CS222

LAB ASSIGNMENT - 3

➔ In the main function, a variable exit status is set to 0.

➔ While the exit status remains 0, the loop runs.

- ◆ If the user enters 1, the CONFIGURE module, the user gets to select from three options - add a new entry, delete an existing entry or return.
  - If the user selects to add a new entry, he is asked to enter the locker_id.
  - If the locker_id doesn't exist, the user has to enter the k - number of users and L - locker key.
    - To check, if the locker_id exists - searchEntry function is called which opens the configure.txt file
    - Using the get line function to read from file, each line is stored as a string and using a string stream, the locker_id and the validity status are checked and the prime numbers are returned if it exists and is a valid entry else an empty vector is returned.
  - Then the CONFIGURE function is called, which generates the secondary keys by doing L modulo a prime number for each prime number in the generated prime numbers list (secondary_keys[i] = L modulo prime[i]) and the locker_id, valid status, k and prime numbers are entered in the configure.txt file.

- The prime numbers are generated in the generatePrimes function which also calls isPrime function to check if a number is rime

and getPrimeProduct function to get the product of the primes.

    - The first k - 1 prime numbers are generated from the beginning and if the product of the generated k - 1 prime numbers and square root of L is greater than L, then the k^{th} prime number is square root of L.

    - Else to find the k^{th} prime number, check for the product of generated prime numbers and L / 2, if it doesn't exceed L, then check for the next prime number after L / 2 until the condition is satisfied.

- Else if the locker_id exists, that entry cannot be added.

- If the user selects to delete an existing entry, checks if the locker-id exists and is valid.(checking is done through searchEntry function as explained above)
- If it exists, that entry is marked invalid.

    - To delete an entry, the deleteEntry function is called which opens the text file, reads the entire file line wise into a string, while reading the file, when the line with locker_id is found, the position of "VALID" is found using find function and it is replaced with "INVALID" using replace function.
    - The read line is now added to a string and the string is later written into the configure.txt file.

- When the user selects to return nothing is done and the process starts again.

- If the user enters 2, the USE module - the user is prompted to enter the locker_id
  - If the locker_id exists, the user is prompted to enter k, number of users and the secondary keys, u_i's.
  - Then the Use function is called and the locker access code is displayed on screen.
    - In the USE function:
    - getX function is called which returns a vector consisting of the product of primes divided by the prime number at the position in the vector of prime numbers. (X[i] = prime product / prime[i])
    - The getCoefficients function is called which uses the gcdExtended function which follows the extended euclidean algorithm and gives coefficients for two numbers such that $c_1x + c_1y = 1$. All the coefficients are generated using this gcdExtended function and by multiplying the previously generated coefficients with the recently generated coefficient of X.
    - To generate the locker key, L is added with the product of each of coefficients[i], secondary_keys[i] and X[i] and modulo with the product of the generated primes.
- If the user enters 3, the EXIT module, the variable exit status is changed to 1 and the loop breaks ending the program.

The code seems to work well for k = 7 and a 8 digit Locker key value(99999999) and also for k = 8 for small L value

Long long int(ll) and unsigned long long int(ull) are used to prevent any integer overflow errors.

Challa Sruthi

2003111

CSE