Homework5

1.Pick two small primes p, q. Calculate n=pq.

P = 5 q = 7

n = p q = 5 7 = 35

2. Start from n to find p and p independently by using the Shor algorithm.

N = 35, a = 2, f(k) = mod N

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| k | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| F(k) | 1 | 2 | 4 | 8 | 16 | 32 | 29 | 23 | 11 | 22 | 9 | 18 | 1 | 2 | 4 | 8 | 16 | 32 | 29 | 23 | 11 |

r = 12 is even, and 35 doesn’t divide by + 1 which is 65 or – 1 which is 63

p = gcd( – 1,35) = gcd(63,35) = 7

Q = gcd( + 1,35) = gcd(65,35) = 5