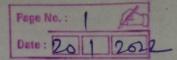
Lab-05



AIM:- Write a Program to implement

Knupsack Courto System:

Key Generation, Encryption, De Esyption.

code:-

include & bits / stdc+t:h>

include & "functions.h" # hus function like

Entended Gullidian

Unsigned long long mine;

vectore Mty generate Super Increasing Array (Mtsize)

Vector<mt> commy(size);

Gray[6] = 1+ rund().1.5;

Srund(0); 11 to reintruize rund(),

corruy[1] = corruy[0] + (1+rund().1.5);

Int next Num = corruy[0] + corruy[i]

for (int i=2; 12 size; t+i)

{

Srand(time(0));

corrug(i] = next Num +1;

next yum += corrug(i];

return array;

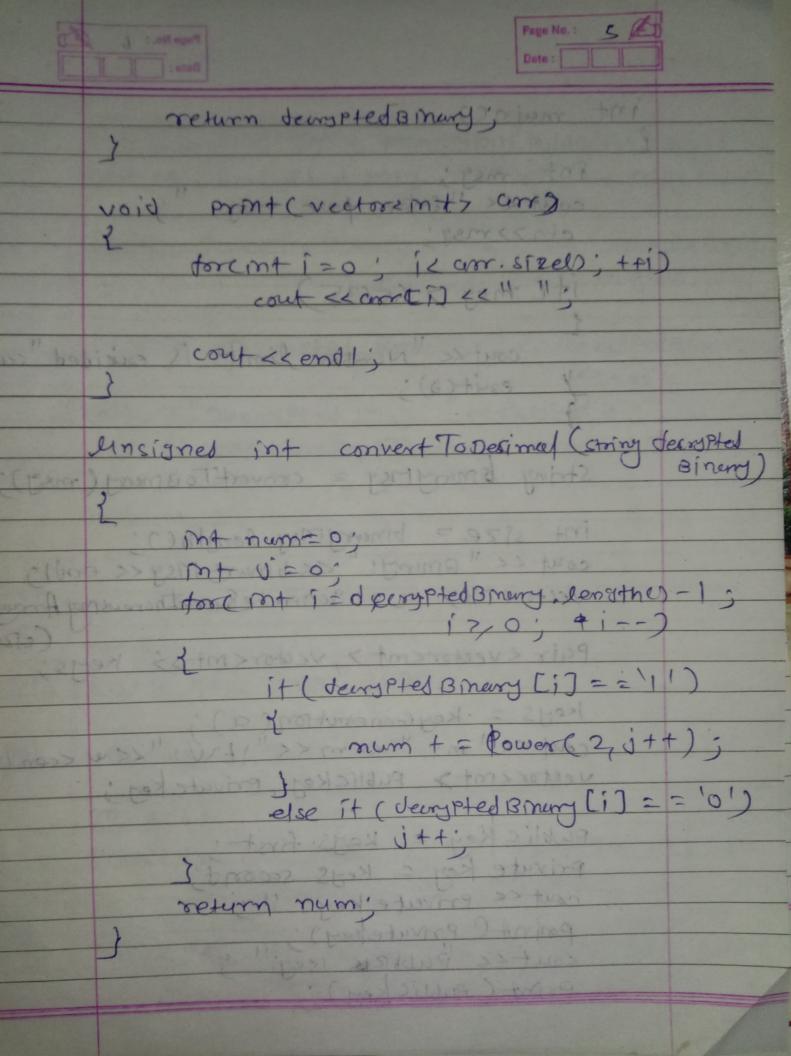
string convert To Binary (int msy) bitset < 167 bingry Num (msg).
string temp, binery = ""; temps binary Num, to stringer; Il remove exstru zero trom 16 bit num
Inti forcest i=0; (< temp, length(); ++i) it (temp[i] = = 1 1) breuk; brung = temp, substr(i, temp length()); power (nt num, int pou) m+ (Pow = = 0) seturn (num + power num, pou -1)); Paire vector (mt), vector (mt) Key Generation (vector < int > -a) replant of 1051 to med sensition m = acoumulate (-a. besines, -a. ender, o 1 +(rund () 1/ m)] freetorsinty ac-assize(); forcint i=p; i<m, ++i)} 17 (gcd Usmy EEA (i, m) = = 1) forcint (=0; iz -a. size; ++i) - (wx _a[i]) -/. m; return make-Pair(a, -a);

