Master Degree Curriculum for

Cybersecurity Program

Course Descriptions

King Hussein School of Computing Sciences
Princess Sumaya University for Technology
Cybersecurity Department

Prepared By
Dr. Mustafa Al-Fayoumi
Dr. Qasem Abu Alhaija
Dr. Khaled Mahmoud

2023-2024

Courses Indexing

Appendix A : Course Description/Mandatory Courses

Course No.	**15710**	**15710**	**الرقم**
Course Name	**Advanced Cryptography**	التشفير المتقدم	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course aims to introduce the mathematical principles of cryptography and its application to computer-network security services and mechanisms. Topics include: basic concepts in cryptography, mathematical background, Symmetric-key cryptography, such as block ciphers, stream ciphers, and cryptographic hash functions, including widely-used algorithms like AES, MD5 and SHA. Public-key cryptography, including key exchange algorithms like Diffie-Hellman, public-key encryption schemes like RSA, ElGamal, Elliptic curve Cryptosystems, and digital signature algorithms like Digital Signature Algorithm (DSA), ElGamal signature schemes, ECDSA. Cryptanalysis: Attacks on cryptosystems, cryptanalysis techniques, and key management. Cryptanalysis: Attacks on cryptosystems, cryptanalysis techniques: Attacks against private key ciphers: (Differential attack, Linear attack, and Man-in-the-middle attack), Attacks against public key ciphers (Pollard's p-1 and rho methods, quadratic sieve, and number field sieve). Introduction to post-quantum cryptography and its implications for current cryptographic systems. By the end of the course, students will have a solid understanding of the principles and practices of cryptography and will be able to design, implement, and analyze cryptographic algorithms for secure communications.

يهدف هذه المساق إلى تقديم المبادئ الرياضية للتشفير وتطبيقها على خدمات وآليات أمان شبكات الحاسوب. تتضمن الموضوعات: المفاهيم الأساسية في التشفير، الخلفية الرياضية، التشفير ذو المفتاح المتماثل، مثل تشفير المربعات وتشفير التدفق ووظائف التجزئة الشفرية، بما في ذلك خوارزميات شهيرة مثل AES و MD5 و SHA. التشفير ذو المفتاح العام، بما في ذلك خوارزميات تبادل المفتاح مثل ديفي هيلمان، مخططات التشفير ذات المفتاح العام مثل RSA و ElGamal ومنظومات المنحنى البيضاوي، وخوارزميات التوقيع الرقمي التوقيع الرقمي مثل خوارزمية التوقيع الرقمي(DSA) ، مخططات التوقيع (ElGamal)، (ECDSA). تحليل الشفرات: هجمات على أنظمة التشفير، تقنيات التحليل البديهي، وإدارة المفاتيح. التحليل البديهي: هجمات على أنظمة التشفير، تقنيات التحليل البديهي: هجمات ضد تشفيرات المفتاح الخاص: (الهجوم التفاضلي، الهجوم الخطي، وهجوم الوسيط)، هجمات ضد تشفيرات المفتاح العام) طرق Pollard's p-1 ورو، المنخل التربيعي، ومنخل مجال الأرقام .(مقدمة إلى التشفير ما بعد الكم وآثاره على أنظمة التشفير الحالية. مع نهاية هذا المقرر، سيكون لدى الطلاب فهم قوي لمبادئ وممارسات التشفير وسيكونون قادرين على تصميم وتنفيذ وتحليل خوارزميات التشفير للاتصالات الآمنة.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15711**	**15711**	**الرقم**
Course Name	**Digital Forensics Investigation (DFI)**	**تحقيقات الأدلة الرقمية**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

In this cybercrime course, students will become familiar with the basics of solving cybercrimes. By learning how to identify, protect and gather evidence, retrieve data, prepare crime reports and present information in courts, students master the correct methods for investigating cybercrimes so they can be solved and prosecuted. Students read case studies to become familiar with cybercrime scene investigation techniques. Techniques and tools used to build and solve cybercrime cases are presented and analyzed. Also, the requirements for conducting a cybercrime investigation through lecture, practical exercises, scenarios and case studies are presented. Students will learn the processes, techniques, specialized documentation, and legal guidelines necessary to investigate a computer crime.

هذا المساق سيمكن الطلاب من الإلمام بأساسيات حل الجرائم الحاسوبية وذلك من خلال تعلم كيفية تحديد وحماية وجمع الأدلة، واسترجاع البيانات، واعداد التقارير والمعلومات عن الجريمة الرقمية للمساعدة في تقديمها للمحاكم وذلك بإتباع الأساليب الصحيحة للتحقيق في جرائم الانترنت بحيث يمكن حلها ومحاكمة مرتكبيها. قراءة الدراسات المتخصصة للتعرف على تقنيات التحقيق في مسرح الجريمة الرقمية التقنيات والأدوات المستخدمة لبناء وحل الجرائم الحاسوبية وتحليلها. أيضا، يتم تقديم الاحتياجات اللازمة لإجراء التحقيق في الجريمة الرقمية من خلال المحاضرات والتمارين العملية، والسيناريوهات ودراسات الحالة. سوف يتعلم الطلاب العمليات والتقنيات والوثائق المتخصصة، والمبادئ التوجيهية القانونية اللازمة للتحقيق في الجرائم الحاسوبية

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15720**	**15720**	**الرقم**
Course Name	**Advanced Network Security**	**أمن الشبكات المتقدم**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	**15710**	**15710**	**المتطلب السابق**
Co-requisite	**----------**	**----------**	**المتطلب المرافق**

This course covers essential topics in data communication and network security. Topics covered include a review of data communication and networking concepts, network models, internetworking (addressing, protocols, forwarding, and routing), process-to-process delivery and protocols (UDP/TCP) congestion control, quality of service, network access control, cloud security, transport-level security, wireless network security, IP security, intruders and malicious software/attacks, firewalls, security for internet of things, network attacks encoding and analysis and selected topics in network security. Paper summarization and presentation, as well as design/modeling project, will be conducted to comprehend the course materials and ideas fully.

