

Cybersecurity Concepts

Prepared by Dr. Sumaya Alkubaisi

FNT625
Cybersecurity Concepts

Lecture 0



Agenda

Introduction

- a. Welcome & Overview
- b. Brief on the Cybersecurity concepts

Chapter Overviews

- **a. Chapter 1: Introduction to Cybersecurity** - introduces the fundamentals of cybersecurity in fintech, covering core principles (CIA triad), major threats, protective measures, and regulatory frameworks. It also explores key technologies and emerging trends like AI, zero trust, and privacy vs transparency.

Agenda

- **b. Chapter 2: Introduction to Network and Network Security** - introduces computer networks and how they enable communication. It explains key network security principles, common attacks, and defenses in fintech.
- **c. Chapter 3: Classical Encryption Techniques** - explores classical encryption methods such as substitution and transposition ciphers. It highlights their historical importance and how they form the basis of modern cryptography.

Agenda

- **d. Chapter 4: Block Cipher and DES(Feistel Cipher) -**
Introduces block cipher principles with a focus on DES as a foundational algorithm. Explains structure, operation, and its role in modern encryption evolution.
- **e. Chapter 5: Block Cipher and DES(Attacks on DES) -**
Explains how block ciphers work with DES as a case study. Discusses known attacks on DES and why stronger algorithms are needed.

Agenda

- **f. Chapter 6: Finite Fields (Fields and Modular Arithmetic)** - Introduces the math behind modern cryptography, focusing on finite fields and modular arithmetic. Shows how these concepts support encryption algorithms.
- **g. Chapter 7: Advanced Encryption Standard (AES)** - Covers AES design, structure, and operation as today's global standard. Highlights why it replaced DES and its role in protecting fintech data.

Agenda

- **h. Chapter 8: Public Key Cryptography (RSA)** - Explains RSA for secure communication, digital signatures, and key exchange.
- **i. Chapter 9: Message Authentication and Hashing** - Shows how hashing and MACs protect data integrity and prevent tampering.
- **j. Chapter 10: Introduction to Cloud Computing** - Explains cloud basics and key security issues in fintech systems.

Closing Remarks

Course Description

- This course aims to provide students with a solid foundation in Cybersecurity Fundamentals, focusing on the protection of computer systems, networks, and data against the growing landscape of digital threats.
- The course covers core cybersecurity concepts, starting with network security and communication protocols, progressing through classical and modern cryptographic techniques, and extending to data integrity, authentication, and cloud security concepts.

Course

Description

- The course emphasizes both conceptual understanding and practical awareness of cybersecurity. Students will explore common cyber attacks, threat models, and defense mechanisms used in modern digital environments, with particular attention to sensitive domains such as the financial sector.
- The course also includes optional hands-on exercises using the Python programming language to demonstrate, at a conceptual level, how cryptographic and hashing algorithms operate. These activities are designed to bridge theory and practice without requiring advanced programming experience.

Course Description

- By the end of the course, students will be able to understand key cybersecurity challenges, assess basic security risks, and comprehend the fundamental principles behind secure systems in contemporary digital environments.

Introduction to Cybersecurity

Cybersecurity is the discipline focused on protecting computer systems, networks, applications, and digital data from cyber threats that may lead to:

- Information theft
- Service disruption
- Financial losses
- Privacy violations

Introduction to Cybersecurity

With the rapid digital transformation and the increasing reliance on information systems, digital data has become a valuable asset, especially in:

- Banks and financial institutions
- Government systems
- Technology companies
- Individual users

A single security breach can result in serious consequences at the level of individuals, organizations, or even nations.

Introduction to Cybersecurity

The Three Pillars of Cybersecurity (People – Process – Technology)

Cybersecurity does not rely on technology alone; it is built on three interconnected pillars:

- **People:**

User awareness and security training

Ability to recognize phishing and social engineering attacks

Compliance with security policies

Introduction to Cybersecurity

The Three Pillars of Cybersecurity (People – Process – Technology)

- **Processes:**

- Password and access management policies
- Incident response and recovery procedures
- Risk management and security governance

Introduction to Cybersecurity

The Three Pillars of Cybersecurity (People – Process – Technology)

- **Technology:**

- Firewalls
- Intrusion Detection and Prevention Systems (IDS/IPS)
- Encryption mechanisms
- Security monitoring tools

Introduction to Cybersecurity

Common Cyber Threats

- **Phishing:** Fraudulent messages designed to steal login credentials
- **Malware:** Malicious software that damages or compromises systems
- **Ransomware:** Encrypts data and demands payment to restore access

Introduction to Network and Network Security

- Computer networks enable communication between systems through structured models (e.g., TCP/IP, OSI).
- Network security applies firewalls, IDS/IPS, VPNs, and secure protocols to protect data in transit.

