Primes

A prime number p is a positive integer that has exactly 2 divisors, 1 and p.

Facts about primes:

- Every $n \in \mathbb{N}$ is the product of primes.
- Prime factorization is UNIQUE. (proof: read chap. 7) [Fundamental Theorem of arithmetics]
- $p \mid ab \Rightarrow p \mid a \vee p \mid b$
- $p \mid b \wedge p \nmid a \Rightarrow p \mid \frac{b}{a} \quad \left(\frac{b}{a} = k \in \mathbb{N}\right)$

- $p \mid ab \Rightarrow p \mid a \lor p \mid b$

Proof: $p \mid ab \Rightarrow ab = mp$

If we factor a and b into primes, p must show up by uniqueness of prime factorization.

$\Rightarrow p \mid a \lor p \mid b$

- $p \mid b \land p \nmid a \Rightarrow p \mid \frac{b}{a}$ $\left(\frac{b}{a} = k \in \mathbb{N}\right)$

proof: $\frac{b}{a} = k \Rightarrow p \mid ak \Rightarrow \underbrace{p \mid a}_{\text{false}} \lor p \mid k \Rightarrow p \mid k.$

- Some other properties can be found in chp. 7.

Fermat Theorem

p prime $\wedge$ $p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$

- $p \nmid a \Rightarrow \gcd(a,p) = 1$
- Consider set $\{1, 2, 3, \dots, p-1\}$

$\times a \pmod{p}$

... permute ... (because $\gcd(a,p)=1$)

[idea: $\gcd(a,p)=1$]

So, $a \cdot (2a) \cdot (3a) \cdot (4a) \cdots [(p-1)a] \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) = (p-1)!$

$$a^{p-1} \cdot \cancel{(p-1)!} \equiv \cancel{(p-1)!} \pmod{p}$$

- Now $(p-1)!$ and p are co-prime : $D_p = \{1, p\}$

  and $p \nmid (p-1)!$ because p can't divide any $x \in \{1, \dots, p-1\}$

  So $(p-1)!$ has an inverse mod p $\Rightarrow$ $a^{p-1} \equiv 1 \pmod{p}$

Strengthen:

$$p \text{ prime} \iff \forall a \in \{1,\dots,p-1\},\ a^{p-1} \equiv 1 \pmod{p}$$

Idea: To check if a number n is prime, make sure $a^{n-1} \equiv 1 \pmod{n}$ for all $a < n$.

Not better than checking $\{1, \dots, n-1\}$ for divisors!

But it turns out, it has good random behavior:

```
repeat 100 times
    - pick random a < n
    - if a^(n-1) ≢ 1 (mod n)
          return false      (n is composite)
return true.
```

Problem: n might be composite and we still return true because we did not pick the "good" a: $a^{n-1} \not\equiv 1 \bmod n$

For most composites, the probability of picking a "bad" a is $\leq \frac{1}{2}$ (see chp. 7). Therefore, the prob. of making wrong decision $\leq \left(\frac{1}{2}\right)^{100}$

Other Problems

- a^{n-1} requires $(n-1)$ multiplication
- a^{n-1} is HUGE !

Repeated Squaring:

$$a^b = \begin{cases} 1 & b=0 \\ a \cdot a^{b-1} & b \text{ odd} \\ \left[a^{b/2}\right]^2 & b \text{ even} \quad [\text{save mult.}] \end{cases}$$

Combine this with computing everything modulo n on the fly.

Example: $a = 2$, $n = 30$

Need to find $a^{n-1} = 2^{29}$

$$29 \quad 28 \quad 14 \quad 7 \quad 6 \quad 3 \quad 2 \quad 1 \quad \boxed{0}$$ Base case

$$\times \quad {}^{\wedge}2 \quad {}^{\wedge}2 \quad \times \quad {}^{\wedge}2 \quad \times \quad {}^{\wedge}2 \quad \times$$

$$64 \quad 8 \quad 4 \quad 2 \quad 1$$

$$64 \quad 8 \quad 4$$

$$32 \quad 16 \quad 4$$

$$2$$

$$\#\text{mult} \approx 2 \cdot \log_2 b$$

Cryptography

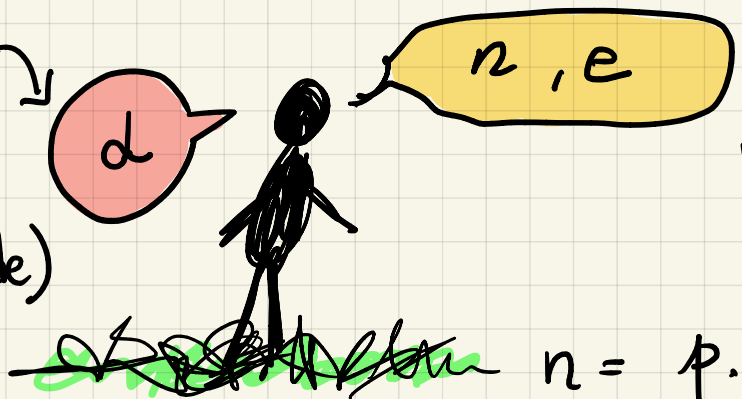
Assume every message is an integer $x < n$.

To send x to person A, send $x^e \bmod n$

where e and n are advertized by A

private key

(see next slide)



public key

$n = p \cdot q$ where p, q are large primes

Fact 1: It's hard to factor n into primes, so it's hard to discover p and q

Fact 2: Given $y = x^e \bmod n$, it's hard to figure out x.

Person A also has : $\gcd(e, (p-1)(q-1)) = 1$

so there exists d such that

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

d can be easily found by A (how?) but not by others.

claim : $y^d \bmod n = x$

$$y^d \equiv (x^e)^d \equiv x^{ed} \equiv x^{(p-1)(q-1)+1} \equiv x.(x^{q-1})^{p-1}$$

- $p \mid x \Rightarrow y^d \equiv x \equiv 0 \pmod{p}$
- $p \nmid x \Rightarrow p \nmid x^{q-1} \Rightarrow (x^{q-1})^{p-1} \equiv 1 \pmod{p}$ [Fermat]

  $\Rightarrow y^d \equiv x \pmod{p}$

$$y^d \equiv x \pmod{p} \Rightarrow p \mid y^d - x$$

$$y^d \equiv x \pmod{q} \Rightarrow q \mid y^d - x$$

$$\overline{\qquad\qquad\qquad\qquad}$$

$$n = pq \mid y^d - x$$ (p, q both prime factors)

Therefore $y^d \equiv x \pmod{pq}$

$$y^d \equiv x \pmod{n}$$

:)