يغطي هذا المساق الموضوعات الأساسية في مجالات اتصالات البيانات وأمان الشبكات. تتضمن الموضوعات المغطاة مراجعة لمفاهيم اتصالات البيانات والشبكات، نماذج الشبكات، التواصل بين الشبكات (العنونة، البروتوكولات، التوجيه والتوصيل)، تسليم العمليات من وإلى العمليات والبروتوكولات (UDP/TCP)، التحكم في الازدحام، جودة الخدمة، التحكم في الوصول إلى الشبكة، أمان السحابة، أمان المستوى النقل، أمان الشبكة اللاسلكية، أمان IP، المتطفلون والبرامج الخبيثة/الهجمات، جدران الحماية، الأمان لإنترنت الأشياء، ترميز هجمات الشبكة وتحليلها وموضوعات مختارة في أمان الشبكات. سيتم إجراء تلخيص وعرض الأوراق البحثية، بالإضافة إلى مشروع التصميم/النمذجة، لفهم المواد الدراسية والأفكار بشكل كامل. في نهاية هذا المقرر من المتوقّع أن يمتلك الطلاب المهارات والمعرفة اللازمة في أمن الشبكات والمراقبة اللازمة للكشف عن المهاجمين وحماية الشبكة منهم.

Head of the Department

Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15750**	**15750**	**الرقم**
Course Name	**Cyber Threat Intelligence**	**التهديد السيبراني الذكي**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course aims to familiarize students with computational intelligence techniques and adopt them in the system (i.e., network) hardening/defense and anomaly detection (implementing IDS/IPS). Topics include an introduction to artificial intelligence (AI), neural networks, fuzzy logic systems, machine learning algorithms, threat/risk identification, behavior, assessment and analysis, data/attack analytics, capturing network traffic Wireshark tool, security intelligence, performance measures (system metrics), and threat hunting. This course introduces the concept of evading and poisoning intelligent detection systems that provide improved network traffic monitoring/analysis, help minimize exposure (attack surface and vectors), and improve system availability.

يهدف هذا المساق إلى تعريف الطلاب بتقنيات الذكاء الحوسبي وتبنيها في تقوية/الدفاع عن النظام (أي الشبكة) واكتشاف التشوهات) تنفيذ نظام الكشف عن الاختراق .(IDS/IPS تتضمن الموضوعات مقدمة إلى الذكاء الاصطناعي(AI) ، الشبكات العصبية، أنظمة المنطق الضبابي، خوارزميات التعلم الآلي، تحديد الأهداف/المخاطر، السلوك، التقييم والتحليل، تحليلات البيانات/الهجمات، التقاط حركة مرور الشبكة باستخدام أداةWireshark ، الذكاء الأمني، مقاييس الأداء (مقاييس النظام)، وصيد التهديدات. يقدم هذا المقرر مفهوم تجنب وتسميم أنظمة الكشف الذكية التي توفر رصد وتحليل محسّن لحركة مرور الشبكة، وتساعد في تقليل التعرض (سطح الهجوم والمتجهات)، وتحسين توفر النظام.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15760**	**15760**	**الرقم**
Course Name	**Secure Software Development**	بناء البرمجيات الامنة	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course teaches students how to integrate security into software development processes, covering topics such as secure software development lifecycle models and methodologies, security requirements engineering, secure design principles and patterns, secure coding practices, including common programming vulnerabilities (e.g., buffer overflows, SQL injection, and cross-site scripting), mitigation techniques, and secure coding standards., security testing and validation, and secure deployment and maintenance. Industry best practices, such as OWASP Top Ten and IEEE "Avoiding the Top 10 Software Security Design Flaws", are also covered. Students will gain the knowledge and skills needed to design and develop secure software systems, reducing the risks associated with common vulnerabilities and design flaws. The course also includes practical experience in applying Secure Systems Development principles to real-world scenarios. By the end of the course, students will have the knowledge and skills needed to design and develop secure software systems, effectively reducing the risks associated with common vulnerabilities and design flaws. They will also gain practical experience in applying Secure Systems Development principles to real-world scenarios.

يهدف هذا المساق الى تعليم الطلاب كيفية دمج الأمن في عمليات تطوير البرمجيات، وتغطي موضوعات مثل نماذج ومنهجيات دورة حياة تطوير البرمجيات الآمنة، وهندسة متطلبات الأمان، ومبادئ وأنماط التصميم الآمن، وممارسات التشفير الآمنة، بما في ذلك الثغرات الأمنية الشائعة في البرمجة (على سبيل المثال، فيضان المخزن المؤقت، و SQL الحقن، والبرمجة عبر المواقع)، وتقنيات التخفيف، ومعايير الترميز الآمن، والاختبار الأمني والتحقق من الصحة، والنشر الآمن والصيانة. تتم أيضًا تغطية أفضل ممارسات الصناعة، مثل (OWASP Top Ten) و (IEEE)"تجنب أفضل 10 عيوب في تصميم أمان البرامج". سيكتسب الطلاب المعرفة والمهارات اللازمة لتصميم وتطوير أنظمة برمجية آمنة، مما يقلل من المخاطر المرتبطة بنقاط الضعف الشائعة وعيوب التصميم. يتضمن المساق أيضًا خبرة عملية في تطبيق مبادئ تطوير الأنظمة الآمنة على سيناريوهات العالم الحقيقي. بحلول مه نهاية المساق، سيكون لدى الطلاب المعرفة والمهارات اللازمة لتصميم وتطوير أنظمة برمجية آمنة، مما يقلل بشكل فعال من المخاطر المرتبطة بنقاط الضعف الشائعة وعيوب التصميم. سيكتسبون أيضًا خبرة عملية في تطبيق مبادئ تطوير الأنظمة الآمنة على سيناريوهات العالم الحقيقي.

Head of the Department

Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15780**	**15780**	**الرقم**
Course Name	**Legal governance and Compliance**	**الحوكمة القانونية والامتثال**	**اسم المقرر**
Credit Hours	**3**	3	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course provides an overview of the policy, legal, ethics, and compliance issues that are relevant to cybersecurity professionals. The course will cover the following topics: Best practices of work ethics in the field of cybersecurity for organizations and individuals, issues related to the ethics and practices of using social media platforms, national and international legislation to combat cybercrimes, judicial authorities, agreements, treaties and international organizations related to cybersecurity, compliance frameworks and standards: National and international cybersecurity standards and controls (e.g. Cybersecurity Framework for Jordan Banking Sector and Cybersecurity Controls issued by the National Cyber Security Center, HIPAA, ISO 27001, PCI DSS, SOX), international cybersecurity law and policy, incident response and reporting requirements, privacy and data protection legislation and regulations (e.g. GDPR), intellectual property protection legislation and regulations, guidelines and best practices in recent trends (e.g. BYOD, Internet of Things protection guidelines), best practices for aligning with cybersecurity legislation, controls and standards.

