Announcements and Review

- Homework 4 due next lecture
- Plan for today: Finish crypto discussion, talk about mathematical induction
- Review: Difference between private and public key crypto?
- Main problem with private key crypto?
- Most commonly used public key system is RSA; nice application of number theory!

RSA History

- Named after its inventors Rivest, Shamir, and Adleman, all researchers at MIT (1978)
- Actually, similar system invented earlier by British researcher Clifford Cocks, but classified – unknown until 90’s

RSA Overview

- Bob has two keys: public and private
- Everyone knows Bob’s public key, but only he knows his private key
- Alice encrypts message using Bob’s public key
- Bob decrypts message using private key
- Since public key cannot decrypt, no one can read message except Bob

High Level Math Behind RSA

- In the RSA system, private key consists of two very large prime numbers \( p, q \)
- Public key consists of a number \( n \), which is the product of \( p, q \) and another number \( e \), which is relatively prime with \( (p - 1)(q - 1) \) (\( \phi(n) \), Euler’s totient function)
- Encrypt messages using \( n, e \), but to decrypt, must know \( p, q \)
- In theory, can extract \( p, q \) from \( n \) using prime factorization, but this is intractable for very large numbers
- Security of RSA relies on inherent computational difficulty of prime factorization

Encryption in RSA

- To send message to Bob, Alice first represents message as a sequence of numbers
- Call this number representing message \( M \)
- Alice then uses Bob’s public key \( n, e \) to perform encryption as:
  \[
  C = M^e \pmod{n}
  \]
- \( C \) is called the ciphertext
Encryption Example

- Encrypt message "STOP" using RSA with $n = 2537$, $e = 13$
- First convert each letter to a number in $[0, 25]$: $S = 18$, $T = 19$, $O = 14$, $P = 15$
- Group sequence into blocks of 4 digits:

$$M = 1819 1415$$
- Now encrypt each block as $C = M^{13} \pmod{2537}$
- For first block, $1819^{13} \pmod{2537} = 2081$; for second block $1415^{13} \pmod{2537} = 2182$
- Ciphertext: $2081 2182$

Why Does RSA Work?

- To show that RSA works, we need to prove that the encryption and decryption function are inverses, i.e.,

$$M^{ed} \equiv M \pmod{\phi(n)}$$
- To prove this, we'll use Euler’s theorem ($a, n$ co-prime):

$$a^{\phi(n)} \equiv 1 \pmod{\phi(n)}$$
- Since $d$ is inverse of $e$ modulo $\phi(n)$, we have:

$$ed - 1 = k \cdot \phi(n)$$

Decryption Example

- Decrypt the cipher text $0981 0461$ for the RSA cipher with $p = 43$, $q = 59$, and $e = 13$.
- First we need to compute $d$, the inverse of $e$ modulo $(p - 1)(q - 1)$:

$$d \cdot e \equiv 1 \pmod{(p - 1)(q - 1)}$$
- As we saw earlier, $d$ can be computed reasonably efficiently if we know $(p - 1)(q - 1)$
- However, since adversaries do not know $p, q$, they cannot compute $d$ with reasonable computational effort!

Example, cont.

Decrypt $0981 0461$ using $p = 43$, $q = 59$, $n = 2537$, and $e = 13$.
- To solve $13x \equiv 1 \pmod{2436}$, computed $s = 937$, $t = -5$
- Recall: Solution to this system is given by:

$$x = \frac{sb + m \cdot d}{d} \pmod{n} \text{ where } u \in \mathbb{Z}$$
- Here, $s = 937$, $b, d = 1, m = 2436$, thus solution: $x = 937$
- $0981^{937} \pmod{2537} = 0704$; $0461^{937} \pmod{2537} = 1115$
- Thus, decrypted message is $0704 1115$, or in English, "HELP"

RSA Decryption

- Decryption function: Given cipher text $C$, decrypt as $C^d \pmod{n}$
- Decryption key $d$ is the inverse of $e$ modulo $(p - 1)(q - 1)$:

$$d \cdot e \equiv 1 \pmod{(p - 1)(q - 1)}$$
- As we saw earlier, $d$ can be computed reasonably efficiently if we know $(p - 1)(q - 1)$

RSA proof sketch, cont.

- Now, consider $M^{ed}$:

$$M^{ed} = M \cdot M^{ed - 1} = M \cdot M^{\phi(n)} = M \cdot M^{\phi(n)}$$
- Using Euler’s theorem,

$$M \cdot M^{\phi(n)} \equiv M \cdot 1 \pmod{\phi(n)} \equiv M \mod{\phi(n)}$$
- Thus, applying decryption function to cipher text gives us original message!
## Security of RSA

- The encryption function used in RSA is a **trapdoor function**
- Trapdoor function is easy to compute in one direction, but very difficult in reverse direction without additional knowledge
- Decryption without private key is very hard because requires prime factorization (which is intractable for large enough numbers)
- **Interesting fact:** There are efficient (poly-time) prime factorization algorithms for quantum computers (e.g., Shor’s algorithm)
- If we could build quantum computers with sufficient “qubits”, RSA would no longer be secure!

