Tahim Bhuiya

April 21, 2024

CIS5371/CIS 4634: Practical Aspects of Modern Cryptography

**Practical Aspects of Modern Cryptography Final Project**

**Introduction**

Encryption plays a crucial role in safeguarding data from unauthorized access. However, implementing encryption schemes can be complex and intimidating. To address this challenge, this project introduces a user-friendly interface powered by the open-source Python library, ‘Streamlit’. This interface simplifies the process of selecting and implementing various encryption schemes allowing the user to properly encrypt and decrypt with ease.

**Functionality**

This project offers a range of encryption schemes, each serving distinct purposes:

ElGamal - Asymmetric Encryption Scheme: Utilizes public and private keys for encryption and decryption. Ideal for secure communication and digital signatures.

DES - Symmetric Encryption Scheme: Employs a single secret key for both encryption and decryption. Known for its speed and simplicity, suitable for large-scale data encryption.

3DES - Symmetric Encryption Scheme: Triple Data Encryption Standard enhances security by applying DES algorithm three times consecutively. Offers better protection against brute-force attacks than DES.

Blum-Goldwasser Probabilistic Scheme - Asymmetric Encryption: Provides secure encryption with a probabilistic approach. Suitable for scenarios requiring high levels of security and randomness.

Hybridized Scheme – ElGamal and DES: Combines the strengths of asymmetric and symmetric encryption for enhanced security and efficiency. Well-suited for scenarios demanding a balance between security and performance.

Hybridized Scheme – ElGamal and 3DES: Fusion of ElGamal and 3DES encryption schemes, offering robust security with triple-layered encryption. Ideal for scenarios necessitating maximum protection against sophisticated attacks.

**User Interface**

The Streamlit-based interface provides a seamless experience for users to interact with encryption schemes effortlessly:

Selection menu allows users to choose their desired encryption scheme.

Input fields enable users to input plaintext and select encryption parameters.

Real-time feedback and error handling enhance user experience and ensure smooth operation.

Output display presents encrypted data and decryption results in a clear and accessible format.

**Conclusion**

In summary, this project bridges the gap between encryption complexity and user accessibility. By leveraging the Streamlit framework, it empowers users to implement robust encryption schemes with minimal effort. Whether securing sensitive communications or protecting valuable data, this interface offers a streamlined solution for encryption needs. With its user-friendly design and versatile functionality, this project stands as a valuable tool in the pursuit of digital security.