يقدم هذا المساق نظرة عامة على قضايا السياسة والقانون والأخلاق والامتثال ذات الصلة بمتخصصي الأمن السيبراني. سيغطي المقرر المواضيع التالية: أفضل ممارسات أخلاقيات العمل في مجال الأمن السيبراني للمنظمات والأفراد، القضايا المتعلقة بأخلاقيات وممارسات استخدام منصات التواصل الاجتماعي، التشريعات الوطنية والدولية لمكافحة الجرائم الإلكترونية، السلطات القضائية، الاتفاقيات والمعاهدات والمنظمات الدولية ذات الصلة بالأمن السيبراني، أطر الامتثال والمعايير: معايير وضوابط الأمن السيبراني الوطنية والدولية (مثل إطار الأمن السيبراني للقطاع المصرفي الأردني وضوابط الأمن السيبراني الصادرة عن المركز الوطني للأمن السيبراني)، HIPAA، ISO 27001، (PCI DSS، قانون الأمن السيبراني الدولي والسياسات، الاستجابة للحوادث ومتطلبات الإبلاغ، تشريعات ولوائح حماية الخصوصية والبيانات (مثل القانون العام لحماية البيانات)، تشريعات ولوائح حماية الملكية الفكرية ، المبادئ التوجيهية وأفضل الممارسات في الاتجاهات الحديثة (مثل BYOD ، وإرشادات حماية إنترنت الأشياء)، وأفضل الممارسات للمواءمة مع تشريعات وضوابط ومعايير الأمن السيبراني.

Head of the Department

Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15781**	**15781**	**الرقم**
Course Name	**Information systems risk management**	**إدارة مخاطر أنظمة المعلومات**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course introduces information systems risk management, including risk identification, risk assessment and analysis, insider threats, risk measurement and evaluation models and methodologies, and risk control. The course will cover the following topics: risk management lifecycle and steps, cyber risk assessment and analysis methodologies, methodologies for measuring and evaluating cyber risks, cyber risk management standards and frameworks, cyber risk management processes across levels in the organization, cyber risks mitigation economics, transference, acceptance and mitigation of cyber risks, cyber risks policies for technologies, risk procedures, and standards, individuals and entities, characteristics of organizations that influence cyber risk, analysis and management, communication of cyber risks, and overview of business continuity and disaster recovery, including business impact analysis, disaster recovery planning, and testing. By the end of the course, students will have gained a strong understanding of information systems risk management and be able to apply risk management methodologies and frameworks to manage risks to information systems in their organizations

يقدم هذا المساق مقدمة لإدارة مخاطر نظم المعلومات، بما في ذلك تحديد المخاطر، وتقييم المخاطر وتحليلها، والتهديدات الداخلية، ونماذج ومنهجيات تقييم وتقييم المخاطر، ومراقبة المخاطر. سيغطي هذا المقرر الموضوعات التالية: دورة حياة إدارة المخاطر وخطواتها ، ومنهجيات تقييم وتحليل المخاطر السيبرانية، ومنهجيات قياس وتقييم المخاطر السيبرانية، ومعايير وأطر إدارة المخاطر الإلكترونية، وعمليات إدارة المخاطر الإلكترونية عبر المستويات في المؤسسة، واقتصاديات التخفيف من المخاطر السيبرانية ونقل وقبول وتخفيف المخاطر الإلكترونية وسياسات المخاطر الإلكترونية للتقنيات وإجراءات ومعايير المخاطر والأفراد والكيانات وخصائص المنظمات التي تؤثر على المخاطر الإلكترونية والتحليل والإدارة والإبلاغ عن المخاطر الإلكترونية ونظرة عامة على استمرارية الأعمال والكوارث التعافي، بما في ذلك تحليل تأثير الأعمال، وتخطيط التعافي من الكوارث، والاختبار. مع نهاية هذا المقرر، سيكون الطلاب قد اكتسبوا فهمًا قويًا لإدارة مخاطر أنظمة المعلومات وسيكونون قادرين على تطبيق منهجيات وأطر إدارة المخاطر لإدارة المخاطر على أنظمة المعلومات في مؤسساتهم.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15790**	**15790**	**الرقم**
Course Name	**Seminar**	**ندوه وحلقة دراسية**	**اسم المقرر**
Credit Hours	**1**	**1**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course is designed to provide a comprehensive understanding of the research process, various research designs, and data collection and analysis techniques applicable to their field of study. The course emphasizes the development of critical thinking and analytical skills necessary for conducting independent research and evaluating research findings in the context of information security and digital criminology. In this course, the students will explore a range of research methods, including qualitative, quantitative, and mixed-methods approaches. Topics include: research design, literature review, research questions and hypotheses formulation, sampling techniques, data collection methods (e.g., surveys, interviews, observations, and experiments), and data analysis strategies (e.g., descriptive and inferential statistics, content analysis, and thematic analysis). At the end of the course, students will have a clear understanding of research processes and methodologies, allowing them to effectively plan, execute, and assess studies, while contributing to the advancement of knowledge in their field.

تم تصميم هذا المساق لتوفير فهم شامل لعملية البحث وتصاميم البحث المختلفة وتقنيات جمع وتحليل البيانات المناسبة لمجال دراستهم. يركز المقرر على تطوير مهارات التفكير النقدي والتحليلي اللازمة لإجراء البحوث المستقلة وتقييم نتائج البحث في سياق أمن المعلومات والجريمة الرقمية. في هذا المقرر، سيتعرف الطلاب على مجموعة من طرق البحث، بما في ذلك الطرق النوعية والكمية والمنهجية المختلطة. تشمل الموضوعات: تصميم البحث، مراجعة الأدب، صياغة أسئلة البحث والفرضيات، تقنيات العينة، طرق جمع البيانات (مثل الاستطلاعات والمقابلات والملاحظات والتجارب)، واستراتيجيات تحليل البيانات (مثل الإحصاءات الوصفية والاستدلالية وتحليل المحتوى والتحليل الموضوعي). بنهاية المقرر، سيكون لدى الطلاب فهم واضح لعمليات البحث والمنهجيات، مما يتيح لهم التخطيط والتنفيذ وتقييم الدراسات بفعالية، مع المساهمة في تطور المعرفة في مجالهم.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15791**	**15791**	**الرقم**
Course Name	**Project**	**مشروع**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

In this course, students will conduct an individual study to demonstrate their ability to formulate, investigate, and analyze a problem in the field of information systems security. The project proposal must be approved by a major professor and/or supervisory committee. The course will emphasize the development of research skills, including research design, data collection, and analysis. Students will be expected to produce a written report and deliver an oral presentation of their findings. The project document should be written with direction from a major professor and/or supervisory committee, and in accordance with the description provided to students. Upon completion, both the project and the document must be successfully defended to the department in an open forum, with approval from the major professor and/or supervisory committee. This course provides students with an opportunity to apply their knowledge and skills in information systems security to a comprehensive project, demonstrating their mastery of the subject matter. The project provides valuable experience in independent research, critical thinking, and problem-solving skills, which will be beneficial to their future careers in information systems security.

