24. Write a C program for RSA system, the public key of a given user is e = 31, n = 3599. What is the private key of this user? Hint: First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo f(n).

#include <stdio.h>

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

if (a == 0) {

\*x = 0;

\*y = 1;

return b;

}

int x1, y1;

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

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

\*y = x1;

return gcd;

}

int modInverse(int e, int phi) {

int x, y;

int g = gcdExtended(e, phi, &x, &y);

if (g != 1)

return -1;

else

return (x % phi + phi) % phi;

}

int main() {

int e = 31;

int n = 3599;

int p = 59, q = 61;

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

int d = modInverse(e, phi);

printf("Public Key (e, n): (%d, %d)\n", e, n);

printf("p = %d, q = %d\n", p, q);

printf("φ(n) = %d\n", phi);

printf("Private Key d = %d\n", d);

return 0;

}

Output

