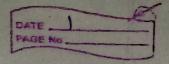
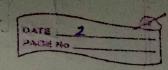
· Lab-07



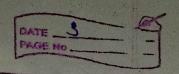
Aim: - Write a Program to implement Flgament cryptosystem. -> +n too primitive poots and Muli Group -) Key Generation -> Encyption -> Decryption code:-# melude "function.h" struct key2 int a, e, Pid; vectorint 7 find Group Zp (int P) forcint i=0; ix P; ++i) it (medtiplicative Inverse (i, p) =+1) ZP. Push\_buck (1); octum zp;



int find Primitive Root ( int Prime) int a; vector < m+> group Zp & = find group Zp (prime). forcintj=0; il groupzp. size(); ++vi) a= groupzp [j]; for (int i=2; i <= (prime-1); ++i) int m = squerre And Multiply (a, i, prime); i+( i==(prime-1) \* ( m==1) retim a; else if cm==1 break; Key generate Key () int prime;

Key Keys; while (1)

couter "Enter ed-a large Prime number"



it (is Prime (Immer))

break;

veltor<mt> groupZp = findGroup Zp(prime));

koys.e, = fmdprimt(veltoot (prime);

int K=0;

while (group ZPCKT K=1 Vt group [K] 7 (prime-2))

Kogs.d = groupzp[K];

Koys. ez = squerrefind Myltiply (Koys.ei, Koys.d pmm) kers.p = prime,

return kegs:

Pair < mt, mt) energetion (int msg, inter, interint

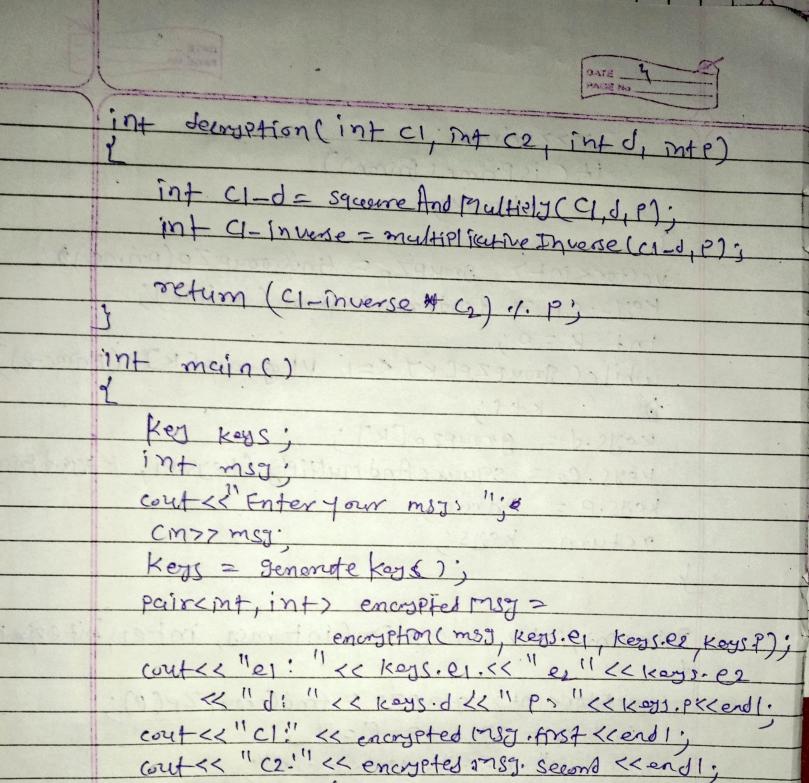
vettor<mt> groupzp = fmdGroupzp(p);

contex" | no: " < < r < cend!

int c1 = squeene And Multiply (e1, o, p);

int c2 = ((msg 7.P) # square And Multiply (e2, r, P))-6

return make-Pair (c1, c2);



cout < < decription (enworted msg. first) encyptul msg. sangkers d, Kos p) return o: output Input v: 3 Friter your msg = 1234 Enter prime number: 3497

e1:2, e2=2, d=1, p;3499 C1=8, C2=2874 Decrypted m89: 1234