Cryptography

Dov Kruger

Department of Electrical and Computer Engineering
Rutgers University

January 23, 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 $m = D(key, c)$

Encryption and decryption both require same key

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

Complexity of RSA

Select two random prime numbers What is the complexity of finding a $prime > 2^n$

Readings on Cryptography

Non-technical book: The Codebreakers by David Kohn

Practical Cryptography:

`https://www.schneier.com/books/applied-cryptography/`