---

## Book Recommendation

If you are interested in (history of) cryptography, read "The Code Book" by Simon Singh!

---

## Induction

- Suppose we have an infinite ladder, and we know two things:
  1. We can reach the first rung of the ladder
  2. If we reach a particular rung, then we can also reach the next rung
- From these two facts, can we conclude we can reach every step of the infinite ladder?
- Answer is yes, and mathematical induction allows us to make arguments like this

---

## Mathematical Induction

- Used to prove statements of the form $\forall x \in \mathbb{Z}^+. P(x)$
- An inductive proof has two steps:
  1. **Base case:** Prove that $P(1)$ is true
  2. **Inductive step:** Prove $\forall n \in \mathbb{Z}^+. P(n) \rightarrow P(n+1)$
- Induction says if you can prove (1) and (2), you can conclude:
  $\forall x \in \mathbb{Z}^+. P(x)$

---

## Example 1

- Prove the following statement by induction:
  $$\forall n \in \mathbb{Z}^+. \sum_{i=1}^{n} i = \frac{(n)(n+1)}{2}$$
- **Base case:** $n = 1$. In this case, $\sum_{i=1}^{1} i = 1$ and $\frac{(1)(1+1)}{2} = 1$; thus, the base case holds.
- **Inductive step:** By the inductive hypothesis, we assume $P(k)$:
  $$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$
  Now, we want to show $P(k+1)$:
  $$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$
Example 1, cont.

- First, observe:
  \[ k + 1 \sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k + 1) \]

- By the inductive hypothesis, \( \sum_{i=1}^{k} i = \frac{k(k+1)}{2} \); thus:
  \[ \sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + (k + 1) \]

- Rewrite left hand side as:
  \[ \sum_{i=1}^{k+1} i = \frac{k^2 + 3k + 2}{2} = \frac{(k+1)(k+2)}{2} \]

- Since we proved both base case and inductive step, property holds.

Example 2

- Prove the following statement for all non-negative integers \( n \):
  \[ \sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \]

Example 3

- Prove that \( 2^n < n! \) for all integers \( n \geq 4 \)

Example 4

- Prove that \( 3 \mid (n^3 - n) \) for all positive integers \( n \).

The Horse Paradox

- Easy to make subtle errors when trying to prove things by induction – pay attention to details!
- Consider the statement: All horses have the same color
- What is wrong with the following **bogus proof** of this statement?
  - \( P(n) \): A collection of \( n \) horses have the same color
  - Base case: \( P(1) \) \( \checkmark \)
Bogus Proof, cont.

- Induction: Assume $P(k)$; prove $P(k + 1)$
- Consider a collection of $k + 1$ horses: $h_1, h_2, \ldots, h_{k+1}$
  - By IH, $h_1, h_2, \ldots, h_k$ have the same color; let this color be $c$
  - By IH, $h_2, \ldots, h_{k+1}$ have same color; call this color $c'$
  - Since $h_2$ has color $c$ and $c'$, we have $c = c'$
- Thus, $h_1, h_2, \ldots, h_{k+1}$ also have same color
- What’s the fallacy?

Strengthening the Inductive Hypothesis

- Suppose we want to prove $\forall x \in \mathbb{Z}^+. P(x)$, but proof doesn’t go through
- Common trick: Prove a stronger property $Q(x)$
  - If $\forall x \in \mathbb{Z}^+. Q(x) \rightarrow P(x)$ and $\forall x \in \mathbb{Z}^+. Q(x)$ is provable, this implies $\forall x \in \mathbb{Z}^+. P(x)$
  - In many situations, strengthening inductive hypothesis allows proof to go through!

Example

- Prove the following theorem: “For all $n \geq 1$, the sum of the first $n$ odd numbers is a perfect square.”
- We want to prove $\forall n \in \mathbb{Z}^+. P(n)$ where:
  $$P(n) = \sum_{i=1}^{n} 2i - 1 = k^2$$
  for some integer $k$
- Try to prove this using induction...

Example, cont.

- Let’s use a stronger predicate:
  $$Q(n) = \sum_{i=1}^{n} 2i - 1 = n^2$$
- Clearly, $Q(n) \Rightarrow P(n)$
- Now, prove $\forall n \in \mathbb{Z}^+. Q(n)$ using induction!