R.V. COLLEGE OF ENGINEERING
OBSERVATION / DATA SHEET

Date 11-1-21 Name SHUVAM MITRA

Dept./Lab NPS Class CSE 5C Expt./No. 8

Title Lab Internal 1RV18CS165

8) Encrypt and decrypt using RSA and exchange key securely using diffie-hellman key exchange protocol.

//RSA

```
#include <stdio.h>
#include <math.h>
#include <stdlib.h>
#include <string.h>

long int gcd(long int a, long int b)
{  if(a==0)
        return b;
   if(b==0)
        return a;
   return (gcd(b, a%b));
}

long int isprime(long int a)
{ int i;
  for(i=2; i<a; i++)
  {  if(a%i==0)
        return 0;
  }
```

Signature of Teacher incharge

```
    return i;
}
long int encrypt (long int ch, long int n, long int e)
{   long int i, temp = ch;
    for (i=1; i<e ; i++)
        temp = (temp * ch) %. n;
    return temp;
}
long int decrypt (long int ch, long int n, long int d)
{   long int i, temp = ch;
    for (i= 1; i < d ; i++)
        temp = (temp * ch) %. n ;
    return temp;
}
int main ()
{ long int i, p, q, n, phi, e, d, cipher [50];
  int len;
  char text [50];
  printf (" enter text to be encrypted : \n");
  scanf ("%.5", text);
  len = strlen (text);
  do { p = rand () %. 30;
     } while ( ! isprime (p));
  do { q = rand () %. 30
     } while (! isprime (q));
```

R.V. COLLEGE OF ENGINEERING
OBSERVATION / DATA SHEET

Date _____ Name _____

Dept./Lab _____ Class _____ Expt./No. _____

Title _____

```
n = p*q ;
phi = (p-1) * (q-1);
do { e = rand() % phi ;
   } while ( gcd (phi, e) != 1);
do { d = rand() % phi;
   } while (((d*e) % phi) != 1);
printf ("2 prime no's are : %ld and %ld \n", p, q);
printf (p, q, p*q);
printf (phi);
printf ("PU = (n, e) : (%ld, %ld) \n" , n, e);
printf ("PR = (n, d) : (%ld, %ld) \n", n, d);
printf ("encrypted message");
for (i = 0; i < len; i++)
{ cipher [i] = encrypt ( text [i], n, e);
   printf ("%ld", cipher [i]);
}
```

Signature of
Teacher incharge

```
printf("decrypted message")
for(i=0; i<len ; i++)
{  text[i] = decrypt( cipher[i] , n, d);
    printf("%c", text[i]);
}
 return 0;
}
```

R.V. COLLEGE OF ENGINEERING
OBSERVATION / DATA SHEET

Date _____ Name _____

Dept./Lab _____ Class _____ Expt./No. _____

Title _____

// Diffie Hellman

```
#include <stdio.h>
#include <math.h>
long long int power(long long int a, long long int b, long long int p)
{ if(b==1)
    return a;
  else
    return((long long int) pow(a,b)%p);
}
int main()
{ long long int P, G, x, a, y, b, ka, kb;
  scanf("%lld", P)
  scanf("%lld", G)
  scanf("%lld", a)
  scanf("%lld", b)
  x = power(G, a, P);
  y = power(G, b, P);
```

Signature of
Teacher incharge

```
    ka = power(y, a, P);
    kb = power(x, b, P);
    printf("Secret info/key for Alice is %.lld \n", ka);
    printf("Secret info/key for Bob is %.lld \n", kb);
    return 0;
}
```