Classical Encryption Techniques

- Early encryption methods include substitution (e.g., Caesar cipher) and transposition methods of ciphers.
- Though simple and breakable today, they laid the foundation for modern cryptography.
- Caesar cipher example: BANK → EDQN

Block Cipher and DES (Feistel Cipher)

- Block cipher encrypts data in fixed-size blocks (e.g., 64 or 128 bits) using a secret key.
- DES (Data Encryption Standard) introduced the Feistel structure, dividing data into halves and applying round functions.
- This design influenced modern block ciphers despite DES now being insecure.

Block Cipher and DES (Attacks on DES)

- DES's short 56-bit key made it vulnerable to brute force and differential/linear cryptanalysis.
- Its weaknesses led to the adoption of stronger algorithms like AES.
- it's studied to understand the evolution of encryption.

Finite Fields (Fields and Modular Arithmetic)

Why Do We Need Mathematics in Cryptography?

- Modern cryptography does not depend on hiding algorithms; instead, it relies on strong mathematical foundations that make breaking encryption computationally infeasible.

Finite Fields (Fields and Modular Arithmetic)

What is Modular Arithmetic?

- Modular arithmetic is a system of arithmetic where numbers “wrap around” after reaching a certain value (the modulus).
- Simple example: $17 \bmod 5 = 2$

Finite Fields (Fields and Modular Arithmetic)

What is Modular Arithmetic?

- It is widely used in cryptography because it is:
 - Efficient to compute
 - Difficult to reverse without the correct key

Finite Fields (Fields and Modular Arithmetic)

What Are Finite Fields?

- Finite fields are mathematical structures that contain a limited number of elements, where arithmetic operations (addition, multiplication, etc.) follow specific rules.

Finite Fields (Fields and Modular Arithmetic)

What Are Finite Fields?

- They are essential because they:
 - Guarantee well-defined and consistent results
 - Prevent computational ambiguity
 - Provide the mathematical structure needed for secure encryption

Finite Fields (Fields and Modular Arithmetic)

Role in Modern Cryptography

Finite fields and modular arithmetic form the mathematical backbone of many cryptographic algorithms, including:

- AES: Based on operations in the finite field $GF(2^8)$
- RSA: Relies on modular arithmetic with very large prime numbers

Finite Fields (Fields and Modular Arithmetic)

Why Is This Important?

- To understand how and why cryptographic algorithms work
- To distinguish between strong and weak encryption schemes

Finite Fields (Fields and Modular Arithmetic)

Why Is This Important?

- To build a solid foundation for advanced cryptography topics

The goal here is not deep mathematical detail, but rather a conceptual understanding of the principles behind modern encryption.

Advanced Encryption Standard (AES)

- AES is the global standard for symmetric data encryption and is widely used in modern systems to protect sensitive information.

Advanced Encryption Standard (AES)

- AES is based on a Substitution-Permutation Network (SPN) structure, where data passes through multiple rounds of substitution, permutation, and mixing operations to enhance security.

Advanced Encryption Standard (AES)

- AES supports different key sizes:
 - 128,
 - 192,
 - and 256 bits

with larger key sizes providing higher security levels.

Advanced Encryption Standard (AES)

AES is commonly used in practical applications such as:

- Encrypting data stored in databases
- Securing network communications (TLS/SSL)
- Protecting data in financial systems and banking applications

Advanced Encryption Standard (AES)

- AES is known for its high efficiency, making it suitable for both software and hardware implementations, and it remains secure when used with proper configurations.

Public Key Cryptography (RSA)

- RSA introduced asymmetric cryptography: public keys for encryption, private keys for decryption.
- It enables secure communication, digital signatures, and key exchange in fintech.

Message Authentication and Hashing

- Hash functions and MACs provide data integrity and authenticity.
- They are used in digital signatures, password storage, and blockchain.

Introduction to Cloud Computing

This chapter is an overview about cloud computing and its role in modern fintech.

Cloud computing means using internet-based services (like servers, storage, and applications) instead of local computers.



Introduction to Cloud Computing

Why we use it?

It offers scalability, flexibility, and cost savings – fintech apps can grow fast without buying expensive hardware.



Introduction to Cloud Computing

Main models:

IaaS (Infrastructure as a Service): rent servers/storage.

PaaS (Platform as a Service): rent tools for building apps.

SaaS (Software as a Service): use ready-made apps (e.g., online banking platforms).



Introduction to Cloud Computing

Security concerns: Protecting sensitive financial data, managing access, and ensuring compliance with regulations.

Today: Almost all fintech companies rely on cloud services (AWS, Azure, Google Cloud) – making cloud security a core part of cybersecurity.



Closing Remarks

"Over the coming weeks, we'll explore key cybersecurity concepts, from network security to encryption techniques, and learn how to apply them in real scenarios. Stay curious, ask questions, and engage actively – this course is designed to build both your knowledge and your practical skills."



Thank you!

Thank You