CCSE RSA cheatsheet

Nicholas Miehlbradt

October 2022

1 Generating Keys

Choose two prime numbers p and p. Keep these secret!

Calculate $n = p \times q$

Calculate $\phi(n) = (p-1) \times (q-1)$

Choose e such that $1 \leq e \leq \phi(n)$ and is co-prime with $\phi(n)$

Find d such that $e \times d = 1 \equiv mod\ \phi(n)$

Your public key is (e, n) and your private key is (d, n)

$\phi(n)$ is Euler's totient function. $\phi(n)$ is equal to the number of positive integers less than n which are co-prime to n.

2 Encrypting

To encrypt a message m convert it to a number (e.g. using ASCII) and make sure that it is less than n.
The encrypted message $c = m^e\ mod\ n$

Using properties of modular exponents we can calculate this without the numbers getting too big.

3 Decryption

To decrypt a message $m = c^d\ mod\ n$

4 Breaking RSA

If you know someone's public key, to get their private key you need to factorize n. This is a hard problem that cannot in general be computed quickly. Once you have the factors p and q you can calculate d using the algorithm above.
This isn't the only way to break RSA, but it is the most general.