RSA Cryptosystem

- Choose two large prime numbers p and q
- Set $n = pq$.
- The private key is any number k between 1 and n which is coprime with $(p-1)(q-1)$ (for example, we could choose k to be prime); this means that $\text{hcf}(k, (p-1)(q-1)) = 1$.
- By Euclid's algorithm, there are integers a and b such that

  $$ak + b(p-1)(q-1) = 1. \quad (1)$$

  We can assume that $0 < a < (p-1)(q-1)$.
- The pair of numbers (a, n) forms the public key.

RSA Encryption and Decryption

- Suppose that we have an integer M in the range 0 to $n-1$.
- To encrypt M we apply the encryption function e

$$e(M) = M^a \bmod n. \tag{2}$$

  This clearly only requires knowledge of the public key.
- We can decrypt a message C using the private key k:

$$d(C) = (C)^k \bmod n. \tag{3}$$

RSA Example I

- Take $p = 3$ and $q = 5$, so that $n = 15$ and we require k coprime to $(p-1)(q-1) = 2 \times 4 = 8$. Because n is so small, it is easy to factorise, so this algorithm is not secure. Let us choose the private key $k = 3$ (which is actually prime).
- Using Euclid's algorithm we find that

$$3k - 1 \times 8 = 1$$

  so $a = 3$ and the public key is $(3, 15)$. Note that in this case, the private and the public key are the same. This is a coincidence, and does not alter the security of the algorithm.
- A number M between 0 and 15 is encrypted as $M^3 \bmod 15$. For example, if $M = 2$ this is $2^3 \bmod 15 = 8$.
- We decrypt this by computing $8^3 \bmod 15$. $8^2 = 64 = 4 \bmod 15$ and $8^3 = 4 \times 8 = 32 = 2 \bmod 15$.

RSA Example I

- Take $p = 11$ and $q = 13$, so that $n = 143$ and we require k coprime to $(p-1)(q-1) = 10 \times 12 = 120$. Because n is so small, it is easy to factorise, so this algorithm is not secure. Let us choose the private key $k = 11$ (which is actually prime).
- Using Euclid's algorithm we find that

$$11k - 1 \times 120 = 1$$

  so $a = 11$ and the public key is $(11, 143)$. Note that in this case, the private and the public key are the same. This is a coincidence, and does not alter the security of the algorithm.
- A number M between 0 and 143 is encrypted as $M^{11} \bmod 143$.

Efficient Computation of Modular Powers

To compute $L = M^k$:

1. Write k as a binary number with d bits; the most significant bit is 1. We number the bits from most to least significant.

$$a = b_1 \ldots b_d \tag{4}$$

2. Compute $L = M^2$. Set the index $i = 2$.
3. If $b_i = 1$, let $L := L \times M$.
4. If $i < d$, let $L := L^2$, $i := i + 1$ and go to step 3.

Suppose that we want to compute M^{11}. The binary representation of 11 is 1011, which requires 4 bits. So we calculate

$$\begin{array}{cccccc} b_1 & b_2 & & b_3 & b_4 & \\ M \rightarrow & M^2 \rightarrow & M^4 \rightarrow & M^5 \rightarrow & M^{10} \rightarrow & M^{11} \end{array}$$

Now let us encrypt $M = 2$ with the public key $(11, 143)$.

$$2 \to 2^2 \to 2^4 = 16 \to 2^5 = 32$$

$$\to 2^{10} = 1024 = 23 \bmod 143$$

$$\to 2^{11} = 2 \times 23 = 46 \bmod 143.$$

So $e(2) = 46$. As a test, let us decrypt $C = 46$ with the private key 11.

$$46 \to 46^2 = 2116 = 114 \bmod 143$$

$$\to 46^4 = 114^2 = 12996 = 126 \bmod 143$$

$$\to 46^5 = 46 \times 126 = 5796 = 76 \bmod 143$$

$$\to 46^{10} = 76^2 = 5776 = 56 \bmod 143$$

$$\to 46^{11} = 56 \times 46 = 2576 = 2 \bmod 143.$$

So $d(46) = 2$, as expected.