في هذا المساق، سيقوم الطلاب بإجراء دراسة فردية لإثبات قدرتهم على صياغة مشكلة والتحقيق فيها وتحليلها في مجال أمن نظم المعلومات. يجب أن تتم الموافقة على اقتراح المشروع من قبل أستاذ رئيسي و / أو لجنة إشراقية. سيركز المساق على تطوير مهارات البحث، بما في ذلك تصميم البحث وجمع البيانات والتحليل. يُتوقع من الطلاب إعداد تقرير مكتوب وتقديم عرض شفوي لنتائجهم. يجب كتابة وثيقة المشروع بتوجيه من أستاذ رئيسي و / أو لجنة إشراف، ووفقًا للوصف المقدم للطلاب. عند الانتهاء، يجب الدفاع عن المشروع والوثيقة بنجاح أمام لجنة تحدد بالتنسيق من القسم، بموافقة الأستاذ الرئيسي و / أو اللجنة الإشراقية. يوفر هذا المساق للطلاب فرصة لتطبيق معارفهم ومهاراتهم في مجال أمن نظم المعلومات لمشروع شامل، مما يدل على إتقانهم للموضوع. يوفر المشروع خبرة قيمة في البحث المستقل والتفكير النقدي ومهارات حل المشكلات ، والتي ستكون مفيدة لمهنهم المستقبلية في أمن أنظمة المعلومات.

Head of the Department

Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15799**	**15799**	**الرقم**
Course Name	**Thesis**	**الرسالة**	**اسم المقرر**
Credit Hours	9	**9**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course requires students to complete, document, present, and defend a thesis under the supervision of a faculty member in the fields of Information Systems Security and Digital Criminology. The thesis must be equivalent to 9 credit hours and describe research work of publishable quality. Upon completion of 15 credits, a student is eligible to register for thesis. The thesis defense will be before a committee, consisting of the supervisor and at least three other faculty members, one of whom must be from outside the university. The defense will be open to all interested faculty and students. The thesis should demonstrate the student's ability to conduct independent research and contribute to the field of Information Systems Security. The thesis should also show the student's mastery of the relevant literature and research methods. The course will cover topics such as research design, data collection and analysis, literature review, and academic writing. Students will be expected to work closely with their faculty supervisor to develop a research question, plan and execute their research, and write a high-quality thesis. By the end of the course, students will have completed a substantial research project that demonstrates their expertise in Information Systems Security and prepares them for further research or professional work in the field.

يتطلب هذا المساق من الطلاب الانتهاء من إعداد وثائق وعرض ودفاع عن رسالة الماجستير تحت إشراف عضو هيئة التدريس في مجالات أمن نظم المعلومات والجريمة الرقمية. يجب أن تكون رسالة الماجستير مكافئة لـ 9 ساعات دراسية وتصف أعمال بحثية قابلة للنشر. عند الإنتهاء من 15 ساعة دراسية، يحق للطالب التسجيل في رسالة الماجستير. سيتم عقد جلسة دفاع عن رسالة الماجستير أمام لجنة مؤلفة من المشرف وثلاثة أعضاء هيئة تدريس، واحد منهم على الأقل خارج الجامعة، في المجالات ذات الصلة. ستكون جلسة الدفاع مفتوحة أمام جميع أعضاء هيئة التدريس والطلاب المهتمين. يجب أن تظهر رسالة الماجستير قدرة الطالب على إجراء بحوث مستقلة والمساهمة في مجال أمن نظم المعلومات. كما يجب أن تظهر رسالة الماجستير إتقان الطالب للأدبيات وطرق البحث اللازمة. ستغطي الرسالة موضوعات مثل تصميم البحث وجمع البيانات وتحليلها ومراجعة الأدبيات والكتابة الأكاديمية. من المتوقع أن يعمل الطلاب عن كثب مع مشرفهم في هيئة التدريس لتطوير سؤال البحث وتخطيط وتنفيذ بحثهم وكتابة رسالة الماجستير عالية الجودة. عند الانتهاء من مساق الرسالة، سيكون لدى الطلاب مشروع بحث كبير يظهر خبرتهم في أمن نظم المعلومات ويجهزهم للعمل البحثي أو المهني في المجال.

Head of the Department

Name: Dr. Mustafa Al-Fayoumi	**Signature:** .....
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Appendix B : Course Description/Elective Courses

Course No.	**15713**	**15713**	**الرقم**
Course Name	**Advanced Digital Forensic**	**الأدلة الرقمية المتقدمة**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	**15711**	**15711**	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course aims to provide a comprehensive understanding of the principles, techniques, and tools used in the collection, preservation, analysis, and presentation of digital evidence. Topics include: Legal and ethical considerations in digital forensics, including search and seizure, chain of custody, admissibility of digital evidence, and privacy concerns. Digital forensics methodologies and best practices, including the digital forensics process, evidence handling procedures, and documentation standards. File systems and data storage analysis, including file system structures, file carving, data recovery, and timestamp analysis. Network forensics, including network traffic analysis, log analysis, intrusion detection and prevention systems, and network-based evidence collection techniques. Memory forensics, including volatile data collection, malware analysis, and memory-based evidence analysis. Mobile and IoT device forensics, including data extraction techniques, mobile operating system analysis, and forensic challenges in IoT environments. Incident response and digital forensics integration, including the role of digital forensics in incident response, threat hunting, and cyber threat intelligence.

