Date: 3-11-22 Experiment No. 3 Suppose Alice worts, hor friends to enveyet email messayes before sending them to here white a perogram to help here briends to enought and descript the duto (RSA algorithm) # include < stdip . h> # include < stable, h> # include < moth. h> # include < string . h> long int god Clony int a, long int b setwin ac, setwin gcd (b, a.1.b); long int isprime (long int a) for (i= 2; i < a; i++) if ((a+i)==0) return 1; long int enought Cehar ih, long int n, long inte Page No. MALNAD COLLEGE OF ENGINEERING, HASSAN

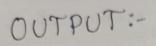
Date: 3-11-22 Experiment No. 3 for (i=1; i <e; i++)

timp = (timp = h) 1. n;

return timp; shove deveypt (long int ih, long int n, long int d) int is long int time = ih; for (i=1; i<d; i++) ih = (ih = timp) 1-n; int p, q, n, phi, e, d, eighen [so]; print f ("Entire text to be energypted:");

Egets (text, 50, stoin); In = steller (text); p=rand()-1.30; while(! in prume (P)); Page No. MALNAD COLLEGE OF ENGINEERING, HASSAN

Date: 3-11-22 Experiment No. 3 8 = scond () 1. Phi; 3 while (gcd (phi, e) !=1); 1 23 3 while (((d * e).1. phi)!=1 d = 2 cand () -1. phi; while (((d = e) -1. phi 111166 "Two prime num ova: 1.1d and "n= (p*q) = 1 wate key (n,e) (-1.1 "1.1d", lipher [i]; ought Cupher [i] n.d); i < los; i++); vint ["1.c" text [i] iturin O Page No. MALNAD COLLEGE OF ENGINEERING, HASSAN



. 1 a. out

Enter text to be enveypted: Punya

Two preime numbers (P and q) lare: 13 and 23

N = (P+q) = 13 × 23 = 299

(P-1)*(0x-1) = 264

(P-1)*(0x-1) = 264

(P-1)*(0x-1) = 264

Private key (n,e) (299, 103)

Pablic key (n,e) (299, 223)

Pablic key (n,d) (299, 223)

Enveypted message: 982251111841326824811613 nng

Drugpted message: Panya.