Cryptography Day 2

Brandon Hernandez

September 17, 2020

Overview

Brief Review

In crypto, we utilize hard problems in mathematics to ensure that breaking the cryptosystem is not trivial.

Diffie-Hellman

The RSA Cryptosystem

Public-key cryptosystem based around the difficulty in factoring a composite integer into primes.

The RSA Problem

- Consider two large primes, p and q
- $N = pq$
- Consider e, m, and c, where $e, C, m \in \mathbb{Z}$
- $C \equiv m^e \pmod{\mathrm{N}}$

Construction

- Consider two large primes, p and q
- Let our modulus, $N = pq$ $(\mathbb{Z}/N\mathbb{Z})$
- Our public key, e, where $gcd(\phi N, e) = 1$ and $1 < e < \phi N$
- The private key, d, where $d * e \equiv 1 (\mathrm{mod} \phi N)$

Encryption

- Given N, m, and e
- $C \equiv m^e (mod N)$

Decryption

- Given N, C, and d
- $m \equiv C^d \equiv m^{e*d} (mod N)$
- **Remeber:** $e * d \equiv 1 (mod \phi N)$

Construction Example

Basic Exploit Example 1

Refer to Day2/Examples/cube

Basic Exploit Example 2 (Factoring)

Refer to Day2/Examples/multiPrime

Basic Exploit Example 3 (Hastad)

Refer to Day2/Examples/hastad

What's left?

- Elliptic Curve Cryptography
- Post Quantum Cryptography
  - Lattice-Based Cryptography
  - LWE
  - Multivariate Cryptograhy