Shamir’s Secret Encryption Breaking

Group – 9

Pardha Saradhi Pamarthi

Eeshwar Reddy Kotha

Litwin

Hemanth Kumar Munagala

Objective:

This project's goal is to breakdown and decipher Shamir's Secret Encryption, a unique encryption method used in the supplied code. The main goals will be to comprehend the encryption process, spot security holes, and create a way to decrypt messages without needing to know the secret key.

Project Elements & Implementation:

1. Encryption Scheme Analysis:

   To comprehend the encryption procedure, thoroughly examine the source code that has been provided.
   Determine which of Shamir's Secret Encryption's essential elements are present in the code.
   Examine the implementation's flaws and vulnerabilities.

2. Mathematical Model Development:

   Based on the components that have been identified, create a mathematical model that depicts the encryption process.
   Comprehend how the encryption and decryption processes are affected by the randomly generated key.

3. Cryptanalysis Techniques:

Examine established cryptanalysis methods that can be used to Shamir's secret sharing plans.
Examine the implementation for any potential vulnerabilities or side-channel attacks.

4. Statistical Analysis:

   Create a brute-force strategy to try every key combination and evaluate this method's viability.
   Examine encrypted messages statistically to find trends or vulnerabilities that can help with decryption.
5. Decryption Tool:

   Put into practice a decryption tool that draws from the analysis and mathematical model.
   To make sure the tool works, test it with encrypted messages.

6. Documentation & Reporting:

   Record every step of the analysis, model-building, and tool-implementation processes.
   Write a thorough report describing the advantages and disadvantages of Shamir's Secret Encryption in the example situation.

Implementation Overview:

This implementation, as shown in the provided Python source code, takes a multifaceted approach to breaking the unique encryption scheme used in Shamir's Secret Sharing. The project involves the creation of a mathematical model that represents these cryptographic operations after a thorough source code analysis is conducted to understand the nuances of the encryption and key generation procedures. One of the project's main objectives is to investigate different cryptanalysis methods, such as statistical analysis and brute-force attacks. Then, using the mathematical model and the knowledge gathered from the analysis, a decryption tool is put into practice. The decryption tool's accuracy and effectiveness are guaranteed by rigorous testing and validation. The entire procedure is well documented, yielding a thorough report that explains the results and highlights the advantages and disadvantages of the Shamir's Secret Sharing encryption method.

Conclusion:

By using Shamir's Secret Sharing to break the custom encryption scheme, this project assumes to increase knowledge of its flaws and restrictions. The creation of useful decryption tools will bring light on the security implications of this particular application of Shamir's Secret Encryption.