

Cybersecurity project

Shamir’s Secret Encryption Breaking



[Date]

Student Name

Student ID

Table of Contents

[1 Project Overview 2](#_Toc163471447)

[2 Completed Activities 2](#_Toc163471448)

[3 Current Status 2](#_Toc163471449)

[4 Next Steps 3](#_Toc163471450)

[5 Conclusion 3](#_Toc163471451)

[6 Reference 5](#_Toc163471452)

# Project Overview

The objective of the project is to break Shamir's Secret Encryption, a unique way to protect data that relies on Shamir's Secret Sharing. Considering a polynomial with random values in certain locations is needed to make an encrypted pair, and a generated at random key is required to indicate the difference between genuine and counterfeit pairs. For the decrypted flag, the polynomial values are obtained using Lagrange interpolation before assessing the polynomial. Shamir's Secret Encryption encrypts messages, and the goal is to figure out how to retrieve them, as well as the difficulty it is to break.

# Completed Activities

**Source Code Analysis:**

The journey began with a close look at the provided Python source code. Listed below are the first things we observed while we examined into it:

* It was necessary to make a polynomial with random values and assess it in specific places to get encrypted pairs for encoding to function properly.
* A key was created to indicate the difference between "real" pairs (locked with the polynomial) and "fake" pairs (made by chance).
* It needed to use Lagrange interpolation to identify the polynomial coefficients and calculate the polynomial at x=0 to obtain the decrypted flag. The procedure taught us more about the way Shamir's Secret Encryption works (Maji, et al., 2021). The fundamental parts of both the encryption and decryption methods can be found by carefully examining the code. Therefore, it could be done to look into and study more.



Figure 1 Source code analysis

# Current Status

**Mathematical Model Development:**

As we continue to look at the source code, the primary objective now is to make a mathematical model that correctly demonstrates the way encryption and decryption process. The point of it is to teach us a bit more about cryptography and the way the randomly generated key works with it. It includes success in these areas:

* In order to figure out a way to get returned polynomial values from encrypted pairs, it's necessary to learn about Lagrange interpolation. It is endured hard for people to figure out where this technique for interpolation fits into Shamir's Secret Encryption. The process of action is continuing.
* The ways of both encryption and decryption are being studied to see the way the randomly generated key changes them (Gupta, et al., 2020). An important part of this study involves looking at how changes in the key impact both how fast the decryption step works and how safe the technique for encryption is. The main goal of this field of research is to learn more about Shamir's Secret Encryption to people comprehend it better.

# Next Steps

**Cryptanalysis Techniques:**

To break Shamir's Secret Encryption and find any holes, we plan to look at some distinct cryptanalysis methods. It means the following to follow these steps:

* To find vulnerabilities in the encryption system, standard cryptanalysis methods like brute-force attempts and statistical evaluation. With these techniques, to be able to find vulnerabilities as well as flaws in Shamir's Secret Encryption that will let us decrypt it (Gupta, and Bedekar, 2021).
* The code is being examined very carefully to determine if there are any vulnerabilities or side-channel vulnerabilities that could allow someone to get past the security. To ensure that messages obtained with Shamir's Secret Sharing can be read, it is anticipated that an in-depth examination will show any flaws or holes in the code. This approach is crucial for those who want to figure out how to break Shamir's Secret Encryption and what its limits are as individuals (Abdel Hakeem, and Kim, 2022).

# Conclusion

In general, it looks like the initial work on breaking Shamir's Secret Encryption has been going well. Following an in-depth examination of the given source code, work on a mathematical model has started. Additionally, there are currently studies on cryptanalysis techniques, and now people are working on a tool that will decode messages. The work that's coming up is going to involve mostly making strategies better, researching more, and attempting to figure out messages that Shamir's Secret Sharing has submerged. The investigation shows how driven and dedicated people are in figuring out Shamir's Secret Encryption and reaching their project's goals, which is challenging but gratifying.

# Reference

Maji, H.K., Nguyen, H.H., Paskin-Cherniavsky, A., Suad, T. and Wang, M., 2021, June. Leakage-resilience of the shamir secret-sharing scheme against physical-bit leakages. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 344-374). Cham: Springer International Publishing.

Gupta, K.D., Rahman, M.L., Dasgupta, D. and Poudyal, S., 2020, January. Shamir's secret sharing for authentication without reconstructing password. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0958-0963). IEEE.

Gupta, V. and Bedekar, S., 2021. Alternative to Shamir’s secret sharing scheme Lagrange interpolation over finite field. *Int. J. Tech. Res. Sci*.

Abdel Hakeem, S.A. and Kim, H., 2022. Centralized threshold key generation protocol based on Shamir secret sharing and HMAC authentication. *Sensors*, *22*(1), p.331.