Cryptography 4/20

Reagan Shirk

April 20, 2020

Updates

- Wednesday we're going to have an extra credit quiz
  - 10 points
  - I think we have to have our cameras on
  - "As long as you write something you'll probably get the credit" - Dr. Cheng
- We will have a sample final like we had a sample midterm
- Submit your evals
- Looks like the fall semester *might* be on Zoom too
- This was a good way to kill 12 minutes of class time

RSA

- Based on the difficulty of factoring
  - Factoring is a v hard problem
  - This is why RSA is a good choice
  - RSA won't be secure if you have a quantum computer

RSA Mathematics

- Generalized Fermat Little Theorem
  - Says that if p is a prime and p doesn't divide a, then $a^{p-1} = 1(\text{mod} p)$
  - If $\gcd(a, n) = 1$, then $a^{\phi(n)} = 1(\text{mod} n)$
  - In particular, if $n = pq$ then $a^{(p-1)(q-1)} = 1(\text{mod} n)$

RSA Key Generation

- Two large, random, prime numbers p and q that will be your private keys
  - $n = pq$
- e is the encryption key
  - $\gcd(e, (p-1)(q-1)) = 1$
- d is the decryption key
  - $d = e^{-1}(\text{mod}(p-1)(q-1))$
  - $\phi(n) = (p-1)(q-1)$
- The public key is (n, e)
- The secret key is (n, d)

RSA Encryption (textbook version)

- ciphertext $= m^e \bmod n$
- Usually $e = 2^{16} + 1 = 65537$

RSA Decryption (textbook version)

- $m = c^d \bmod n$
  - We want to prove this- correctness of RSA

Correctness of RSA

$$
\begin{aligned}
&c^d \bmod n \\
&= ((m^e)^d) \bmod n \\
&= m^{ed} \bmod n \\
&= m^{1+a\phi(n)} \bmod n \text{ (where } a \in \mathbb{Z}) \\
&= m(m^{\phi(n)})^a (\mathrm{mod} n) \\
&= m, \text{ because } \gcd(m, n) = 1
\end{aligned}
$$

Efficiency of RSA

- For efficiency, $e = 65537 = 2^{16} + 1$
  - We need 17 modular multiplications for encryption which is fine
    - Somehow we come to 17 because of $16 + 1$ from $2^{16} + 1$
- Decryption still slow af though
- You can run into a problem when e is really small because m^e will have less bits than n and doing the $\mathrm{mod} n$ won't do anything
- Best place for RSA is signature because it isn't very efficient for encryption and decryption

Security of RSA

- Different levels of security
  - If $\phi(n)$ can be computed from n, then RSA is broken
  - If d can be computed from n and e, then RSA is broken
  - If p and q can be computed, then RSA is broken