Cryptography Fundamentals

Table of Contents

- Definition
- Symmetric Key
- Asymmetric Key
- Hash Functions
- Digital Signatures
- Cryptanalysis
- Public Key Infrastructure

Definition

- Secure Communication
- Mathematical Foundation
- Encryption/Decryption
- Ensuring CIA Triad
- Broad Application

Symmetric Key

- Single Shared Secret Key
- Secure Key Exchange
- High Encryption Speed
- Key Management Challenge

Asymmetric Key

- Key Pairs - Public and Private
- Encryption/Decryption
- Authentication/Non Repudiation
- Key Exchange/Establishment

Hash Functions

- Fixed Size Output
- One Way Function
- Collision Resistance
- Avalanche Effect
- Application Examples

Digital Signatures

- Cryptographic Mechanism
- Public Key Infrastructure
- Signing and Verification Process
- Non-repudiation and Integrity
- Legal Recogntition and Compliance

Cryptanalysis

- Objective
- Attack types
- Technique
- Escalation of Offense vs. Defense
- Landscape

Public Key Infrastructure

- Asymmetric
- Digital Certificate Management
- Trust Hierarchy
- Authentication and Non Repudiation
- Encrypt and Key Exchange

Cryptography Exercise

Cipher Presentation

- Get into groups of 2-3 People
- Pick a cipher from this page https://privacycanada.net/short-list-of-classical-ciphers/

Slide 1: Origin of this cipher
Slide 2: What is the cipher’s key?
Slide 3: Explain a Key you created using this cipher
Slide 4: Show how you would encrypt a message using this cipher
Slide 5: Show how you would decrypt a message using this cipher

15 Minutes to choose a cipher
30 Minutes to build Presentation
30 Minutes for Presentations

Plain Text Message must be at least 20 Words long
0-5 Points for detail of each slide

Raise your hand if you have a question at any time

Questions?

- https://privacycanada.net/short-list-of-classical-ciphers/
- https://www.testportal.net/test.html?t=SnnDv27gtQa8