BLOCKCHAIN

RAJYALAKSHMI.A

106124096

Shamir’s Secret Sharing Scheme:

This scheme basically employs two concepts:

1)Formation of a polynomial of degree one less than the wanted shares, with secret to be shared as constant in the polynomial.

2)Finding the constant from a few points using Lagrange interpolation formula.

To note: we use mod function with a larger prime or at the least case secret should be less than prime. Larger prime ensures finite field and increases security of secret.

Let’s go through the program in python step by step:

1. Take inputs from user like secret, prime, number of shares, threshold shares. Also we’ll find a prime greater than given secret using a function we defined.
2. We are defining two functions: one to form the polynomial, another one using lagrange interpolation to find the secret by finding f(0) in the function. It is necessary that k should be one more than the degree of the polynomial and n can be any number greater than k. Larger the k, implies more security. n doesn’t have any implication on security.
3. Then the values that are taken as input are used and we get a polynomial whose coefficients are chosen using random module, the shares or points, threshold shares, secret after lagrange interpolation.

The python file is attached along.