Homework5

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

P = 5 q = 5

n = p q = 5 5 = 25

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

N = 25, 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 | 7 | 14 | 3 | 6 | 12 | 24 | 23 | 21 | 17 | 9 | 18 | 11 | 22 | 19 | 13 | 1 |

r = 20 is even, and 25 divides 1025, hence, we need to pick a different a

N = 25, a =3, 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 | 3 | 9 | 2 | 6 | 18 | 4 | 12 | 11 | 8 | 24 | 22 | 16 | 23 | 19 | 7 | 21 | 13 | 14 | 17 | 1 |

r = 20 is even, and 25 divides  + 1 hence, we need to pick a different a

N = 25, a =7, 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 | 7 | 24 | 18 | 1 | 7 | 24 | 18 | 1 | 7 | 24 | 18 | 1 | 7 | 24 | 18 | 1 | 7 | 24 | 18 | 1 |

r = 4 is even, and 25 divides + 1, hence, we need to pick a different a

N = 25, a =9, 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 | 9 | 6 | 4 | 11 | 24 | 16 | 19 | 21 | 14 | 1 | 9 | 6 | 4 | 11 | 24 | 16 | 18 | 11 | 0 | 18 |

R = 10 is even, and 25 divides + 1 which is 59049 + 1 = 59050