RSA Encryption Lecture 3 Example

Thai Nguyen *CITS3004 Sem2 2020*

Given $p = 5$ and $q = 11$ find the public key $\{e, n\}$ and private key $\{d, n\}$.

1. $n = p \times q = 55$
   - This is the modulus used in the public and private keys.
2. $\varphi(n) = (p-1) \times (q-1) = 40$
   - φ is Euler's Totient Function.
3. Choose $e = 13$
   - e can be any integer that is relatively prime to $\varphi(n)$ where $1 < e < \varphi(n)$
   - Any e where $gcd(40, e) = 1$
   - When choosing e it's easiest to start with prime numbers $< \varphi(n)$
   - This way you just need to check factors for $\varphi(n)$ not the prime since it has none other than 1 and itself.
   - For 40, 3 will work but 5 won't for example.
   - If you're able to choose, picking a small number will make things easier in later steps.
4. Find d such that $13d \bmod 40 = 1$
   - $ed \bmod \varphi(n) = 1$
   - Finding d is finding the (modular) multiplicative inverse.
   - In the lecture slides this is shown as $13d \equiv 1 \bmod 40$
   - First we perform GCD until we get a remainder of 1 with this example we get it straight away leaving us with:
     - $40 = 13 \times 3 + 1$
   - Next we use the extended euclidean algorithm
     - We rewrite the above equation in terms of 1, giving:
     - $1 = 40 - 3 \times 13$
     - We want the equation in terms of 40 and 13 as well, so we substitute to reach this, however with this example no substitution is required.
     - We just need to look at the number that is multiplying 13 which is -3 in this case.
     - $(13 \times -3) \bmod 40 = 1$ which matches up, however for RSA we need it to a positive integer.
     - Knowing that it's $\bmod 40$ we can simply do $-3 + 40 = 37$ to get d.
     - You can keep adding 40 to keep getting more d s.
     - $37, 77, 117, etc$ all work as private keys but keep it small to compute it more easily.
5. Therefore we have all the values for the keys, public key $\{13, 55\}$ and private key $\{37, 55\}$.