<u>**R**</u>ivest, <u>**S**</u>hamir, <u>**A**</u>dleman

asymmetric cryptography

Basics

- Designers: Ron Rivest, Adi Shamir, Leonard Adleman
- First published: 1977
- Key sizes: 1024 to 4096 bit typical
- Rounds: 1
- Utilization: asymmetric cryptography, digital signature, https

Why is this safe ?

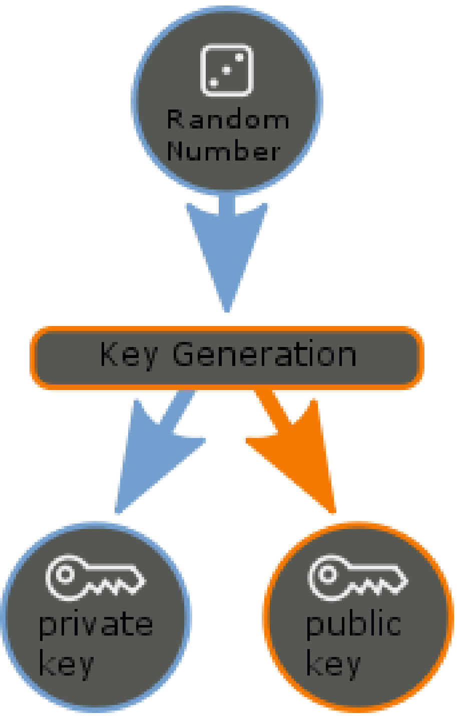
- RSA is based on the practical difficulty of factoring the product of two large prime numbers

- m^e mod n = c → encryption one-way function, m being the message as number

- ?^e mod n = c ← hard to calculate m again

- c^d mod n = m ← decryption

Key generation



1. Choose two distinct prime numbers p and q.
   - p != q

2. Compute $N = p * q$.

3. Compute $\varphi(N) = \varphi(p) * \varphi(q) = (p – 1) * (q – 1)$
   - Where φ() is Euler‘s totient function

4. Choose an integer e such that $1 < e < \varphi(N)$ and e is coprime to φ(N)
   - e is released as the public key exponent

5. Determine (inverse of d) ≡ e (mod φ(N)) as the multiplicative inverse of e (modulo φ(N))
   - This is more clearly stated as: $d * e \equiv 1 \pmod{\varphi(N)}$
   - d is kept as the private key exponent

Encryption and decryption

- Encryption:
  - Mr. Bob send us his public key (N, e)
  - Encrypt the message m to miphertext c
    - $c \equiv m^e \pmod{N}$
    - Can be done quickly using the method of exponentiation by squaring
  - Send the ciphertext to Mr. Bob

- Decryption:
  - Mr. Bob can decrypt the ciphertext c with his private key (N, d)
    - $m \equiv c^d \pmod{N}$

Example

1. $p = 61$ and $q = 53$
2. $N = 61 * 53 = 3233$
3. $\varphi(3233) = (61-1)*(53-1) = 3120$
4. Choose any number $1 < e < 3120$ that is coprime to 3120
   - $e = 17$
5. Compute d, the modular multiplicative inverse of e (mod $\varphi(N)$)
   - $d = 2753$

- The public key is (N = 3233, e = 17)
- The private key is (N= 3233, d = 2753)

- $c = 65^{17} \bmod 3233 = 2790$
- $m = 2790^{2753} \bmod 3233 = 65$