Cryptography

Dov Kruger

Department of Electrical and Computer Engineering
Rutgers University

March 26, 2024

Introduction

Cryptography is the mathematics of obscuring information in a reversible manner. Standard Terminology and conventions

- Alice and Bob are two parties who want to have a secure conversation
- In some scenarios, Eve is evesdropping
- Alice can write an encrypted message to disk, in effect sending a secure message to herself.
- Symmetric cryptography uses a shared secret (the key) to encrypt the message
- Asymmetric cryptography uses a public key and a private key

Symmetric Cryptography

Traditionally cryptography makes secrecy possible with a shared key

- encrypt a message $c = E(key, m)$
- decrypt a message $m = D(key, c)$
- Both require same key
- If multiple parties have the key, impossible to determine who sent message

Public Key Cryptography

Public key cryptography (1976, Diffie, Hellman, Merkle)
Requires a one-way operation

- Two keys (public and private)
- Public key encrypts
- Everyone may see the public key
- private key decrypts

RSA Overview

- Rivest-Shamir-Adleman
- Easy direction $n = pq$ $O(k \log k)$, k is number of bits in p, q
- Hard direction factoring $n = pq$ $O(\sqrt{2^{8192}}) \approx 2^{4096}$

RSA Algorithm

- Pick two random prime numbers p and q
- Compute $n = pq$
- Compute $\phi(n) = (p-1)(q-1)$
- Pick a random integer e such that $1 < e < \phi(n)$ and $gcd(e, \phi(n)) = 1$
- Compute d such that $de \mod \phi(n) = 1$

- Encrypt: $E(m, k_{pub}) = c = m^e \mod n$
- Decrypt: $D(c, k_{priv}) = m = c^d \mod n$
- Sign: $send(m, h' = D(hash(m), k_{priv})$
- Verify: $verify(m, h')hash(m) = E(h', k_{pub})$

Note: since RSA is subject to plaintext attacks, only use RSA to exchange keys for use in symmetric crypto (AES-256 currently)

RSA Example

- $p = 31$ and $q = 47$
- $n = pq = 1457$
- $\phi(n) = (p-1)(q-1) = 30 * 46 = 1380$
- $e = 17$
- $de \mod \phi(n) = 1$
- $d = extendedEuclid(e, \phi(n)) = -487$
- $d = -487 + 1380 = 893$
- Given $m =' A' = 65$
- Encrypt $= c = 65^17 \mod 1457 = 1147$ Decrypt: $D(c, k_{priv}) = m = c^d \mod n$
- Sign: $send(m, h' = D(hash(m), k_{priv})$
- Verify: $verify(m, h')hash(m) = E(h', k_{pub})$

Note: since RSA is subject to plaintext attacks, only use RSA to exchange keys for use in symmetric crypto (AES-256 currently)

Complexity of RSA

- Complexity of finding a $prime > 2^n$
- Complexity of $powermod(a, b, c)$

Readings on Cryptography

- Non-technical book: The Codebreakers by David Kohn
- Practical Cryptography: `https://www.schneier.com/books/applied-cryptography/`
- Practical Cryptography for developers: `https://https://cryptobook.nakov.com/`