يهدف هذا المساق إلى توفير فهم شامل للمبادئ والتقنيات والأدوات المستخدمة في جمع وحفظ وتحليل وعرض الأدلة الرقمية. تشمل الموضوعات: الاعتبارات القانونية والأخلاقية في الطب الشرعي الرقمي، بما في ذلك البحث والمصادرة، وسلسلة العهدة، وقبول الأدلة الرقمية، ومخاوف الخصوصية. منهجيات الطب الشرعي الرقمي وأفضل الممارسات، بما في ذلك عملية الطب الشرعي الرقمي، وإجراءات التعامل مع الأدلة، ومعايير التوثيق. تحليل أنظمة الملفات وتخزين البيانات، بما في ذلك هياكل نظام الملفات، ونحت الملفات، واستعادة البيانات، وتحليل الطابع الزمني. الطب الشرعي للشبكة، بما في ذلك تحليل حركة مرور الشبكة، وتحليل السجل، وأنظمة كشف التسلل والوقاية منه، وتقنيات جمع الأدلة القائمة على الشبكة. الطب الشرعي للذاكرة، بما في ذلك جمع البيانات المتطايرة، وتحليل البرامج الضارة، وتحليل الأدلة القائم على الذاكرة. التحليلات الجنائية للأجهزة المحمولة وأجهزة إنترنت الأشياء، بما في ذلك تقنيات استخراج البيانات وتحليل نظام تشغيل الأجهزة المحمولة والتحديات الجنائية في بيئات إنترنت الأشياء. الاستجابة للحوادث وتكامل الأدلة الجنائية الرقمية ، بما في ذلك دور الأدلة الجنائية الرقمية في الاستجابة للحوادث ، والبحث عن التهديدات ، وذكاء التهديدات الإلكترونية.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15714**	**15714**	**الرقم**
Course Name	**Advanced Data Integrity and Authentication**	**سلامة البيانات والمصادقة المتقدم**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	**15710**	**15710**	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course aims to provide an in-depth exploration of data integrity and authentication, including the principles and best practices for ensuring data accuracy, completeness, and authenticity. The course will cover the following topics: Overview of data integrity and authentication. data integrity techniques including data redundancy, checksums, and error-correcting codes, message authentication codes (HMAC, CBC-MAC), digital signatures including blind signatures, group signatures, and ring signatures. authenticated encryption and hash trees. Authentication techniques including techniques for authenticating data and users, authentication strength (passwords authentication, cryptographic tokens, biometrics authentication, multifactor authentication, and One-Time passwords and knowledge-based authentication). Password attack techniques: dictionary attack, brute force, rainbow table, phishing, and social engineering attacks. Password storage techniques: cryptographic hash functions, collision resistance, salting, iteration count and password-based key derivation. Advanced protocols: Zero-knowledge proofs, Secret sharing, Commitment, Oblivious transfer, Secure multiparty computation and secure function evaluation. Verification analysis (Formal and Informal). By the end of the course, students will have gained practical experience in ensuring data integrity and authenticity and will be able to design, implement, and evaluate data protection solutions for various applications.

يوفر هذا المساق الى توفير استكشاف متعمق لسلامة البيانات والمصادقة عليها، بما في ذلك المبادئ وأفضل الممارسات لضمان دقة البيانات واكتمالها ومصداقيتها. سيغطي المقرر المواضيع التالية: نظرة عامة على تكامل البيانات والمصادقة. تقنيات تكامل البيانات بما في ذلك تكرار البيانات والمجاميع الاختبارية ورموز تصحيح الأخطاء ورموز مصادقة الرسائل (CBC-MAC , MAC)، التوقيعات الرقمية بما في ذلك التوقيعات العمياء، والتوقيعات المجموعاتية، والتوقيعات الحلقية. التشفير المصدق وأشجار التجزئة. تقنيات لمصادقة، بما في ذلك تقنيات لمصادقة البيانات والمستخدمين، قوة المصادقة - مصادقة كلمات المرور، الرموز المميزة للتشفير، مصادقة القياسات الحيوية، المصادقة متعددة العوامل، وكلمات المرور لمرة واحدة والمصادقة المستندة إلى المعرفة. تقنيات هجوم كلمة المرور: هجوم القاموس، هجوم القوة الغاشمة، هجوم جدول قوس قزح، التصيد الاحتيالي، الهندسة الاجتماعية. تقنيات تخزين كلمات المرور: بما في ذلك، وظائف التجزئة المشفرة ومقاومة الاصطدام والتمليح وعدد التكرار واشتقاق المفتاح المستند إلى كلمة المرور. البروتوكولات المتقدمة على سبيل المثال لا الحصر، البراهين والمعرفة الصفرية. تحليل التحقق (تحليل التحقق الرسمي، تحليل التحقق غير الرسمي). في نهاية هذا المقرر، سيكون الطلاب قد اكتسبوا خبرة عملية في ضمان سلامة البيانات ومصداقيتها وسيكونون قادرين على تصميم وتنفيذ وتقييم حلول حماية البيانات لمختلف التطبيقات.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15715**	**15715**	**الرقم**
Course Name	**Block chain Technology**	**تكنولوجيا البلوكشين**	**اسم المقرر**
C.H Dist.	**3**	**3**	**الساعات**
Pre-requisite	**15710**	**15710**	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

The course provides essential understanding and knowledge of Blockchain technology and its applications in various industries. Topics covered are divided into three parts; the first part covers cryptographic preliminaries including hash functions, digital signatures, and commitment schemes. The second part covers design and implementation principles of Blockchain including protocols, frameworks, transactions, platforms, consensus, permissions, smart contracts, privacy, scalability and security. The last part covers Blockchain use cases in financial services, supply chain management and governmental services.

يقدم هذا المساق الفهم الأساسي والمعرفة بتكنولوجيا Blockchain وتطبيقاتها في مختلف الصناعات. المواضيع التي يتم تناولها مقسمة إلى ثلاثة أجزاء ؛ يغطي الجزء الأول مقدمات التشفير بما في ذلك وظائف التجزئة والتوقيعات الرقمية وخطط الالتزام. يغطي الجزء الثاني مبادئ تصميم وتنفيذ Blockchain بما في ذلك البروتوكولات والأطر والمعاملات والمنصات والتوافق والأذونات والعقود الذكية والخصوصية وقابلية التوسع والأمان. يغطي الجزء الأخير حالات استخدام Blockchain في الخدمات المالية وإدارة سلسلة التوريد والخدمات الحكومية.

Head of the Department

Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15721**	**15721**	**الرقم**
Course Name	**Wireless and Mobile Security**	امن الشبكات اللاسلكية والمتنقلة	**اسم المقرر**
C.H Dist.	**3**	**3**	**الساعات**
Pre-requisite	**15720**	**15720**	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course aims to provide a comprehensive understanding of the principles, techniques, and challenges associated with securing wireless networks and mobile devices. Topics include: Introduction to wireless and mobile security, and its role in the broader field of information security and cybersecurity. Wireless network security, including security protocols (e.g., WEP, WPA, WPA2, WPA3), authentication and encryption mechanisms, and wireless intrusion detection and prevention systems. Cellular network security, including GSM, CDMA, 3G, 4G, and 5G security mechanisms, as well as challenges and vulnerabilities associated with these technologies. Mobile device security, including mobile operating systems (e.g., Android, iOS), mobile device management (MDM), mobile application security, and secure data storage on mobile devices. Mobile application security, including secure coding practices, application sandboxing, and runtime application self-protection (RASP) techniques. Bluetooth, NFC, and RFID security, including threats, vulnerabilities, and countermeasures associated with these wireless communication technologies. IoT and wearable device security, including unique challenges and best practices for securing IoT devices, embedded systems, and wearable technology.

يهدف هذا المساق إلى توفير فهم شامل للمبادئ والتقنيات والتحديات المرتبطة بتأمين الشبكات اللاسلكية والأجهزة المحمولة. تشمل الموضوعات: مقدمة في الأمن اللاسلكي والمتنقل، ودوره في المجال الأوسع لأمن المعلومات والأمن السيبراني. أمان الشبكة اللاسلكية، بما في ذلك بروتوكولات الأمان (مثل WEP و WPA و WPA2 و WPA3) وآليات المصادقة والتشفير وأنظمة الكشف عن التسلل اللاسلكي والوقاية منه. أمان الشبكة الخلوية، بما في ذلك آليات أمان GSM و CDMA و G3 و G4 و G5، بالإضافة إلى التحديات ونقاط الضعف المرتبطة بهذه التقنيات. أمان الجهاز المحمول، بما في ذلك أنظمة تشغيل الأجهزة المحمولة (مثل Android و iOS) وإدارة الأجهزة المحمولة (MDM) وأمن تطبيقات الهاتف المحمول وتخزين البيانات الآمن على الأجهزة المحمولة. أمان تطبيقات الأجهزة المحمولة، بما في ذلك ممارسات التشفير الآمنة ووضع الحماية للتطبيق وتقنيات الحماية الذاتية للتطبيقات في وقت التشغيل (RASP). أمان Bluetooth و NFC و RFID، بما في ذلك التهديدات ونقاط الضعف والإجراءات المضادة المرتبطة بتقنيات الاتصالات اللاسلكية هذه. أمان إنترنت الأشياء والأجهزة القابلة للارتداء ، بما في ذلك التحديات الفريدة وأفضل الممارسات لتأمين أجهزة إنترنت الأشياء والأنظمة المضمنة والتكنولوجيا القابلة للارتداء.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15722**	**15722**	**الرقم**
Course Name	**Cloud Computing Security**	**امن الحوسبة السحابة**	**اسم المقرر**
C.H Dist.	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course aims to provide a comprehensive understanding of the principles, techniques, and challenges associated with securing cloud computing environments and big data systems. Topics include: Introduction to cloud and big data security, Cloud computing security, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) security, as well as cloud deployment models (public, private, hybrid, and community clouds). Cloud security best practices and frameworks, including the Cloud Security Alliance (CSA) guidelines, NIST cloud security standards, and ISO/IEC 27017. Cloud security controls and mechanisms, including data encryption, access control, secure multi-tenancy, and secure cloud application development. Cloud security challenges and threats, including data breaches, insider threats, insecure APIs, and denial of service attacks. Big data security, including security and privacy considerations in big data processing, storage, and analytics. Big data security technologies and techniques, such as secure distributed computing, data anonymization, differential privacy, and homomorphic encryption.

يهدف هذا المساق إلى توفير فهم شامل للمبادئ والتقنيات والتحديات المرتبطة بتأمين بيئات الحوسبة السحابية وأنظمة البيانات الضخمة. تشمل الموضوعات: مقدمة إلى السحابة وأمن البيانات الضخمة، وأمن الحوسبة السحابية، بما في ذلك البنية التحتية كخدمة (IaaS)، والنظام الأساسي كخدمة (PaaS)، وأمن البرمجيات كخدمة (SaaS)، بالإضافة إلى نماذج نشر السحابة (السحابة العامة والخاصة والمختلطة والمجتمعية). أفضل ممارسات وأطر أمان السحابة، بما في ذلك إرشادات Cloud Security Alliance (CSA) ، ومعايير أمان السحابة NIST ، و ISO / IEC 27017. ضوابط وآليات أمان السحابة، بما في ذلك تشفير البيانات والتحكم في الوصول والتعددية الآمنة والتطبيق السحابي الآمن تطوير. تحديات وتهديدات أمان السحابة، بما في ذلك انتهاكات البيانات والتهديدات الداخلية وواجهات برمجة التطبيقات غير الآمنة وهجمات رفض الخدمة. أمان البيانات الضخمة، بما في ذلك اعتبارات الأمان والخصوصية في معالجة البيانات الضخمة وتخزينها وتحليلاتها. تقنيات وتقنيات أمان البيانات الضخمة ، مثل الحوسبة الموزعة الآمنة وإخفاء هوية البيانات والخصوصية التفاضلية والتشفير المتماثل.

Head of the Department

Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15723**	**15723**	**الرقم**
Course Name	**Multimedia Security**	**أمن الوسائط المتعددة**	**اسم المقرر**
C.H Dist.	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course will cover selected topics in multimedia security and privacy, including techniques for steganography, steganalysis, digital watermarking, multimedia encryption and authentication, digital rights management, multimedia content tampering and detection, deep fake methods and deep fake detection, and multimedia forensics.

سيغطي هذا المساق موضوعات مختارة متقدمة في أمن وخصوصية الوسائط المتعددة، بما في ذلك تقنيات إخفاء المعلومات، وتحليل إخفاء المعلومات، والعلامات المائية الرقمية، وتشفير الوسائط المتعددة والمصادقة عليها، وإدارة الحقوق الرقمية، والتلاعب في محتوى الوسائط المتعددة والكشف عنه، والأساليب المزيفة العميقة واساليب كشف المزيف العميق، وتحليل الأدلة الجنائية للوسائط المتعددة.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15730**	**15730**	**الرقم**
Course Name	**Malware Reverse Engineering**	**الهندسة العكسية للبرامج الضارة**	**اسم المقرر**
C.H Dist.	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course will introduce students to modern techniques in malware analysis through readings and hands-on interactive analysis of real-world samples. Topics include an overview of the computer system, X86 microprocessor architecture, assembly language (16-bit), addressing modes & machine codes, malware analysis primer, malware analysis in virtual machines, static malware analysis, dynamic malware analysis, reverse engineering (overview, X86 disassembly, the IDA Pro, recognizing C code constructs in assembly, analyzing malicious windows programs, X86 Debugging), malware behavior, malware encoding (obfuscation and encryption). After taking this course, the students will be equipped with the skills to analyze modern malware using static and dynamic analysis. Students will learn to analyze malicious software using reverse engineering concepts safely and thoroughly. This analysis aims to understand malicious software's behavior and potential security impacts.

سيتم تعريف الطلاب من خلال هذا المساق بالتقنيات الحديثة في تحليل البرامج الضارة من خلال القراءات والتحليل التفاعلي لعينات من العالم الحقيقي. وتتضمن المواضيع نظرة عامة على نظام الحاسوب، وهندسة معالجاتX86 ، ولغة التجميع (16 بت)، وطرق العنونة وأكواد الآلة، ومقدمة في تحليل البرامج الضارة، وتحليل البرامج الضارة في الآلات الافتراضية، وتحليل البرامج الضارة الثابت، وتحليل البرامج الضارة الديناميكي، وهندسة العكس)نظرة عامة، تفكيكX86 ، برنامجIDA Pro ، التعرف على بناء الأكواد C في التجميع، تحليل البرامج الخبيثة لنظام ويندوز، وتصحيح الأخطاء لـ (X86، وسلوك البرمجيات الضارة، وتشفير البرامج الضارة (إخفاء الأكواد والتشفير). وفي نهاية هذا المساق، سيتم تجهيز الطلاب بالمهارات اللازمة لتحليل البرامج الضارة الحديثة باستخدام التحليل الثابت والديناميكي. وسيتعلم الطلاب كيفية تحليل البرامج الضارة باستخدام مفاهيم هندسة العكس بطريقة آمنة وشاملة. ويهدف هذا التحليل إلى فهم سلوك البرامج الضارة وتحديد تأثيرات الأمن المحتملة.

Head of the Department

Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15732**	**15732**	**الرقم**
Course Name	**Introduction to Hardware Security and Trust**	**مقدمة في أمن الأجهزة المادية والموثوقية**	**اسم المقرر**
C.H Dist.	**3**	**3**	**الساعات**
Pre-requisite	**----------**	**----------**	**المتطلب السابق**
Co-requisite	**----------**	**----------**	**المتطلب المرافق**

This course will investigate various security and trust issues related to integrated circuits and systems during their design, manufacturing process, and field operation. A wide range of threats will be introduced, including piracy, reverse engineering, hardware Trojan insertion, side-channel attack, and invasive non-invasive attacks. Potential hardware and software-based countermeasures will be studied to detect and prevent these attacks. Implementation of design-time solutions like physically unclonable functions (PUFs), true random number generators (TRNG), security monitors, hardware obfuscation, and many others will be covered.

سيستكشف هذا المساق العديد من القضايا المتعلقة بأمان الدوائر المتكاملة والأنظمة خلال عملية التصميم والتصنيع والتشغيل الميداني. وسيتم تقديم مجموعة واسعة من التهديدات، بما في ذلك القرصنة، وهندسة العكس، وإدخال التروجانات الأجهزة، وهجوم جانبي، والهجمات المتداخلة وغير المتداخلة. وسيتم دراسة الحلول المحتملة بناءً على الأجهزة أو البرامج للكشف عن هذه الهجمات ومنعها. وسيتم تغطية تنفيذ حلول تصميم الوقت مثل الوظائف الفيزيائية غير القابلة للتكرار(PUFs) ، ومولدات الأرقام العشوائية الحقيقية(TRNG) ، ومراقبي الأمان، والتشويش على الأجهزة، وغير ذلك الكثير.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15733**	**15733**	**الرقم**
Course Name	**Cyber-Physical Systems and Security**	**أمن الأنظمة السيبرانية المادية**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course offers a rigorous and comprehensive introduction to the principles of design, specification, modeling, and analysis of cyber-physical systems. Both synchronous and asynchronous models for concurrent computation, continuous-time models for dynamical systems, and hybrid systems for integrating discrete and continuous evolution will be covered. The topics include safety and requirements, temporal logic, model checking, deductive verification, stability analysis for linear systems, and real-time scheduling algorithms. Besides, Challenges in Cyber-Physical Systems, Cyber-Physical Systems Security (CPSS): Concepts and Principles, Security Breaches and Defenses in CPS, Safe-AI based and Secure CPS (reinforcement learning), Attack detection and mitigation in CPS, IoT Security, Simulation-based projects, such as well as paper summarization and presentation, will be included.

يقدم هذا المساق مقدمة صارمة وشاملة لمبادئ التصميم والمواصفات والنمذجة وتحليل الأنظمة السيبرانية الفيزيائية. سيتم تغطية كل من النماذج المتزامنة وغير المتزامنة للحساب المتزامن ونماذج الوقت المستمر للأنظمة الديناميكية والأنظمة الهجينة لدمج التطور المنفصل والمستمر. تشمل الموضوعات السلامة والمتطلبات، والمنطق الزمني، وفحص النموذج، والتحقق الاستنتاجي، وتحليل الاستقرار للأنظمة الخطية، وخوارزميات الجدولة في الوقت الفعلي. إلى جانب ذلك ، التحديات في الأنظمة السيبرانية الفيزيائية ، وأمن الأنظمة السيبرانية الفيزيائية (CPSS): المفاهيم والمبادئ ، والانتهاكات الأمنية والدفاعات في CPS ، و CPS القائم على الذكاء الاصطناعي الآمن والآمن (التعلم المعزز) ، واكتشاف الهجمات والتخفيف من حدتها في CPS ، وأمن إنترنت الأشياء ، سيتم تضمين المشاريع القائمة على المحاكاة ، بالإضافة إلى تلخيص الورق والعرض التقديمي.

