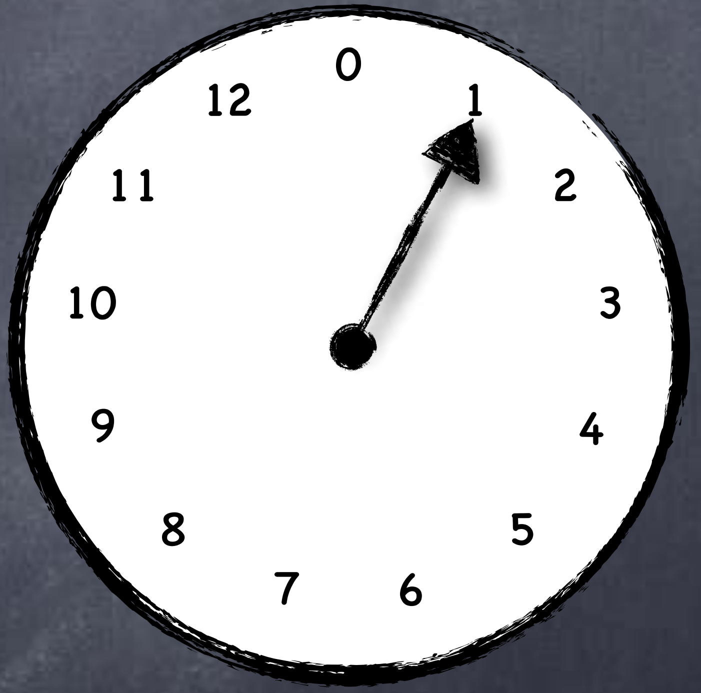
Numb3rs

Some Cryptographic Functions



A Word on Efficiency

- Very huge numbers have very short representation
- Take a 256 bit integer, $11\ldots1 = 2^{256}-1$
- Can a computer just count up to this number?
  - No. Not even if it runs
    - at the frequency of molecular vibrations (10^{14} Hz)
    - for the entire estimated lifetime of the universe ($< 10^{18}$ s)
- What if you recruited every atom in the earth ($\approx 10^{50}$) to do the same?
  - OK, but still will get only to $10^{82} \approx 2^{272}$.
  - And even if you recruited every elementary particle in the known universe ($\approx 10^{80}$), only up to $10^{112} \approx 2^{372}$
- **The whole known universe can't count up to a 400-bit number!**

A Word on Efficiency

- The whole known universe can't count up to a 400-bit number!
- But we can quickly add, multiply, divide and exponentiate much larger numbers. Even find gcd for them!
- Roughly, can "compute on" n-bit numbers in n or n^2 steps
  - But not if you try an algorithm based on counting through all the numbers! That takes 2^n steps. (e.g., exponentiation using naïve repeated multiplication)
- For some problems involving n-bit numbers we don't know algorithms that do much better than 2^n, $2^{n/2}$ etc.
  - We believe for some such problems no better algorithms exist!
  - (Currently, only a belief based on failure to discover better algorithms)
- Such hardness forms the basis of much of modern cryptography

Cryptography from $\mathbb{Z}_m^*$

- Trapdoor One-Way Permutation
  - Often a building block in “public-key encryption”
  - Roughly, it’s a bijection (permutation) that is easy to compute but hard to invert (one-way); but while defining the function you can setup a secret (trapdoor) that makes it easy to invert too
- Will see two trapdoor one-way permutation candidates, based on modular exponentiation
  - Rabin’s function
  - Rivest-Shamir-Adleman (RSA) function
- Both use a modulus of the form m=pq (p,q large primes)
  - Breaking would be easy if m were prime
  - Also can be broken (using CRT) if factors of m known.

Square-roots in $\mathbb{QR}_p^*$

Recall

- In $\mathbb{Z}_p^*$ $\sqrt{(x^2)} = \pm x$
- If $(p-1)/2$ odd, squaring is a permutation in $\mathbb{QR}_p^*$
- This permutation is easy to compute both ways
  - In fact $\sqrt{z} = z^{(p+1)/4} \in \mathbb{QR}_p^*$ (because $(p+1)/2$ even)

Say $z = x^2 \in \mathbb{QR}_p^*$.

$(z^{(p+1)/4})^2 = x^{(p+1)} = x^2$

- Rabin function defined in $\mathbb{QR}_m^*$ and relies on keeping the factorisation of m=pq hidden

Rabin Function

Trapdoor One-Way Permutation Candidate

- $\text{Rabin}_m(x) = x^2$ (in $\mathbb{QR}^*_m$)
  - with m=pq (p,q random k-bit primes for, say k=2000)
  - If p, q $\equiv$3 (mod 4), then in $\mathbb{QR}^*_m$ this function

    i.e., (p-1)/2 and (q-1)/2 are odd

    - Is a permutation
    - Has a trapdoor for inverting, namely (p,q)
      - By CRT: Let $x \mapsto (a,b)$. Then $\sqrt{x} \mapsto (\sqrt{a},\sqrt{b}) = (a^{(p+1)/4}, b^{(q+1)/4})$
  - Conjectured to be a one-way function

RSA Function

Trapdoor One-Way Permutation Candidate

- $RSA_{m,e}(x) = x^e$ (in $\mathbb{Z}_m$)
  - where m=pq (p,q random k-bit primes for, say k=2000) and
  - $\gcd(e,\phi(m)) = 1$ (i.e., $e \in \mathbb{Z}^*_{\phi(m)}$)
- A commonly used version (for efficiency) fixes e=3
- $RSA_{m,e}$ is a permutation with a trapdoor (namely d)
  - In fact, there exists d s.t. $RSA_{m,d}$ is the inverse of $RSA_{m,e}$
    - $d = e^{-1}$ in $\mathbb{Z}^*_{\phi(m)} \Rightarrow x^{ed} = x$ in $\mathbb{Z}_m$
    - For $x \in \mathbb{Z}^*_m$, by Euler's Totient Theorem $x^{ed-1} = 1$
    - For all $x \in \mathbb{Z}_m$, by CRT (since m=pq)
- Conjectured to be a one-way function