25. Write a C program for set of blocks encoded with the RSA algorithm and we don’t have the private key. Assume n = pq, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way?

#include <stdio.h>

int gcd(int a, int b) {

while (b != 0) {

int temp = b;

b = a % b;

a = temp;

}

return a;

}

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 n = 3599;

int e = 31;

int known\_plaintext = 122;

int factor = gcd(known\_plaintext, n);

if (factor == 1 || factor == n) {

printf("No useful factor found.\n");

return 0;

}

int p = factor;

int q = n / p;

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

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

int d = modInverse(e, phi);

printf("φ(n) = %d\n", phi);

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

return 0;

}

OUTPUT:

