Practical no: 6B

Name: Saloni Vishwakarma
Batch-Roll no: C1-13
Subject: Cryptography Lab
Date of execution: 16 June 2023

Aim: Implement the following methods to support cryptography algorithms.
b) Fermat's little theorem for Multiplicative Inverse

b) Fermat's little theorem for Multiplicative Inverse (Code and Output):

```
#include <stdio.h>
// Function to calculate (a^b) % m using modular exponentiation
int powerMod(int a, int b, int m)
{
   int result = 1;
   a = a % m;
   while (b > 0)
   {
      if (b & 1)
      result = (result * a) % m;
      b = b >> 1;
      a = (a * a) % m;
   }
   return result;
}

// Function to calculate the multiplicative inverse of a modulo p
int calculateInverse(int a, int p)
{
   return powerMod(a, p - 2, p);
}

int main() {
  int a, p;
  printf("\n Enter the number whose inverse is to be found (a): ");
  scanf("%d", &a);
  printf("\n Enter the prime modulo (p): ");
```

```
    scanf("%d", &p);

    // Check if p is prime
    int i, isPrime = 1;
    for (i = 2; i * i <= p; i++)
    {
        if (p % i == 0) {
        isPrime = 0;
        break;
        }
    }
    if (!isPrime)
    {
        printf("%d is not a prime number.\n", p);
        return 0;
    }
    if (a % p == 0)
    {
        printf("\n The number %d does not have an inverse modulo %d\n", a, p);
    }
    else
    {
         int inverse = calculateInverse(a, p);
         printf("\n The multiplicative inverse of %d modulo %d is: %d\n", a, p,inverse);
    }
    return 0;
}
```

```
Enter the number whose inverse is to be found (a): 98

Enter the prime modulo (p): 47

The multiplicative inverse of 98 modulo 47 is: 12


...Program finished with exit code 0
Press ENTER to exit console.
```

```
Enter the number whose inverse is to be found (a): 60

Enter the prime modulo (p): 101

The multiplicative inverse of 60 modulo 101 is: 32


...Program finished with exit code 0
Press ENTER to exit console.
```

Conclusion: We have successfully studied and implemented Fermat's Little theorem for multiplicative inverse which supports the algorithms used in cryptography in C.