MA/CSSE 473 Day 10

Data Encryption

RSA

MA/CSSE 473 Day 10

- Solution to Yesterday's quiz
- Student questions?
- Next Session, come prepared to discuss the interview with Donald Knuth (linked from the schedule page, Session 11)
  - and Brute Force Algorithms
  - and amortization
- Today:
  - Cryptography Introduction
  - RSA

We'll only scratch the surface, but there is MA/CSSE 479

CRYPTOGRAPHY INTRODUCTION

Cryptography Scenario

- You want to transmit a message **m** to me
  - You encode the message and send it to me in a form **e**(**m**) that I can readily decode by running **d**(**e**(**m**)),
  - Hopefully, a form that an eavesdropper has little chance of decoding
- Private-key protocols
  - You and I meet beforehand and agree on **e** and **d**.
- Public-key protocols
  - I publish an **e** for which I know the **d**, but it is very difficult for someone else to guess the **d**.
  - Then you can use **e** to encode messages that only I* can decode

* and anyone else who can figure out what **d** is, based on e

Messages can be integers

- Since a message is a sequence of bits …
- We can consider the message to be a sequence of **b**-bit integers (where **b** is fairly large), and encode each of those integers.
- Here we focus on encoding and decoding a single integer.

RSA Public-key Cryptography

- Rivest-Shamir-Adleman (1977)
  - References : Weiss, Section 7.4
  - Dasgupta, Pages 33-34
- Consider a message to be an integer modulo **N**, which has **k** bits (longer messages can be broken up into **k**-bit pieces)
- The encryption function will be a bijection on {0, 1, …, **N**-1}, and the decryption function will be its inverse
- How to pick the **N** and the bijection?

bijection: a function **f** from a set **X** to a set **Y** with the property that for every **y** in **Y**, there is exactly one **x** in **X** such that **f**(**x**) = **y**. In other words, **f** is both one-to-one and onto.

N = p q

- Pick two large primes, **p** and **q**, and let **N** = **pq**.
- **Property**: If **e** is any number that is relatively prime to **N'** = (**p**-1)(**q**-1), then
  - the mapping $\mathbf{x} \rightarrow \mathbf{x}^{\mathbf{e}}$ mod **N** is a bijection on {0, 1, …, N-1}, and
  - If **d** is the inverse of **e** mod **N'**, then for all **x** in {0, 1, …, **N**-1}, $(\mathbf{x}^{\mathbf{e}})^{\mathbf{d}} \equiv \mathbf{x}$ (mod **N**).
- We'll first apply this property, then prove it.

Public and Private Keys

- The first (bijection) property tells us that $\mathbf{x} \rightarrow \mathbf{x}^{\mathbf{e}}$ mod **N** is a reasonable way to encode messages, since no information is lost
  - If you publish (**N**, **e**) as your *public key*, anyone can encode and send messages to you
- The second tells how to decrypt a message
  - When you receive an encoded message **m'**, you can decode it by calculating $(\mathbf{m}')^{\mathbf{d}}$ mod **N**.

Example (from Wikipedia)

- **p**=61, **q**=53. Compute **N** = **pq** = 3233
- **N'** = (**p**-1)(**q**-1) = 60·52 = 3120
- Choose **e**=17 (relatively prime to 3120)
- Compute multiplicative inverse of 17 (mod 3120)
  - Thus **d** = 2753 (evidence: 17·2753 = 46801 = 1 + 15·3120)
- To encrypt **m**=123, take 123^{17} (mod 3233) = 855
- To decrypt 855, take 855^{2753} (mod 3233) = 123
- In practice, we would use much larger numbers for **p** and **q**.
- On exams, smaller numbers ☺

Recap: RSA Public-key Cryptography

- Pick any two large primes, **p** and **q**, and let **N** = **pq**.
- Consider a message to be a number modulo **N**, a **k**-bit number (longer messages can be broken up into **k**-bit pieces)
- **Property**: If **e** is any number that is relatively prime to **N' =** (**p**-1)(**q**-1), then
  - the mapping $\mathbf{x} \rightarrow \mathbf{x}^{\mathbf{e}}$ mod **N** is a bijection on {0, 1, …, **N**-1}
  - If **d** is the inverse of **e** mod **N'**, then for all **x** in {0, 1, …, **N**-1}, $(\mathbf{x}^{\mathbf{e}})^{\mathbf{d}} \equiv \mathbf{x}$ (mod **N**)
- We have applied the property; we should prove it
- Modular arithmetic properties will be used heavily in the proof!

