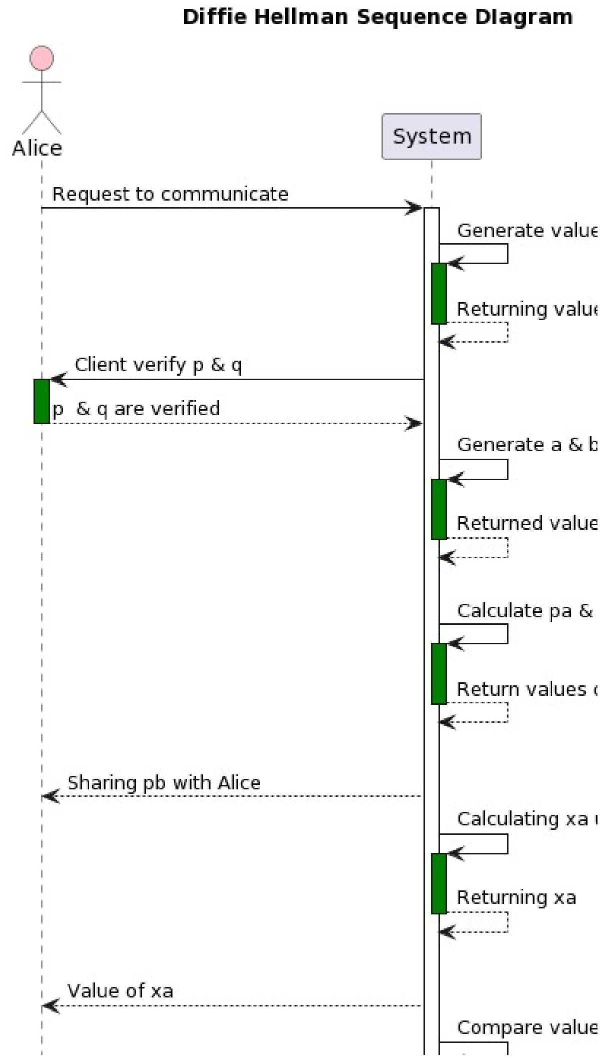
DIFFI HELLMAN

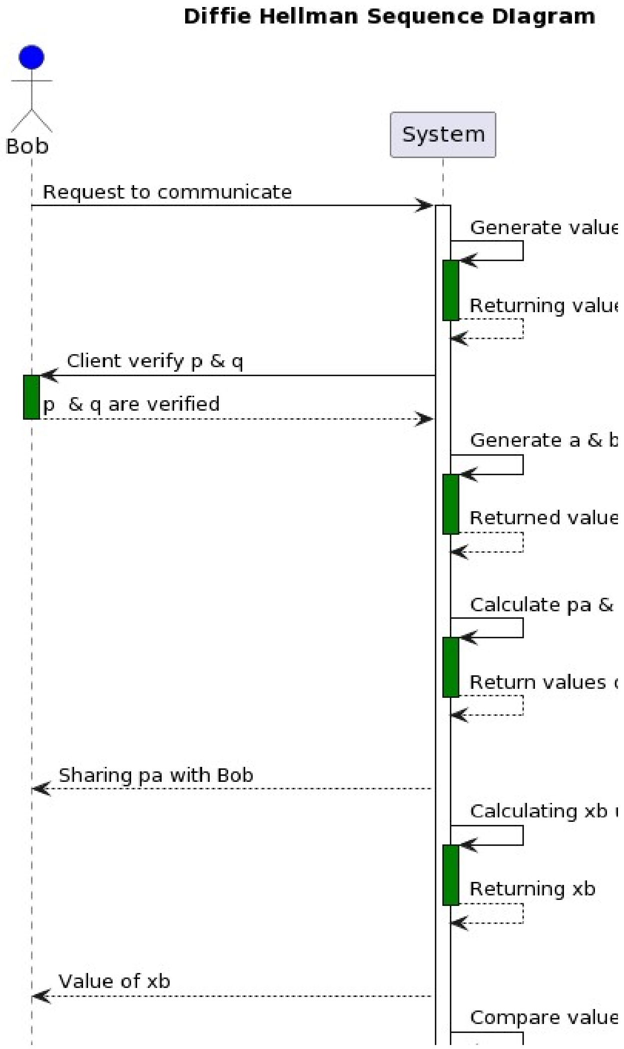
Overview:

Diffi Hellman is a algorithm to exchange keys thus granting a secure connection between client and client or client and server. This algorithm is based on Elliptic Curve Cryptography. When used by clients for example if Alice wants to interact with Bob then she can use this algorithm which will create secret keys, clients can use these secret keys generated to encrypt data and share it. To generate a secret key both parties do not need any prior knowledge of each other.

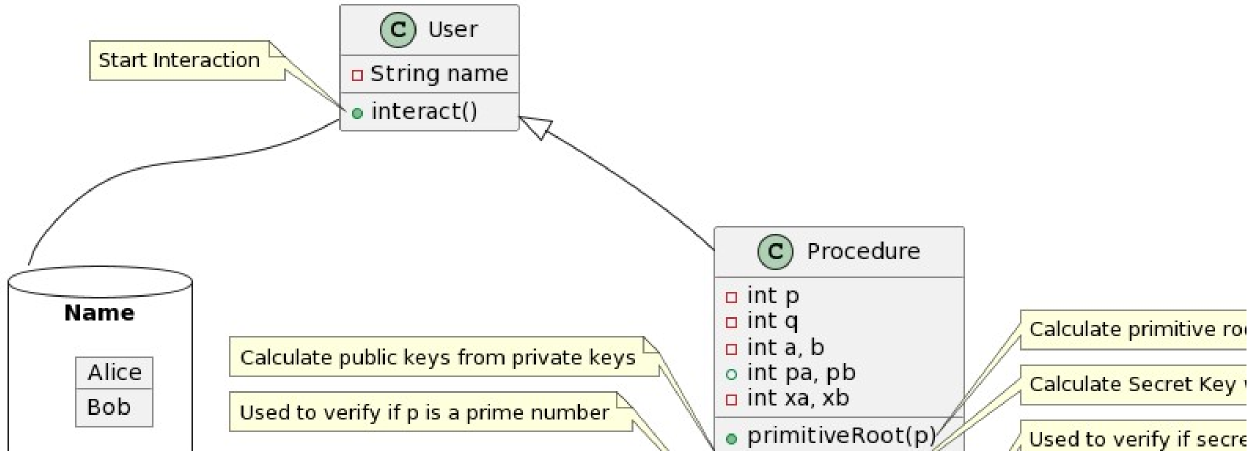
Sequence Diagram:

Bob:





Class Diagram:



Goals:

To understand the working of Diffie Hellman and get familiar with such algorithms so that I can understand the basics to implement cryptography.