Program24 C program for RSA system,

#include <stdio.h>

int gcd(int a, int b) {

if (b == 0)

return a;

return gcd(b, a % b);

}

int extendedGCD(int a, int b, int \*x, int \*y) {

if (b == 0) {

\*x = 1;

\*y = 0;

return a;

}

int x1, y1;

int gcd = extendedGCD(b, a % b, &x1, &y1);

\*x = y1;

\*y = x1 - (a / b) \* y1;

return gcd;

}

int modInverse(int a, int m) {

int x, y;

int gcd = extendedGCD(a, m, &x, &y);

if (gcd != 1) {

printf("Inverse does not exist.\n");

return -1;

}

int result = (x % m + m) % m;

return result;

}

int main() {

int e = 31;

int n = 3599;

int p, q;

for (p = 2; p <= n; p++) {

if (n % p == 0) {

q = n / p;

break;

}

}

int phi\_n = (p - 1) \* (q - 1);

int d = modInverse(e, phi\_n);

printf("Private key d: %d\n", d);

return 0;

}

OUTPUT:

Private Key (d): 3031