

RSA CRYPTOGRAPHY  
ARITHMETIC BACKGROUND

*Jim Borger*

**Introduction.**

- Traditional encryption
- RSA = Rivest, Shamir, Adleman

**Prime numbers.**

- No smaller factors besides 1
- Every number can be factored in to primes... and in only one way
- There are infinitely many primes (Euclid)
- ...but they become rarer and rarer

**Greatest common divisors (GCDs).**

- What is the  $\gcd(a, b)$ ?
- How do we compute it? Euclid's algorithm.
- Writing  $\gcd(a, b) = ax + by$

**Modular arithmetic.**

- The last digit of a number
- Important principle: you can ignore other digits anytime you want
- Remainders and reducing modulo  $n$
- Important principle, II: you can reduce modulo  $n$  anytime you want
- Examples
- Raising to a high exponents modulo  $n$
- Modular division

**Fermat's little theorem.**

- If  $p$  is prime,  $a^p - a \pmod p = 0$  for all  $a$ .
- If  $a$  is not a multiple of  $p$ , then  $a^{p-1} - 1 \pmod p = 0$ .
- Examples