RSA

Key generation

1. Select two prime numbers $p, q, p < q < 2p, p = O(2^{1024})$
2. Compute $n = p * q, \phi(n) = (p-1) * (q-1)$
3. Select e such that $gcd(e, \phi(n)) = 1$. Practice $e = 2^{16} + 1$
4. Compute d such that $ed \equiv 1 \mod \phi(n)$

Public key: (e, n) Private key: d

Encryption

$c \equiv m^e \mod n$

Decryption

$m \equiv c^d \mod n$

Why does it work?

$c^d \mod n \equiv (m^e)^d \mod n \equiv m^{ed} \mod n$

$ed \equiv 1 \mod \phi(n) \Rightarrow ed = k\phi(n) + 1$

$c^d \mod n \equiv m^{ed} \mod n \equiv m^{k\phi(n)+1} \mod n$

$\equiv m * m^{k\phi(n)} \mod n \equiv m * (m^{\phi(n)})^k \mod n$

$m * 1^k \mod n \equiv m$

$3^{12} = \left(3^2\right)^6 = \left(\left(3^2\right)^2\right)^3$

$\lim_{x \to +\infty} \frac{\pi(x)}{\frac{x}{lnx}} = 1$

For large numbers $\pi(x) \approx \frac{x}{lnx}$

What is the probability of x being a prime number?

$\frac{\pi(x)}{x} = \frac{\frac{x}{lnx}}{x} = \frac{\frac{x}{lnx}}{\frac{x}{1}} = \frac{x}{xlnx} = \frac{1}{lnx}$

What is the probability of a random number with 1024 bits being a prime number?

$\frac{1}{ln2^{1024}} = \frac{1}{1024ln2} \approx \frac{1}{1024}$