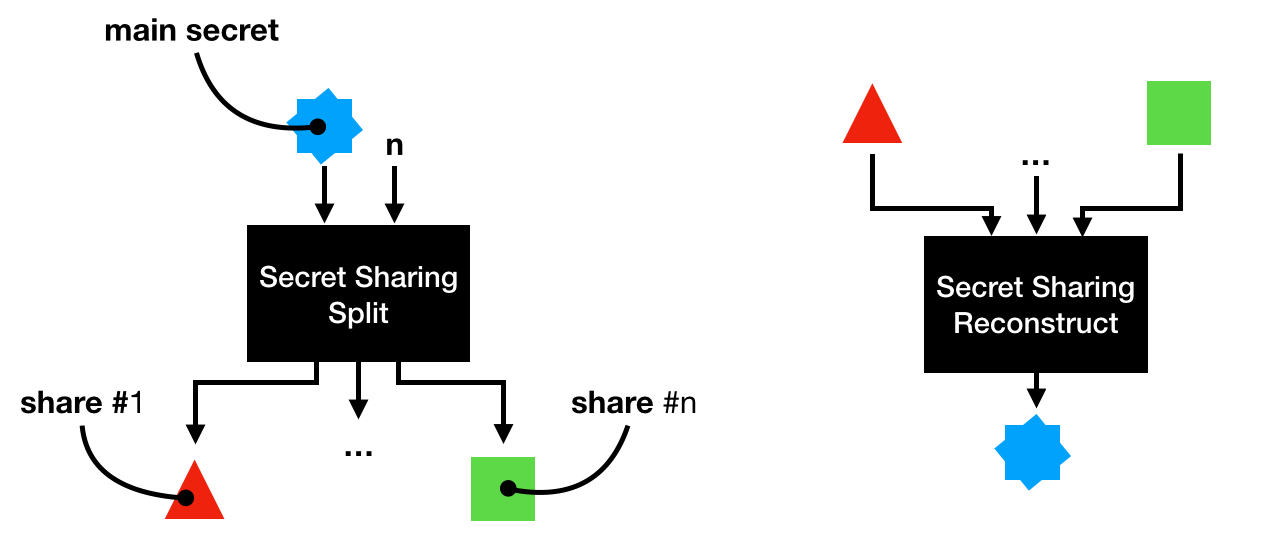
Shamir Secret Sharing Algorithm

Overview: Shamir Secret sharing algorithm is an efficient secret sharing algorithm for distributing private information among a group so that the secret cannot be revealed unless a minimum number of people act together to pool their knowledge. To reconstruct the message secured by SSS a number of shares is needed. If the shares are below that threshold than no information can be gained with those shares. It is impossible for the attacker to reconstruct that secret.

Shamir Secret Sharing algorithm has many useful properties which include.

1. It has information -theoretic security.
2. The size of piece does not exceed the size of data.
3. For any given threshold shares can be added or deleted without affecting the existing shares.
4. Security can be enhanced without changing the secret but by changing the polynomial occasionally and constructing a new share for each participant.
5. It is also possible to share the keys depending upon the importance of the person in the hierarchy .For instance, with a *threshold* of 3, the president could unlock the safe alone if given three shares, while three secretaries with one share each must combine their shares to unlock the safe.

Schematic Diagram :



Class Diagram:

