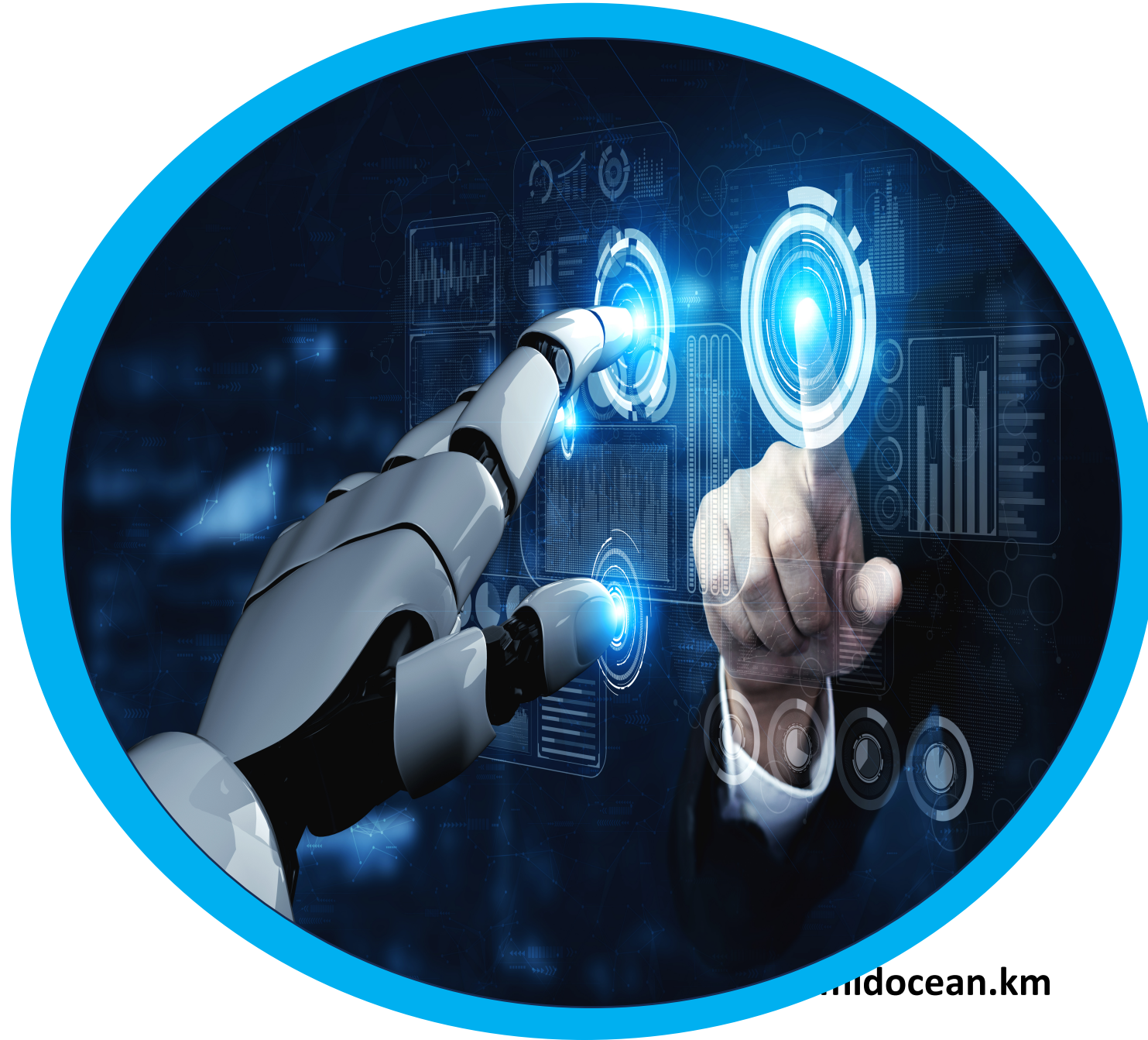


Cybersecurity Concepts

Prepared by Dr. Sumaya Alkubaisi

FNT625
Cybersecurity Concepts

Lecture 0



Agenda

Introduction

- a. Welcome & Overview
- Academic Services and Systems for MidOcean University Students
- 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.
- 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.

Agenda

- 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.
- 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.
- 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.

Agenda

- **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.
- **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. Introduction to Cloud Computing** - Explains cloud basics and key security issues in fintech systems.

Closing Remarks

البوابة الأكاديمية

تُتيح جامعة ميدأوشن للطلاب الحصول على العديد من الخدمات من خلال الدخول إلى البوابة الأكاديمية، حيث يمكن من خلالها التقدم للدراسة بالجامعة، ومتابعة الإدارة لطلبات التقدم، والتواصل مع المتقدمين بشأن استكمال إجراءات القبول والتسجيل، وحفظ بيانات الدفع ومراجعتها، فضلاً عن نشر درجات الطلاب والمعدل التراكمي النهائي في نهاية الفصل الدراسي، كما يمكن من خلال خدمات البوابة الأكاديمية:

- حذف وإضافة المقررات
- البحث عن جداول المقررات
- استعراض الجدول الدراسي بشكل مفصل.
- الاطلاع على الدرجات النهائية للمقررات المسجلة للطلاب.

esu.ac.ae تسجيل الدخول | خدمات ميدأوشن

البوابة التعليمية

تُمثل التجمع الرئيسي بين الطلاب وأستاذ المقرر، وتُقدم العديد من الخدمات التعليمية للطلاب منها:

- الوصول للمقررات الدراسية، حيث يمكن للطلاب قراءة المقررات الدراسية وتحميلها ..
- الفصول الافتراضية التي يلتقي من خلالها أستاذ المقرر بالطلاب لشرح المحاضرات، إلى جانب التواصل المباشر والفعال معهم، والرد على أسئلتهم.
- حلقة تبادل المعلومات، حيث يمكن للطلاب من خلال منصة Moodle الوصول إلى الأنشطة اللامنهجية التي تقدمها الجامعة.
- تتيح البوابة التعليمية الوصول إلى الكتب الإلكترونية التي تساعد الطلاب في حل الأنشطة والواجبات الدراسية.
- إجراء الاختبارات القصيرة التي تعبر عن انتظام الطلاب في الدراسة، فضلاً عن تقديم الواجبات والأبحاث، وعقد الاختبارات الفصلية والنهائية.

نظام التذاكر

يعد نظام التذاكر الآلية التي يمكن للطلاب من خلالها التواصل مع الجامعة، ومع أعضاء هيئة التدريس، وتقديم الطلبات والاستفسارات.

خطوات فتح التذاكر:

- التوجه إلى البوابة الأكاديمية، والدخول من خلال كتابة اسم المستخدم وكلمة السر.
- النقر على خيار تذكرة، ثم الضغط على فتح تذكرة جديدة.
- اختيار القسم المهني بالتذكرة، ثم كتابة الموضوع الرئيسي، والتفاصيل في الخانة المخصصة لذلك.
- يمكن إرفاق الملفات من خلال الضغط على أيقونة الملف المرفق.
- الضغط على فتح تذكرة، ثم سيصلك رسالة إلكترونية توضح حالة التذكرة وآلية متابعتها.

التقويم الأكاديمي للفصل الدراسي الثالث للعام 2025-2026

التاريخ	الحدث
04/10/2025	بداية الفصل الدراسي
01/11/2025	آخر موعد للاعتذار عن الفصل أو مقرر
27/12/2025	بداية الاختبارات النهائية
03/01/2026	نهاية الاختبارات النهائية

