Cryptography Day 2

Brandon Hernandez

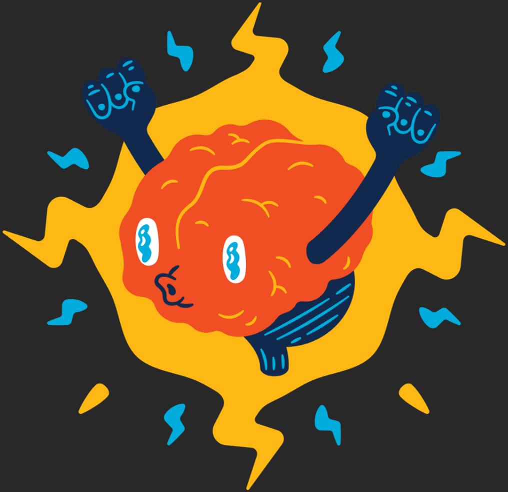
September 18, 2020

Overview

Brief Review

In crypto, we utilize hard problems in mathematics to ensure that breaking the cryptosystem is non-trivial. We looked at basic modular arithmetic last time, we'll continue on with that today with RSA and Diffie-Hellman.

Crytpohack Docker



https://cryptohack.org/

Diffie-Hellman

An early version of what we would call public key protocol, also called asymmetric. If you remember the One-time pad, we used a singular key for encryption and decryption.

If we wish to share a message encrypted using a One-time pad with someone how do we securely give them the key?

Asymmetric and Symmetric

- *Asymmetric* $\longrightarrow$ different keys for encryption and decryption
  - RSA,Diffie-Hellman Key Exchange, ECC
- *Symmetric* $\longrightarrow$ same key is used for encryption and decryption
  - One-time pads, AES

Diffie-Hellman Construction

- Prime modulus, p
- Base, g
- Two individuals Alice and Bob, whose private keys are a and b, respectively
- Alice and Bob's public keys are A and B
  - $A \equiv g^a \ (mod\ p)$
  - $B \equiv g^b \ (mod\ p)$
- Alice and Bob communicate A and B
- Shared secret, $S \equiv g^{a*b} \equiv g^{b*a} \ (mod\ p)$
- *Discrete Logarithm Problem*

Diffie-Hellman Demo

Refer to Day_2/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
- $C \equiv m^e (\mathrm{mod\ N})$

Construction

- Consider two large primes, p and q
- Let our modulus, $N = pq$
- Our public key, e, where $gcd(\phi N, e) = 1$ and $1 < e < \phi N$
  - So our private key, d, exists
- 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
- $m \equiv C^d \equiv m^{e*d}(mod N)$
- **Euler's theorem:** $a^{\phi(N)} \equiv 1(mod N)$
- **Remember:** $e * d \equiv 1(mod \phi N)$
- $ed = k\phi(N) + 1$
- $m^{\phi(N)} \equiv 1 \ (mod \ N)$
- $m^{ed} \equiv m^{\phi(N)+1} \equiv m^{\phi(N)} * m \equiv m \ (mod N)$

Construction Example

Refer to Day_2/Examples/construction

Basic Exploit Example 1

Refer to Day_2/Examples/cube

Basic Exploit Example 2 (Factoring)

Refer to Day_2/Examples/multiPrime

Basic Exploit Example 3 (Hastad)

Refer to Day_2/Examples/hastad

What's left?

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