Applied Cryptography

Course 71582 – 40 Hours

Overview

Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages. This course will introduce you to the fundamentals of Cryptography - from deep theory concepts, to practical applications of the different encryption schemes and where they are used in real world applications (e.g. dig. sign. in Blockchain). We will cover all aspects of modern cryptography such as data confidentiality, data integrity, authentication, and non-repudiation.

On Completion, Delegates will be able to

- Explain the strength of different encryption schemes against different kinds of attacks.
- Choose the correct encryption scheme for your mission.
- Correctly secure your secrets/data in your applications.
- Understand Blockchain, smart contracts and their connection to crypto currencies like Bitcoin/Ethereum.
- Solve Crypto CTF's for fun & profit.

Who Should Attend

- Developers
- Researchers
- Hands-on Pentesters
- Malware Analysts
- Math enthusiasts

Prerequisites

- C and Python programming.
- Linear Algebra, Probability, Group Theory.

Course Contents

Intro & Stream Ciphers

- What is cryptography?
  - Course overview
  - What is cryptography

    - History of cryptography
- Crash course in discrete probability
    - Discrete probability (crash course)
    - Discrete probability (crash course, continued)
- Stream Ciphers 1: the one-time pad and stream ciphers
    - Information theoretic security and the one-time pad
    - Stream ciphers and pseudorandom generators
    - Stream Ciphers 2: attacks and common mistakes
    - Attacks on stream ciphers and the one-time pad
- Stream Ciphers 3: real-world examples
    - Real-world stream ciphers
- Stream Ciphers 4: what is a secure cipher?
    - PRG security definition
    - Semantic security
    - Stream ciphers are semantically secure

Block Ciphers

- Block Ciphers 1: overview
    - What are block ciphers
- Block Ciphers 2: The Data Encryption Standard
    - The Data Encryption Standard (DES)
    - Exhaustive search attacks
    - More attacks on block ciphers
- Block Ciphers 3: AES and other constructions
    - The AES block cipher
    - Block ciphers from PRGs
- How to Use Block Ciphers 1: one-time key
    - Review: PRPs and PRFs
    - Modes of operation: one-time key
- How to Use Block Ciphers 2: many-time key
    - Security for many-time key (CPA security)
    - Modes of operation: many-time key (CBC)
    - Modes of operation: many-time key (CTR)

Message Integrity

- Message Integrity 1: definitions
    - Message authentication codes
    - MACs based on PRFs
- Message Integrity 2: constructions
    - CBC-MAC and NMAC
    - MAC padding
- Collision Resistance 1: what is a collision resistant function?
    - Introduction
    - Generic birthday attack

- Collision Resistance 2: constructions
  - The Merkle-Damgard paradigm
  - Constructing compression functions
- HMAC: a MAC from a hash function
  - HMAC (7 min.)
  - Timing attacks on MAC verification (8 min.)

Basic Key Exchange

- Basic Key Exchange 1: problem statement
  - Trusted 3rd parties
  - Merkle puzzles
- Basic Key Exchange 2: two solutions
  - The Diffie-Hellman protocol
  - Public-key encryption
- Number Theory 1: modular arithmetic
  - Notation
  - Fermat and Euler
  - Modular e'th roots
- Number Theory 2: easy and hard problems
  - Arithmetic algorithms
  - Intractable problems

Public-Key Encryption

- Public Key Encryption from Trapdoor Permutations
  - Definitions and security
  - Constructions
- Public Key Encryption from Trapdoor Permutations: RSA
  - The RSA trapdoor permutation
  - PKCS1
- Public Key Encryption from Trapdoor Permutations: attacks
  - Is RSA a one-way function?
  - RSA in practice

Digital Signatures

Intro to Blockchain

- What is the Blockchain?
- Application of the Blockchain.
- Differences between PoW and PoS.
- Bitcoin
  - Brief History Overview
  - Crypto used in Bitcoin (SHA256, ECDSA)
  - Full nodes
  - Different kinds of wallets (cold, paper, hardware), and the risks of using each.
  - Transactions and blocks structures.

  - The mining process, tx fees, miners reward.
  - Mining difficulty.
- Intro to dapps and smart contracts (Ethereum)
  - Truffle, ERC Process (ERC-20)

Packers

- Different types: Inline, New PE, Resource
- Cryptography techniques used.

Ransomware

- Overview on Ransomware evolution
- How to revert Ransomware operation?
- Petya ransomware full breakdown

CPU Enclaves

- CPU Enclaves technology overview
- Intel SGX breakdown - is it secure?
- What is attestation?
- Known attacks (side-channel)
- Simple Enclave programming