- Don't put the next three slides online before the class meeting.

Proof of the property

- **Property**: If **N**=**pq** for two primes **p** and **q**, and if e is any number that is relatively prime to **N'** = (**p**-1)(**q**-1), then
  - the mapping $\mathbf{x} \rightarrow \mathbf{x}^{\mathbf{e}}$ mod **N** is a bijection on {0, 1, …, **N**-1}
  - If d is the inverse of **e** mod **N'**, then for all **x** in {0, 1, …, **N**-1}, $(\mathbf{x}^{\mathbf{e}})^{\mathbf{d}} \equiv \mathbf{x}$ (mod **N**)
- The second conclusion implies the first, so we prove the second one.

Proof of the property part 2

- **Proving**: If **N**=**pq** for two primes **p** and **q,** and if **e** is any number that is relatively prime to
  N' = (**p**-1)(**q**-1), then
  - If **d** is the inverse of **e** mod **N'** then
    for all **x** in {0, 1, …, **N**-1}, $(\mathbf{x}^{\mathbf{e}})^{\mathbf{d}} \equiv \mathbf{x} \pmod{\mathbf{N}}$
- This is equivalent to $(\mathbf{x}^{\mathbf{e}})^{\mathbf{d}} - \mathbf{x} \equiv 0 \pmod{\mathbf{N}}$. We show this.
- **e** is invertible mod **N'**, because it is relatively prime to **N'**. Let **d** be **e**'s inverse
- **ed** ≡ 1 (mod (**p**-1)(**q**-1)), so there is an integer **k** such that **ed** = 1 + **k**(**p**-1)(**q**-1) **[we could find k using Euclid]**
- $\mathbf{x}^{\mathbf{ed}} - \mathbf{x} = \mathbf{x}^{1 + \mathbf{k}(\mathbf{p}-1)(\mathbf{q}-1)} - \mathbf{x}$.
  If we can show that
  $\mathbf{x}^{1 + \mathbf{k}(\mathbf{p}-1)(\mathbf{q}-1)} - \mathbf{x} \equiv 0 \pmod{\mathbf{N}}$,
  then we'll be done.

Proof of the property part 3

- **Left to show**: If **N**=**pq** for two primes **p** and q, and if **e** is any number that is relatively prime to **N'** = (**p**-1)(**q**-1), then
  - $\mathbf{x}^{1 + \mathbf{k}(\mathbf{p}-1)(\mathbf{q}-1)} - \mathbf{x} \equiv 0 \pmod{\mathbf{N}}$
- By Fermat's Little Theorem, $\mathbf{x}^{\mathbf{p}-1} \equiv 1 \pmod{\mathbf{p}}$
  - so any power of $\mathbf{x}^{\mathbf{p}-1}$ (in particular $\mathbf{x}^{\mathbf{k}(\mathbf{p}-1)(\mathbf{q}-1)}$) is congruent to 1 (mod **p**).
- Subtract 1 from both sides: $\mathbf{x}^{\mathbf{k}(\mathbf{p}-1)(\mathbf{q}-1)}-1$ is divisible by **p**.
- Multiply by **x**: $\mathbf{x}^{1+\mathbf{k}(\mathbf{p}-1)(\mathbf{q}-1)} - \mathbf{x}$ is divisible by **p**
- **q** is also prime, so $\mathbf{x}^{1+\mathbf{k}(\mathbf{p}-1)(\mathbf{q}-1)} - \mathbf{x}$ is divisible by **q**
- Since **p** and **q** are primes, anything divisible by both **p** and **q** is divisible by by **pq** = **N**.
- Conclusion: $(\mathbf{x}^{\mathbf{e}})^{\mathbf{d}} = \mathbf{x}^{\mathbf{ed}} = \mathbf{x}^{1+\mathbf{k}(\mathbf{p}-1)(\mathbf{q}-1)} \equiv \mathbf{x} \pmod{\mathbf{N}}$
- This is what we wanted to show.

RSA security

- **Assumption** (Factoring is hard!):
  - Given **N**, **e**, and $\mathbf{x}^{\mathbf{e}}$ mod **N**, it is computationally intractable to determine **x**
  - What would it take to determine **x**?
- Presumably this will always be true if we choose **N** large enough
- But people have found other ways to attack RSA, by gathering additional information
- So these days, more sophisticated techniques are needed.
- MA/CSSE 479

Student questions

- On primality testing, RSA or anything else?