVANCED ENCRYPTION STANDARD) CRYPTOGRAPHY BASED"

Review: This research focuses on enhancing data security through the Advanced Encryption Standard (AES). It addresses the need for cryptographic measures to protect against data breaches, such as theft and unauthorized alterations. The paper outlines a research framework that includes identifying security issues, analyzing file security, and studying AES cryptography. It also details the development and testing of an AES-based cryptographic system, with a user interface designed for ease of use in encryption tasks. The findings aim to contribute to the field by offering improvements in data encryption practices.

Research paper:
“AES ALGORITHM-BASED FILE TRANSFER SYSTEM”

Review: The research paper focuses on the use of Advanced Encryption Standard (AES) in securing data during transmission. It emphasizes the importance of encryption and decryption in cryptography, with AES highlighted for its efficiency and robust security features. The paper compares AES to other encryption algorithms, demonstrating AES's superior speed and reliability for both encryption and decryption tasks.

A practical application is presented where AES is used in a file transfer system, ensuring secure data handling within an organization. The system employs AES for encryption during file upload and decryption during download, with a user interface developed using HTML and CSS, and backend processes powered by Java. Overall, the paper advocates for AES as a highly effective tool for protecting data against unauthorized access, especially in organizational data transfers.

Paras Suri
Research paper: “PARALLEL MULTIPROCESSING AND SCHEDUULING ON THE HETEROGENEOUS XEON+FPGA PLATFORM”

Review: The paper explores the enhancement of heterogeneous computing through a novel scheduling framework on a CPU-FPGA platform, specifically the Intel HARP system. The study demonstrates that a dynamic, adaptive scheduler can significantly outperform traditional CPU or FPGA-only systems, achieving up to an 8-fold increase in performance. The authors introduce a hybrid algorithm for the n-body problem, tailored to the unique capabilities of both CPUs and FPGAs, and present the Heterogeneous Adaptive Partitioner (HAP) scheduler. This scheduler adeptly balances the computational load between CPUs and FPGAs, showcasing substantial improvements in efficiency and performance. The paper's findings are pivotal for advancing programming models for high-performance, energy-efficient computing in heterogeneous architectures.

Research paper: “ADVANCED ENCRYPTION STANDARD(AES) SECURITY ENHANCEMENT USING HYBRID APPROACH”

Review: The paper proposes a novel enhancement to the Advanced Encryption Standard (AES) to counteract sophisticated cyberattacks. By integrating Dynamic Key Generation and Dynamic S-box Generation, the authors aim to bolster AES against common cryptographic attacks such as Brute-force and Algebraic attacks. The dynamic aspect of the key and S-box introduces complexity, increasing the encryption's resistance to attacks by adding layers of confusion and diffusion. While the theoretical framework suggests improved security, the paper lacks empirical analysis and does not discuss the impact of these enhancements on the algorithm's performance. The proposed method's practicality in real-world applications remains to be evaluated through rigorous cryptanalysis and performance testing.

Common Project Proposal

This team would involve the development of an Advanced Encryption Standard (AES)-based software tool designed to enhance data security for file encryption and decryption. This project aims to address the complexity and accessibility issues present in current cryptographic practices by creating a user-friendly interface that simplifies key management and operational procedures for users with limited technical expertise. Drawing from the collective research, our tool will integrate dynamic key generation and S-box generation to bolster security, as well as incorporate an adaptive scheduling system inspired by heterogeneous computing advances to improve performance. The project targets making AES encryption more approachable for everyday use while maintaining high standards of data confidentiality and integrity.

What is your approach to solve the problem?

The strategy to address the challenges of AES encryption involves constructing a Python-based application that marries AES's robust security features with a user-friendly graphical interface (GUI), effectively lowering the entry barrier for users. The design of the tool centers on a seamless user experience, where complex cryptographic operations are conducted behind a minimalist two-button GUI—one for initiating encryption and the other for decryption. This simplicity is key to encouraging wider adoption among users who may otherwise be daunted by the technicalities of encryption software.

To ensure the security of the encryption, the tool will incorporate the Python **Crypto.Random** module, which is designed to generate cryptographically strong random numbers that will serve as keys. These keys are the cornerstone of AES encryption, and their strength is vital to prevent breaches. The GUI will provide users with a secure method to save or export the generated keys, with clear instructions on how to safely handle this sensitive information.

Under the hood, the **Crypto.Cipher** module will be used to implement the AES encryption and decryption processes. This module is widely recognized for its adherence to contemporary cryptographic standards, ensuring that the tool is not only secure by current benchmarks but also maintained with forward compatibility in mind.

Thorough testing will be a pivotal phase in the project, with the tool being rigorously evaluated across different file formats and sizes. This testing will ensure that the tool maintains integrity and data security across diverse use cases, from text documents to larger multimedia files. Particular attention will be paid to the performance of the tool during these operations to ensure that security does not come at the expense of efficiency.

What is the novelty of the work? What is the deliverable?

The innovative aspect of this endeavor is its dual focus on demystifying the intricacies of cryptographic procedures and reinforcing security protocols. By creating an application that uses the Advanced Encryption Standard (AES), this project addresses a critical need for safeguarding user data against unauthorized access. Recognizing that one of the barriers to widespread utilization of cryptographic tools is their complexity, this project aims to bridge the gap by delivering a tool that combines ease of use with robust encryption.

The final product of this project will be an efficient, user-friendly tool for encrypting and decrypting files. The interface will be designed with the layperson in mind, ensuring that users without extensive knowledge of cryptography can operate it effectively. Its distinctive feature will be the ability to encrypt files with a mere click, a significant enhancement over existing tools that often require multiple steps to secure a file. Moreover, the application will handle the encryption keys in a secure manner, automating their safe storage and retrieval, which is a common challenge in encryption practices.

By the completion of this project, the tool will not only serve as a means to protect data but will also exemplify a leap forward in the practical application of cryptographic techniques. This contribution is expected to resonate within the data security domain, promoting a more accessible approach to preserving data confidentiality.