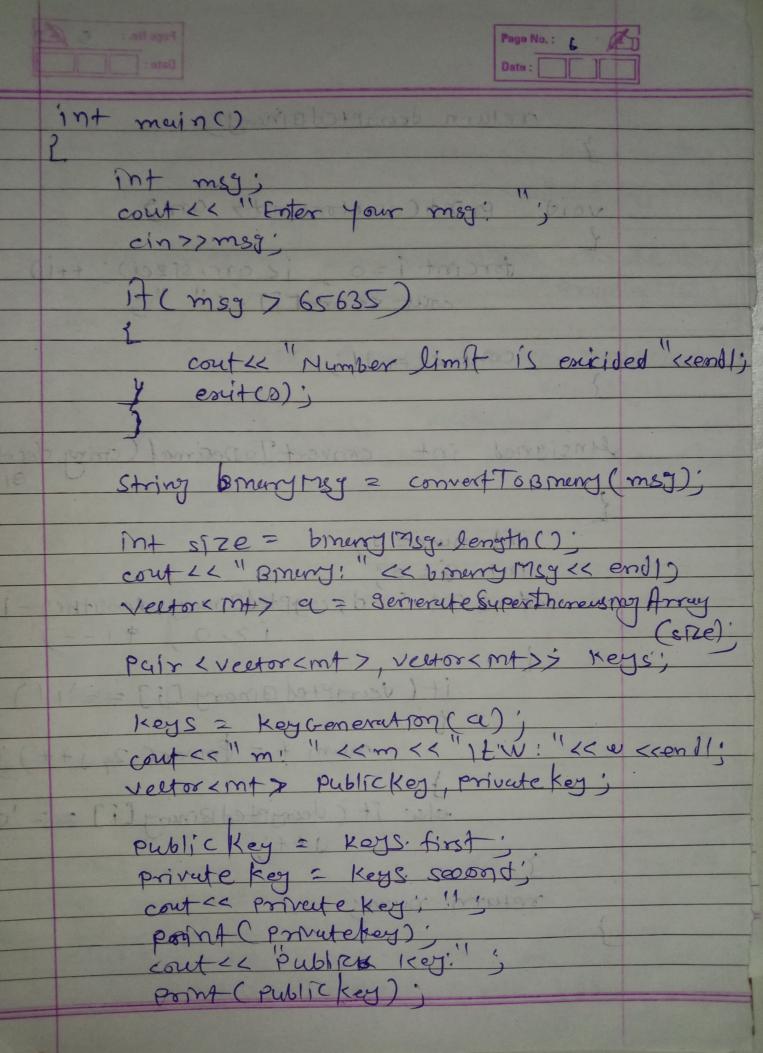
Page No.: 4

```
Int encryption (veltor (mt > key, String msy)
     unsigned int encrypted Mag = 0.
     tor (mt 120; 1 < msg.length (); + fi)
       17 (msci] == 11)
              encrypted Msgf = key[i];
    neturn enorypted msg;
Strong deery ptron ( vectors mt) key int encoryptesting)
     mt sym = 12th multipliative there (w, m) &
                    energeted Msg ) .m.
    cont «'sum: " << sum << end!;

cher teerypted Binerry [key. size() +1);

decrypted 13 inury [key. size()] = 10';
  forcint 1 = keysizer) -1, 1750; --
         if (sum > = Key Ci])
                decrypted Binary [] = ')';
sum = = Key[];
            else
                 deery Pted Binury [i] = 101:
```





int encrypted Msg = encryption (publicker, binerythis); cout << "Encrypted rasg: " << encryted rasg < enoly

String de-crypted Browny = derrypton (private Key, encypted MSS);

Contex "Decrypted Brown: "xcdecrypted Brown" < decrypted Brown: "xcdecrypted Brown"

cont << "Descripted Insy: " to Destined o
</ convert Deciment Tobanery (decripted Binery) '
</ end 1's

return 0;

5

m: Enter your msg: 3425

out: Binary: 110101100001

m: 6144 w:5

Private key: 236 12 24 48 96 192 384 768 1536 3072

Publica Key: 10 15 30 60 120 240 480 960

Encrypted may: 3877

Sum: 3233

Decrypted Brung: 110101100001

Decrypted msg: 3425:

sempling code: -

1000011010111 penaid 13

Private key 2 2 2 12 24 48 9

ENDIFFERENT 10 15 SO GO 120 240 END