SHAMIR SECRET SHARING

INTRODUCTION

“Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Counting on all participants to combine the secret might be impractical, and therefore sometimes the threshold scheme is used where any “k” of the parts are sufficient to reconstruct the original secret.”

SRC: Wikipedia

LINK TO THE VIDEO

https://www.screencast.com/t/e7BkKc4w6PT

PROCEDURE

We were asked to basically build on a given UI. We should implement methods to

create the shares:

1) For creating shares, I took a random finite modulo prime value, a1 and a2
2) A0 was taken as the secret and f(x) was build
3) For x values 1 to 5 shares were computed and displayed in the panel.

Reconstruct the Secret:

1) The share values were taken from the panels.
2) For each share values, it is passed through the Lagrange interpolation and substituting the value of x as 0 we would get our secret back
3) Each secret is retrieved back and collected in a string buffer and finaaly stored as a string and displayed in the panel

CHANGES MADE TO UI

1) Added 2 jTextFields to display the time taken to construct the share and also to reconstruct back the secret
2) For the bonus question added a checkbox called “Construct Full Polynomial” Once checked will construct shares by having secret 1 as a0 and secret 2 as a1. This pattern repeats for all the secret values.

ANALYSIS

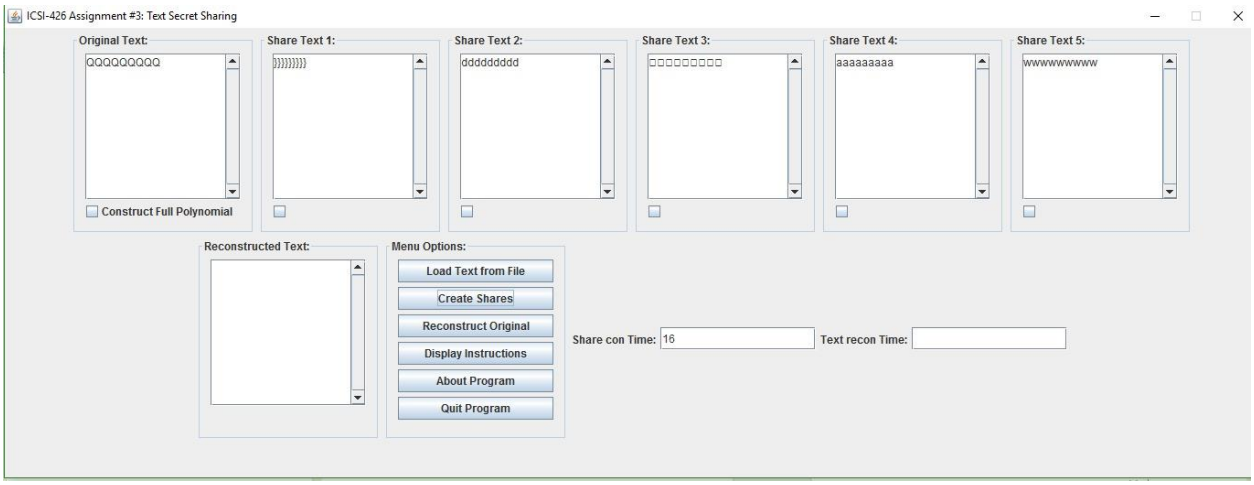
1) Observe the share creation and secret reconstruction times for texts of varied sizes i.e. 50, 100, 200, 400, 800, 1600 and 3200 words, and provide your observations in a table

Text size (words)	**50**	**100**	**200**	**400**	**800**	**1600**	**3200**
Share creation (ms)	30	38	45	49	67	94	132
Secret Reconstruction (ms)	16	21	30	34	58	81	118

2) Also analyze whether you can get some knowledge about the original text from the shares. Specifically, does it withstand the frequency analysis attack? If yes, suggest the changes you would do in the methodology to make it secure against this attack?

It's difficult to get knowledge about the secret values from the shares as all the shares with have same probability But still its **prone to frequency attack**.

Lest say we give the secret as a same value.



The share value in each share would be the same.

We can overcome this by choosing random values of x. In this code, the x values are fixed. But if we choose a random value then we can overcome this situation.