Final Year B. Tech, Sem VII 2022-23
PRN – 2020BTECS00211
Name – Aashita Narendra Gupta
Cryptography And Network Security Lab
Batch: B4
Practical No – 14

Title: Implementation of Chinese Remainder Theorem.

Theory:
Chinese Remainder Theorem states that there always exists an x that satisfies given congruences.
Let num[0], num[1], …num[k-1] be positive integers that are pairwise coprime. Then, for any given sequence of integers rem[0], rem[1], … rem[k-1], there exists an integer x solving the following system of simultaneous congruences.

$$\begin{cases} x \equiv rem[0] & (\text{mod } num[0]) \\ \quad \cdots & \\ x \equiv rem[k-1] & (\text{mod } num[k-1]) \end{cases}$$

Furthermore, all solutions x of this system are congruent modulo the product, prod = num[0] * num[1] * ... * nun[k-1]. Hence

$$x \equiv y \ (\text{mod } num[i]), \quad 0 \leq i \leq k-1 \quad \Longleftrightarrow \quad x \equiv y \ (\text{mod } prod).$$

The first part is clear that there exists an x. The second part basically states that all solutions (including the minimum one) produce the same remainder when divided by-product of num[0], num[1], .. num[k-1]. In the above example, the product is 3*4*5 = 60. And 11 is one solution, other solutions are 71, 131, .. etc. All these solutions produce the same remainder when divided by 60, i.e., they are of form 11 + m*60 where m >= 0.
A Naive Approach to find x is to start with 1 and one by one increment it and check if dividing it with given elements in num[] produces corresponding remainders in rem[]. Once we find such an x, we return it.

Example:

```
Input:  num[] = {5, 7}, rem[] = {1, 3}
Output: 31
Explanation:
31 is the smallest number such that:
  (1) When we divide it by 5, we get remainder 1.
  (2) When we divide it by 7, we get remainder 3.

Input:  num[] = {3, 4, 5}, rem[] = {2, 3, 1}
Output: 11
Explanation:
11 is the smallest number such that:
  (1) When we divide it by 3, we get remainder 2.
  (2) When we divide it by 4, we get remainder 3.
  (3) When we divide it by 5, we get remainder 1.
```

Code Snapshots:

```cpp
#include <bits/stdc++.h>
using namespace std;


// Function for extended Euclidean Algorithm
int ansS, ansT;
int findGcdExtended(int r1, int r2, int s1, int s2, int t1, int t2)
{
    // Base Case
    if (r2 == 0)
    {
        ansS = s1;
        ansT = t1;
        return r1;
    }

    int q = r1 / r2;
    int r = r1 % r2;

    int s = s1 - q * s2;
    int t = t1 - q * t2;

    cout << q << " " << r1 << " " << r2 << " " << r << " " << s1 << " " << s2
<< " " << s << " " << t1 << " " << t2 << " " << t << endl;

    return findGcdExtended(r2, r, s2, s, t2, t);
}
```

```cpp
int modInverse(int A, int M)
{
    int x, y;
    int g = findGcdExtended(A, M, 1, 0, 0, 1);
    if (g != 1) {
        cout << "Inverse doesn't exist";
        return 0;
    }
    else {

        // m is added to handle negative x


        int res = (ansS % M + M) % M;
        cout << "inverse is " << res << endl;
        return res;
    }
}



int findX(vector<int> num, vector<int> rem, int k)
{
    // Compute product of all numbers
    int prod = 1;
    for (int i = 0; i < k; i++)
        prod *= num[i];

    // Initialize result
    int result = 0;

    // Apply above formula
    for (int i = 0; i < k; i++) {
        int pp = prod / num[i];
        result += rem[i] * modInverse(pp, num[i]) * pp;
    }

    return result % prod;
}



int main()
{

    // 3
    // 3 4 5
```

```
    // 2 3 1
cout<<"Enter value of k: ";
    int k;
    cin >> k;

    vector<int> num(k), rem(k);
    cout<<"Value of numbers: ";
    for (int i = 0; i < k; i++)
        cin >> num[i];
    cout<<"Value of Remainders: ";
    for (int i = 0; i < k; i++)
        cin >> rem[i];

    int x = findX(num, rem, k);
    cout << "\nx is " << x;


    return 0;
}
```

Output Snapshots:

Conclusion:

1. The Chinese Remainder Theorem determines a number n that when divided by some given divisors give some remainders.
2. In conclusion, with the help of the Chinese Remainder Theorem, the only knowledge to guide with two remaining secret messages to get what we desire is the solution of the form: $142 + (143 \times i)$.
3. It can further be concluded that the Chinese Remainder Theorem has a lot of uses in our everyday life activities.