Visvesvaraya National Institute of Technology, Nagpur

System and Network Security – CSL443 (Practicals)

1. Verify whether GMP Library is already installed:

open the terminal by mouse right click and select.

Type the Command: gcc -o prg prg.cpp -lgmp

if error contains “gmp unknown or no file found” then it means “gmp” need to be install.

2. Installation of GMP package in Ubuntu

Command: sudo apt-get install libgmp3-dev

2.1 For installation in windows: (better to use ubuntu)

VScode, msys/mingw, gmp

https://code.visualstudio.com/docs/cpp/config-mingw

https://www.msys2.org/

https://packages.msys2.org/package/mingw-w64-x86_64-gmp

3. Download the latest manual for gmp package

Search “gmp manual pdf” on Google
It is at website - https://gmplib.org/

4. Download the pdf version of “Handbook of Applied Cryptography”

Search “Handbook of Applied Cryptography PDF” on google, Author: Alfred Menezes and download it.

Program 1 – To print default initialized gmp integer value

```
#include<gmp.h>
main() {
	mpq_t x;
	mpq_init(x);

	gmp_printf("Hello world, the default value initialized is :
%Zd\n", x);
}
```

Compile the gcd.c prog using the command: gcc -o gcd gcd.c -lgmp

Execute the output file: ./gcd

Program 2 – Multiplication of two large numbers

```
#include<gmp.h>
#include<stdio.h>
```

```
main () {
      mpz_t m, n;
      mpz_init(m);
      mpz_init(n);

      printf("Enter the first number\n");
      gmp_scanf("%Zd",m);

      printf("\nEnter the second number\n");
      gmp_scanf("%Zd",n);

      mpz_mul(m, m, n); //calling predefined function
      gmp_printf("\nThe multiplication of the two numbers is :
\n%Zd\n", m);
}
```

Note: In gmp the input can be a large integer, can be more than 20 digits.

Program 3 – Compute Factorial of a given integer

```
main () {
      mpz_t num,facto;
      mpz_inits(facto, num);
      unsigned long int u;

      printf("\nEnter the number :\n");
      gmp_scanf("%Zd",num);

      u=mpz_get_ui(num);
      printf("\n The number entered is : %lu", u);

      mpz_fac_ui(facto, mpz_get_ui(num));
      gmp_printf("\nThe factorial is :\n %Zd\n", facto);
      }
```

Program 4 – Generate 10 random integers of given bit length

- use function - mpz_urandomb (random, rstate, n)// see gmp manual section #

Program 5 – Generate n random prime numbers of given bit length

- search gmp manual of the appropriate function

Program 6 - Implement Euclidean Algorithm to find the GCD of two large numbers

-Refer: Algorithm 2.104 from Handbook of Applied Cryptography

use appropriate functions from gmp manual

Program 7 – Extended Euclidean Algorithm

Visvesvaraya National Institute of Technology, Nagpur

System and Network Security – CSL443 (Practicals)

-Refer: Algorithm 2.107 from Handbook of Applied Cryptography