Secure Software Design

Andey Robins

Spring 23 - Week 5

Cryptography

Outline

- Cryptographic Primitives
- Hashing
- Symmetric Encryption
- Asymmetric Encryption
- KDAs
- Signing
- CAs and Certificates

Crypto Primitives

Crypto Primitives

- Hashes
- SRNGs
- Keys

Hashes

SRNGs

Cryptographically Secure RNGs vs Pseudo RNGs

Keys

Hashing

Symmetric Encryption

Asymmetric Encryption

Diffie-Helman Key Exchange

RSA

Elliptic Curve

NIST Curve Controvery

Key Derivation Algorithms

Signing

CAs and Certificates