Week ∞

A Sample TEX SIGma Presentation

Ma, Sig

Outline

Updates!

Weekly updates:

- SIGma is an excellent SIG.
- I'm out of ideas for updates.

Section 1

Basics

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem

There is no largest prime number.

1. Suppose p were the largest prime number.

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem

There is no largest prime number.

1. Suppose p were the largest prime number.
2. Let q be the product of the first p primes.

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem

There is no largest prime number.

1. Suppose p were the largest prime number.
2. Let q be the product of the first p primes.
3. Then $q + 1$ is not divisible by any of them.

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem

There is no largest prime number.

1. Suppose p were the largest prime number.
2. Let q be the product of the first p primes.
3. Then $q + 1$ is not divisible by any of them.
4. But $q + 1$ is greater than 1, thus divisible by some prime number not in the first p numbers.

There Is No Largest Prime Number

The proof uses *reductio ad absurdum*.

Theorem

There is no largest prime number.

1. Suppose p were the largest prime number.
2. Let q be the product of the first p primes.
3. Then $q + 1$ is not divisible by any of them.
4. But $q + 1$ is greater than 1, thus divisible by some prime number not in the first p numbers.
5. There exists a prime larger than p.

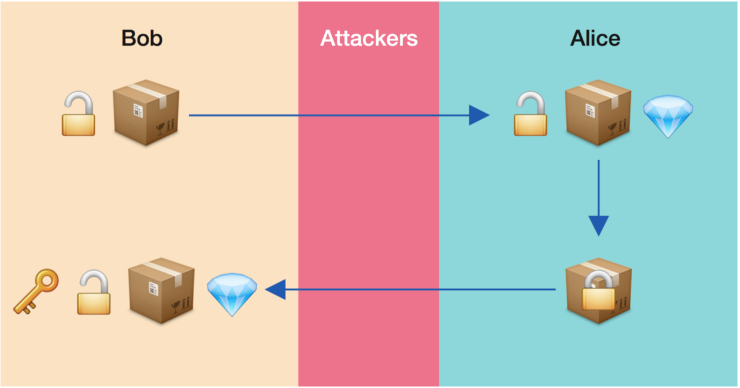
Section 2

RSA

Subsection 1

Some Intuition

Image



Subsection 2

The Math

Key Generation

1. Find primes p, q. Compute $n = pq$.
2. Compute $\phi = (p-1)(q-1)$.
3. Let e be a number coprime to n.
4. Compute $d = e^{-1} \pmod{\phi}$.
5. (n, e) is the **public key** tuple, d is the **private key**.

Message Exchange

1. To send message m to Alice, Bob computes $c = m^e \pmod{n}$ using Alice's public key (n, e) and sends c to Alice.
2. Alice computes $m = c^d \pmod{n}$ to recover m.

Some Math Mode Testing

$$\frac{x^2 + 3}{y^2 + 7}$$

$$\mathcal{L}_{\mathcal{T}}(\vec{\lambda}) = \sum_{(\mathbf{x},\mathbf{s})\in\mathcal{T}} \log P(\mathbf{s} \mid \mathbf{x}) - \sum_{i=1}^{m} \frac{\lambda_i^2}{2\sigma^2}$$

$$\int_0^8 f(x)dx$$

Some Sample Code

Section 3

Conclusion

So long, and thanks for all the fish!