Head of the Department

Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15751**	**15751**	**الرقم**
Course Name	**Ethical Hacking Techniques**	**تقنيات القرصنة الأخلاقية**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course covers the most common methods used in computer and network hacking with the intention of learning how to better protect systems from such intrusions. These methods include reconnaissance techniques, system scanning, and system access by network and application level attacks, and denial of service attacks. Traffic analysis methods and tools will be studied in this course. Also, it covers the techniques for traffic filtering and monitoring, and intrusion detection.

هذا المساق يغطي الطرق الأكثر شيوعا في القرصنة والتسلل إلى الشبكات بغرض تعلم طرق لحماية النظم الحاسوبية من هذه القرصنات والتسللات. هذه الطرق تشمل الاستطلاع، مسح النظم، الدخول الى النظم عن طريق الهجوم على الشبكات أو التطبيقات وهجمات رفض الخدمة. كما يشمل هذا المساق دراسة طرق وأدوات تحليل الحركة في الشبكات وتنقيتها ومراقبتها إضافة إلى طرق كشف التسلل.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15784**	**15784**	**الرقم**
Course Name	**Cyber Resilience and Business Continuity**	**المرونة السيبرانية واستمرارية الأعمال**	**اسم المقرر**
C.H Dist.	**3**	**3**	**الساعات**
Pre-requisite			**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

In this course, students will learn the principles and best practices for ensuring cyber resilience and business continuity in the face of various cyber threats and incidents. Topics include: understanding the relationship between cybersecurity and business continuity, incident response planning (Anticipate, Detect and Mitigate), disaster recovery planning, crisis communication, and managing the human element in cyber incidents, business continuity (Contingency Planning, Incident Response, Emergency Response, Backup and Recovery). the implementation of effective backup strategies, and the importance of testing and refining these plans regularly. By the end of the course, students will have the knowledge and skills to develop, implement, and maintain comprehensive cyber resilience and business continuity strategies, effectively reducing downtime and mitigating the impact of cyber incidents on an organization's operations.

في هذا المساق، سيتعلم الطلاب المبادئ وأفضل الممارسات لضمان المرونة السيبرانية واستمرارية الأعمال في مواجهة التهديدات الإلكترونية المختلفة والحوادث. تتضمن الموضوعات: فهم العلاقة بين الأمن السيبراني واستمرارية الأعمال، التخطيط لاستجابة الحوادث (توقع، كشف وتقليل)، تخطيط استعادة الأعمال بعد الكوارث، الاتصال في أوقات الأزمات، وإدارة العنصر البشري في الحوادث السيبرانية، استمرارية الأعمال (التخطيط البديل، استجابة الحوادث، الاستجابة للطوارئ، النسخ الاحتياطي والاستعادة). تنفيذ استراتيجيات النسخ الاحتياطي الفعّالة، وأهمية اختبار وصقل هذه الخطط بانتظام. بنهاية المقرر، سيكون لدى الطلاب المعرفة والمهارات اللازمة لتطوير وتنفيذ وصيانة استراتيجيات شاملة للمرونة السيبرانية واستمرارية الأعمال، مما يقلل بفعالية من التوقف عن العمل ويقلل من تأثير الحوادث السيبرانية على عمليات المنظمة.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15792**	**15792**	**الرقم**
Course Name	**Special Topics in Cybersecurity**	**موضوعات خاصة في الأمن السيبراني**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق**

This course delves into specialized topics in the fields of information systems security and digital criminology, providing students with a comprehensive understanding of the latest advances, challenges, and methodologies. The course content is designed to adapt to the ever-evolving landscape of information security and digital criminology, addressing contemporary issues and cutting-edge research. Topics will be assigned by the department on evolving techniques and related topics to support the study plan and to encourage further research by students

يتعمق هذا المساق في موضوعات متخصصة في مجالات أمن نظم المعلومات وعلم الجريمة الرقمية، مما يوفر للطلاب فهمًا شاملاً لأحدث التطورات والتحديات والمنهجيات. تم تصميم محتوى الدورة للتكيف مع المشهد المتطور باستمرار لأمن المعلومات وعلم الجريمة الرقمي، ومعالجة القضايا المعاصرة والبحوث المتطورة. سيتم تحديد الموضوعات من قبل القسم حول التقنيات المتطورة والموضوعات ذات الصلة لدعم الخطة الدراسة وتشجيع المزيد من البحث من قبل الطلاب.

Head of the Department	
Name: Dr. Mustafa Al-Fayoumi	**Signature:** ……
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**

Course No.	**15793**	**15793**	**الرقم**
Course Name	**Current Emerging Trends in Cybersecurity**	**الاتجاهات الناشئة الحالية في مجال الأمن السيبراني**	**اسم المقرر**
Credit Hours	**3**	**3**	**الساعات**
Pre-requisite	----------	----------	**المتطلب السابق**
Co-requisite	----------	----------	**المتطلب المرافق***

This course provides an in-depth exploration of the ever-changing landscape of information security. Students will gain a comprehensive understanding of the various aspects and challenges in the field, without focusing on specific topics. The course will examine the implications of emerging trends for individuals, organizations, and society, while emphasizing the importance of staying current with the latest developments in information security. Topics will be assigned by the department on evolving techniques and related topics to support the study plan and to encourage further research by students

يوفر هذا المساق دراسة معمقة للمشهد المتغير باستمرار في مجال أمن المعلومات. سيحصل الطلاب على فهم شامل للجوانب المختلفة والتحديات في هذا المجال، دون التركيز على موضوعات محددة. سيتناول المقرر الدراسي تداعيات الاتجاهات الناشئة على الأفراد والمنظمات والمجتمع، مع التأكيد على أهمية البقاء على اطلاع بأحدث التطورات في مجال أمن المعلومات. سيتم تحديد الموضوعات من قبل القسم حول التقنيات المتطورة والموضوعات ذات الصلة لدعم الخطة الدراسة وتشجيع المزيد من البحث من قبل الطلاب.

Head of the Department

Name: Dr. Mustafa Al-Fayoumi	**Signature:** .....
Session number/Academic year: (1) 20-2022/2023	**Date: 05/07/2023**