Cryptography: HW6

Trevor Bramwell

Professor Mike Rosulek
March 5, 2015

1

2

3a Given an RSA modulus N and $\phi(N)$, it is possible to factor N easily without computing d or finding a non-trivial square root of unity.

To start with, we know:

$$\begin{aligned} N &= pq \\ \phi(N) &= (p-1)(q-1) \end{aligned}$$

Factoring $(p-1)(q-1)$ and doing some algebra, we arrive at:

$$N - \phi(N) + 1 = q + p$$

This allows us to now use the quadratic equation:

$$(x-q)(x-p) = 0$$

and find roots equal to q and p. Factoring we have:

$$\begin{aligned} (x-q)(x-p) &= x^2 - qx - px + pq \\ &= x^2 + (-q-p)x + pq \end{aligned}$$

This provides us with the quadractic equations constants:

$$
\begin{aligned}
a &= 1 \\
b &= (-q - p) \\
-b &= (q + p) \\
c &= pq = N
\end{aligned}
$$

Which when plugged into the quadratic equation, give us:

$$p, q = \frac{(q + p) \pm \sqrt{(-q - p)^2 - 4N}}{2}$$

3b The prime factors (p, q) of N are:

```
p =
10506334523061610465734801363429770178600654212894190908310118588883281398192754
15784491038859906064060912154239886412322904143688606612352349055162088314100023
95649542617648887800946357680235133745987328106517234870888931439344639465469
3557226572538703470381806340282069971496180947616992507650491611580103 33
```

```
q =
93524195713675969769392792891804134476995933511802171872806533613894125318127028
91792282763505995136608679026507582290903916195465065737145139940492408335268162
35957699648688337327410429196529474184107065919242793511757586398184746028719
1342833560356018485176253542816589237713501814110266911435430483265167
```