INTRODUCTION TO CRYPTOGRAPHY – PROJECT 1

B.Tech. Computer Science and Engineering (Cybersecurity)

Name: Anish Sudhan Nair	Roll No.: K041
Batch: K2/A2	Date of performance: 25/12/2021

Code:

Language: C

Editor: VSCode

Compiler: clang/ZSH

```c
#include <stdio.h>

void main()
{
  int arr1[7],u,v, temp_u1,temp_u2,temp_u3;

  printf("Enter the greater number: ");
  scanf("%d", &u);

  printf("Enter the lesser number: ");
  scanf("%d", &v);

  arr1[0]=1;
  arr1[1]=0;
  arr1[2]=0;
  arr1[3]=1;
  arr1[4]=u;
  arr1[5]=v;
  arr1[6]=0;

  for (int i=0;i<7;i++)
      printf("%d\t", arr1[i]);
    printf("\n");

  while (arr1[5]!=0)
  {
```

```
    arr1[6]=arr1[4]/arr1[5];
    temp_u1=arr1[1];
    temp_u2=arr1[3];
    temp_u3=arr1[5];
    arr1[1]=arr1[0]-(arr1[6]*arr1[1]);
    arr1[3]=arr1[2]-(arr1[6]*arr1[3]);
    arr1[5]=arr1[4]-(arr1[6]*arr1[5]);
    arr1[0]=temp_u1;
    arr1[2]=temp_u2;
    arr1[4]=temp_u3;
    for (int i=0;i<7;i++)
       printf("%d\t", arr1[i]);
    printf("\n");
  }


}
```

Test Cases:

a) 28056, 3032
b) 48432, 47376

Output:

```
(base) anish@Anishs-MacBook-Pro Theory % clang gcd.c -o gcd
gcd.c:3:1: warning: return type of 'main' is not 'int' [-Wmain-return-type]
void main()
^
gcd.c:3:1: note: change return type to 'int'
void main()
^~~~
int
1 warning generated.
(base) anish@Anishs-MacBook-Pro Theory % ./gcd
Enter the greater number: 28056
Enter the lesser number: 3032
1       0       0       1       28056   3032    0
0       1       1       -9      3032    768     9
1       -3      -9      28      768     728     3
-3      4       28      -37     728     40      1
4       -75     -37     694     40      8       18
-75     379     694     -3507   8       0       5
(base) anish@Anishs-MacBook-Pro Theory % ./u
Enter the greater number: ^C
(base) anish@Anishs-MacBook-Pro Theory % ./gcd
Enter the greater number: 48432
Enter the lesser number: 47376
1       0       0       1       48432   47376   0
0       1       1       -1      47376   1056    1
1       -44     -1      45      1056    912     44
-44     45      45      -46     912     144     1
45      -314    -46     321     144     48      6
-314    987     321     -1009   48      0       3
(base) anish@Anishs-MacBook-Pro Theory %
```