Shamir secret cryptography

Shamir secrets are used to store secrets and share them with multiple parties. Only by associating all or some of the pieces of the secret together can the recipient recreate the original message.

Motivation

Shamir secrets are useful tools for creating partial messages that can be sent over gossiping networks. They preserve a form of privacy.

Scope of work

Review existing Shamir secret implementations out there. Some exist in Java but are no longer maintained.

Implement an easy Shamir secret generation and recovery.