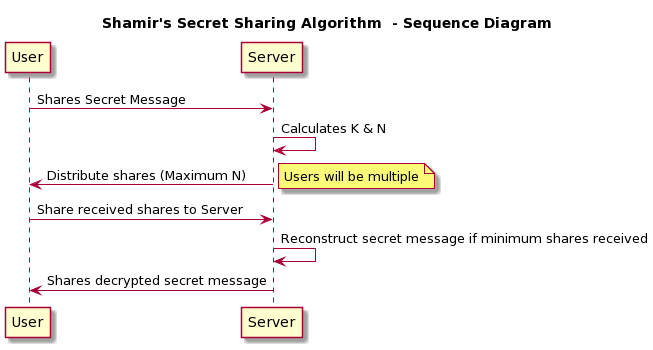
**Shamir’s Secret Sharing Design Document**

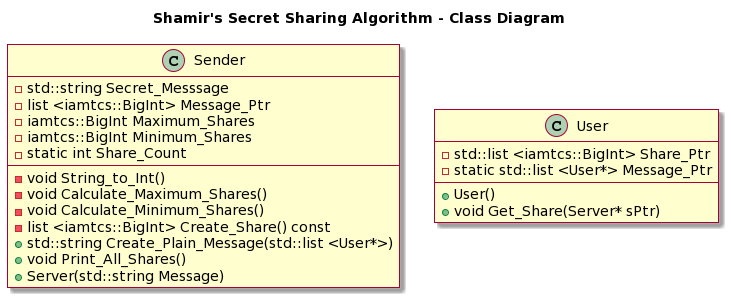
* Shamir’s Secret Sharing is an algorithm in cryptography created by Adi Shamir.
* The main aim of this algorithm is to divide secret into various unique parts.
* The main idea behind the Shamir’s Secret Sharing Algorithm lies behind the concept that for the given K points we can find a polynomial equation with the degree (K – 1)..
* In this first Server receives a Secret Message for encryption then it decides the minimum number of shares to reconstruct(K) and number of shares to distribute(N).
* After creating shares it distributes them to User and to decrypt if User shares required number of shares(K) then Server decrypts the Secret Message.

**Sequence Diagram for Shamir's Secret Sharing Algorithm**

****

**Fig 1.1**

**Class Diagram for Shamir's Secret Sharing Algorithm**

****

**Fig 1.2**