RSA - generating the key pair

1. Pick $\mathbf{p}$ and $\mathbf{q}$ two large prime numbers and calculate $\mathbf{n = p \,.\, q}$ (see primality tests)
2. Compute $\mathbf{z = (p\text{-}1).(q\text{-}1)}$
3. Pick a prime number $\mathbf{e < z}$ such that $\mathbf{e}$ and $\mathbf{z}$ are relative primes

➡ (e,n) is the **public key**

4. Solve the linear equation $\mathbf{e * d = 1\ (\ mod\ z\ )}$ to find $\mathbf{d}$

➡ (d,n) is the **private key**
however p and q must be kept secret too

RSA - encryption and decryption

Given $\mathbf{Kp = (e, n)}$ and $\mathbf{Ks = (d,n)}$

➡ Encryption : $\mathbf{E_{kp}(m) = m^e \bmod n = c}$

➡ Decryption : $\mathbf{D_{ks}(c) = c^d \bmod n = m}$

➡ **$\mathbf{(m^e)^d \bmod n = (m^d)^e \bmod n = m}$**