الأسبوع	الوصف	التاريخ
الأسبوع 1	محاضرة توجيهية - اختبار قصير	04/10/2025
الأسبوع 2	محاضرة - حلقة نقاش - اختبار قصير	11/10/2025
الأسبوع 3	محاضرة - حلقة نقاش - اختبار قصير	18/10/2025
الأسبوع 4	محاضرة - حلقة نقاش - اختبار قصير	25/10/2025
الأسبوع 5	محاضرة - حلقة نقاش - اختبار قصير آخر موعد للاعتذار عن الفصل أو عن مقرر	01/11/2025
الأسبوع 6	محاضرة - حلقة نقاش - اختبار قصير	08/11/2025
الأسبوع 7	محاضرة - حلقة نقاش - اختبار قصير	15/11/2025
الأسبوع 8	محاضرة - حلقة نقاش - اختبار قصير	22/11/2025
الأسبوع 9	محاضرة - حلقة نقاش - اختبار قصير	29/11/2025
الأسبوع 10	محاضرة - حلقة نقاش - اختبار قصير	06/12/2025
الأسبوع 11	محاضرة - حلقة نقاش - اختبار قصير	13/12/2025
الأسبوع 12	حلقة نقاش- مراجعة شاملة	20/12/2025
الأسبوع 13	بداية الاختبارات النهائية	27/12/2025
نهاية الدراسة	نهاية الاختبارات النهائية	03/01/2026

الاعمال وتوزيع درجات الفصل الدراسي الثالث 2025 لمرحلتى البكالوريوس والماجستير

الأعمال	توزيع الدرجات - 100%
محاضرة مُسجلة أسبوعيًا السبت من كل أسبوع	حضور المحاضرة وحل الأسئلة المصاحبة
اختبار قصير مُصاحب للمحاضرة بشكل أسبوعي	8 درجات لكل اختبار قصير بمجموع 80%
حلقة نقاش افتراضية أسبوعية لمناقشة محتوى المحاضرة المُسجلة	الحضور اختياري
الاختبار النهائي	20%

يتم احتساب الغياب من خلال حل الطالب للاختبار القصير المُصاحب للمحاضرة المُسجلة الأسبوعية، وفي حال تغيب الطالب عن 4 اختبارات قصيرة يؤدي هذا إلى الحرمان من الاختبار.

آخر موعد للاعتذار عن أي اختبار قصير يكون قبل إغلاق موعد الاختبار مع إرفاق الدلائل الثبوتية لأي أعذار قهرية أو مرضية عبر نموذج الأعذار عن اختبار قصير عبر منصة (SIS).

آخر موعد للاعتذار عن الاختبار النهائي يكون قبل موعد عقد الاختبار مع إرفاق الدلائل الثبوتية لأي عذر قهري أو طبي عبر نموذج الأعذار عن اختبار نهائي عبر منصة (SIS)، ولن يتم احتساب أي أعذار بعد نهاية الموعد.

يحق لإدارة الجامعة مراعاة بعض الظروف القهرية.

منهجية التدريس

يتم تقديم محاور البرنامج باستخدام المحاضرات المسجلة وحلقات النقاش عن بعد والتي يتم خلالها مناقشة جميع المحاضرات التي تم تسجيلها على المنصة بالإضافة إلى الإجابة عن استفساراتكم.

يتم تحقيق نتائج التعلم المستهدفة من خلال النشاطات والاستراتيجيات التدريسية الآتية:

- المحاضرات.
- الاختبارات القصيرة. (في كل أسبوع اختبار قصير من ثماني درجات وثمانية أسئلة).
- الامتحان النهائي (20 سؤال لكل سؤال درجة واحدة = 20 درجة).

Course Description

- This module introduces fundamental concepts in computer and network security.
- enabling the identification of vulnerabilities and the selection and implementation of suitable mitigation technologies.
- Throughout this module you'll learn about securing data through the use of cryptography, operating system security and multi-user environments, creating secure programs, state-of-the-art methods for identifying potential threats, and legal and ethical issues surrounding computer security.

Introduction to Cybersecurity

- Cybersecurity is the practice of protecting systems, networks, and data from attacks, damage, or unauthorized access.
- It combines people, processes, and technology to defend against threats like phishing, malware, and ransomware.

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.

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)

- Finite fields and modular arithmetic form the math backbone of cryptography.
- They are essential for algorithms like AES, RSA, and elliptic curve cryptography.

Advanced Encryption Standard (AES)

- AES is the global encryption standard, based on substitution–permutation networks.
- It supports key sizes of 128, 192, and 256 bits and secures most fintech systems today.

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.

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).

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

"That wraps up our introduction to this course. 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. I'm excited to start this journey with you."



Thank you!