

RSA - Rivest, Shamir and Alderman

| | |
|-------------------------|---|
| Key Size | 1024 - 4096 |
| Speed | <p>~ factor of 10^6 cycles / byte</p> <ul style="list-style-type: none">• Key generation: 10 - 100 ms• Encryption: 0.2 - 2 ms• Decryption: 5 - 10 ms |
| Mathematical Foundation | Prime number theory |

Number Theory - Prime numbers

Prime Numbers

- p is prime if 1 and p are its only divisors e.g 3, 5, 7, 11 ...
 - p and q are relatively prime (a.k.a. coprime) if $\gcd(p, q) = 1$
e.g $\gcd(4, 5) = 1$
- ➡ There are infinitely many primes

Euler-Fermat Theorem

If $n = p \cdot q$ and $z = (p-1) \cdot (q-1)$

and a such that a and n are relative primes

Then $a^z \equiv 1 \pmod{n}$