18. RSA

Here we give a short explanation of how to use number theory to send encoded messages.

Two people, Alice and Bob, would like to send each other secret messages. Suppose that Bob wants to send Alice a secret message.

At the start Alice picks two prime numbers p and q, typically with lots of digits, and she computes the product $n = pq$. Note that the group of units U_n modulo n has order

$$\begin{aligned}\varphi(n) &= \varphi(pq) \\ &= \varphi(p)\varphi(q) \\ &= \varphi(p)\varphi(q) \\ &= (p-1)(q-1).\end{aligned}$$

Alice then picks a number e between 1 and $\varphi(n)$ which is a unit modulo $\varphi(n)$, that is, a number coprime to $(p-1)(q-1)$. Suppose that d is the inverse modulo $\varphi(n)$, so that

$$de \equiv 1 \mod \varphi(n),$$

so that there is an integer k with the property that

$$de = 1 + k\varphi(n).$$

e is public knowledge but d is kept secret. Alice sends Bob both e and the number n.

If Bob wants to send Alice a message then Bob encodes his message as a single number $1 \leq a \leq n$, coprime to n, that is, neither a multiple of p nor q. He then computes

$$b = a^e \mod n.$$

He sends Alice the encrypted message b. To decode b, Alice computes

$$\begin{aligned}b^d &= (a^e)^d \mod n \\ &= a^{de} \\ &= a^{1+k\varphi(n)} \\ &= a + a^{k\varphi(n)} \\ &= a \cdot (a^{\varphi(n)})^k \\ &= a \cdot 1^k \mod n \\ &= a.\end{aligned}$$

The security of RSA relies on the fact that it is relatively easy to pick prime numbers p and q with lots of digits but it is relatively hard

to factor n, which has roughly twice the number of digits as p and q. Note that

$$\varphi(n) = n - p - q - 1,$$

so knowing $\varphi(n)$ is practically equivalent to knowing p and q.

Here is a simple example to illustrate these methods. Suppose that Alice picks $p = 61$ and $q = 53$. In this case

$$n = 61 \cdot 53 = 3233.$$

Then

$$\begin{aligned} \varphi(3233) &= (61-1)(53-1) \\ &= 60 \cdot 52 \\ &= 3120. \end{aligned}$$

Pick $e = 17$. We want to find the multiplicative inverse d of e modulo 3120. We use the Euclidean algorithm to solve the linear Diophantine equation

$$17x + 3120y = 1.$$

We have

$$\begin{aligned} 3120 &= 183 \cdot 17 + 9 \\ 17 &= 1 \cdot 9 + 8 \\ 9 &= 1 \cdot 8 + 1. \end{aligned}$$

Going backwards we get

$$\begin{aligned} 1 &= 9 - 8 \\ &= 9 - (17 - 9) \\ &= 2 \cdot 9 - 17 \\ &= 2 \cdot (3120 - 183 \cdot 17) - 17 \\ &= 2 \cdot 3120 - 367 \cdot 17. \end{aligned}$$

Therefore we should take $x = -367$ and $y = 2$. It follows that

$$\begin{aligned} d &= 3120 - 367 \\ &= 2753. \end{aligned}$$

Suppose that the message is $a = 123$. Bob has to compute 123^{17}. For this, one can use the trick of computing repeated squares. Note that

$$\begin{aligned} 17 &= 16 + 1 \\ &= 2^4 + 1. \end{aligned}$$

So we have to square 123 four times and then multiply by 123. This gives

$$\begin{aligned}(123)^2 &= 15129\\ &= 2197 \mod 3233.\end{aligned}$$

Therefore

$$\begin{aligned}(123)^4 &= (2197)^2\\ &= 4826809\\ &= 3173 \mod 3233.\end{aligned}$$

It follows that

$$\begin{aligned}(123)^8 &= (2197)^4\\ &= (3173)^2\\ &= 10067929\\ &= 367 \mod 3233.\end{aligned}$$

Finally, then

$$\begin{aligned}(123)^{16} &= (2197)^8\\ &= (3173)^4\\ &= (367)^2\\ &= 134689\\ &= 2136 \mod 3233.\end{aligned}$$

Hence

$$\begin{aligned}(123)^{17} &= 123 \cdot (2197)^{16}\\ &= 123 \cdot 2136 \mod 3233\\ &= 262728\\ &= 855.\end{aligned}$$

Alice decodes 855 by raising it to the power $d = 2753$ to get 123.