كلية : الهندسة وعلوم الحاسب **قسم هندسة الحاسب**

ماجستير الهندسة في الامن السيبراني

المستوي الأول						
الرمز/ الرقم	CODE/ NO.	اسم المقرر		المتطلب السابق	الوحدات الدراسية (Credits)	
		عربي	English		نظري (Th.)	عملي (Pr.)	معتمد (Total)
هال ٦٠٠	CE600	الامن السيبراني المتقدم	Advanced Cyber Security		٣	٠	٣
عال ٦٥١	CS651	أمن نظم التشغيل	Operating Systems Security		٣	٠	٣
هال ٦٠٣	CE603	أمن الحواسب والشبكات المتقدم	Advanced Computer and Networks Security		٣	٠	٣
المجموع							٩

المستوي الثاني						
الرمز/ الرقم	CODE/ NO.	اسم المقرر		المتطلب السابق	الوحدات الدراسية (Credits)	
		عربي	English		نظري (Th.)	عملي (Pr.)	معتمد (Total)
هال ٦٠٢	CE602	امن الانظمة اللاسلكية والجوالة	Wireless and Mobile Security		٣	٠	٣
		اختياري ١	Elective 1				٣
		اختياري ٢	Elective 2				٣
المجموع							٩

المستوي الثالث						
الرمز/ الرقم	CODE/ NO.	اسم المقرر		المتطلب السابق	الوحدات الدراسية (Credits)	
		عربي	English		نظري (Th.)	عملي (Pr.)	معتمد (Total)
		اختياري ٣	Elective 3				٣
		اختياري ٤	Elective 4				٣
عال ٦١٧	CS617	مناهج واخلاقيات البحث العلمي	Research Ethics and Methods		٣	٠	٣
المجموع							٩

المستوي الرابع						
الرمز/ الرقم	CODE/ NO.	اسم المقرر		المتطلب السابق	الوحدات الدراسية (Credits)	
		عربي	English		نظري (Th.)	عملي (Pr.)	معتمد (Total)
		اختياري ٥	Elective 5				٣
هال ٦١٦	CE616	مشروع بحثي	Research Project	عال ٦١٧			٤
المجموع							٧

المقررات الاختيارية						
الرمز/ الرقم	CODE/ NO.	اسم المقرر		المتطلب السابق	الوحدات الدراسية (Credits)	
		عربي	English		نظري (Th.)	عملي (Pr.)	معتمد (Total)
عال٦٥٥	CS655	التحليل الجنائي الحاسوبي	Computer forensics	هال٦٠٠	٣	٠	٣
هال٦٠٦	CE606	أمن الحوسبة السحابية	Cloud computing security	هال٦٠٣	٣	٠	٣
هال٦٠٧	CE607	أمن انترنت الأشياء	IoT Security	هال٦٠٣	٣	٠	٣
هال٦٠٨	CE608	أمن الأجهزة	Hardware Security	هال٦٠٠	٣	٠	٣
هال٦٠٩	CE609	موضوعات مختارة في الأمن السيبراني ١	Selected topics in cyber security 1	موافقة المنسق	٣	٠	٣
هال٦١٠	CE610	موضوعات مختارة في الأمن السيبراني ٢	Selected topics in cyber security 2	موافقة المنسق	٣	٠	٣
هال٦١١	CE611	أمن الشبكات وحماية المحيط	Network Security and perimeter protection	هال٦٠٣	٣	٠	٣
هال٦١٢	CE612	الهندسة العكسية للبرمجيات الخبيثة المتقدم	Advanced Malware Reverse Engineering	هال٦٠٠	٣	٠	٣
هال٦١٣	CE613	معالجات التشفير	Cryptographic processors	هال٦٠٠	٣	٠	٣
عال٦٥٦	CS656	القرصنة الأخلاقية المتقدمة والتدابير المضادة	Advanced Ethical hacking and countermeasures	هال٦٠٠	٣	٠	٣
هال٦١٥	CE615	الامن السيبراني بكتلة البيانات المتسلسلة	Cybersecurity with Blockchains	هال٦٠٠	٣	٠	٣

(٢٥) توصيف المقررات

يجب أن يتضمن توصيف المقرر العناصر الثلاثة الآتية: **١. الأهداف ويجب أن تتضمن: البعد المعرفي، والبعد المهاري، والبعد الوجداني.** **٢. الموضوعات.** **٣. وسائل التقويم.**	Course description should include the following three elements: 1.Objectives that include: cognitive dimension, Skills dimension and emotional dimension 2 Topics. 3. Assessment methods.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال٦٠٠	الامن السيبراني المتقدم	٣	

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:
١. تقييم وتقدير احتياجات الأمن السيبراني للمنظمة.
٢. قياس أداء الأنظمة الأمني.
٣. صياغة وتحديث ونشر استراتيجيات وسياسات الأمن السيبراني.

- **المحتوي:**

يستعرض هذا المقرر تغطية شاملة لمختلف جوانب مفاهيم الأمن السيبراني. مقدمة في نظم المعلومات ، أمن المعلومات ، أمن التطبيقات ، التهديدات الأمنية ، تطوير نظام المعلومات الآمن ، القضايا الأمنية في الأجهزة ، سياسات الأمن ، معايير أمن المعلومات.

- **وسائل التقويم:**

١. الواجبات ، استعراض الأبحاث ، التقارير ، ...
٢. الاختبار الفصلي
٣. الامتحان النهائي

Course Code	Course Title	Credits	Prerequisite
CE600	Advanced Cyber Security	3	

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Evaluate and assess cyber security needs of an organization.
2. Measure the performance of security systems.
3. Formulate, update and communicate cyber security strategies and policies.

- **Content:**

This course reviews the comprehensive coverage of various aspects of cyber security concepts, Introduction to Information Systems, Information Security, Application Security, Security Threats, Development of secure Information System, Security Issues In Hardware, Security Policies, and Information Security Standards.

- **Assessment methods.**

1. Assignments, Reviews of Research Papers, Reports, …
2. Midterm Exam
3. Final Exam.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
عال ٦٥١	أمن نظم التشغيل	٣	

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. فهم آليات وسياسات التحقيق والدفاع ضد هجمات نظام التشغيل.
٢. تنفيذ تقنيات أمن نظام التشغيل الأساسية.
٣. تقييم الأدوات والتقنيات لاستخدامها في حماية أنظمة التشغيل.

- **المحتوي:**

يغطي هذا المقرر أساسيات وموضوعات متقدمة في أمان نظام التشغيل (OS). سوف يتضمن آليات وسياسات مستوى نظام التشغيل في التحقيق والدفاع ضد هجمات العالم الحقيقي على أنظمة الحاسب، مثل الديدان ذاتية التكاثر، والجذور الخفية، وشبكات الروبوت الكبيرة. ستتم مناقشة تقنيات أمان نظام التشغيل الأساسية مثل المصادقة ومراقبة مكالمات النظام وحماية الذاكرة. كما سيتم تقديم تقنيات متقدمة حديثة مثل العشوائية على مستوى النظام، والمحاكاة الافتراضية للأجهزة/البرمجيات، وميزات الأجهزة الأخرى.

- **وسائل التقويم:**

١. اختبارات قصيرة مفاجئة.
٢. واجبات منزلية.
٣. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CS651	Operating Systems Security	3	

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Demonstrate understanding of mechanisms and policies in investigating and defending against operating system attacks.
2. Implement basic operating system security techniques.
3. Evaluate tools and technologies for use in protecting the operating systems.

- **Content:**

This course covers both fundamentals and advanced topics in operating system (OS) security. It includes OS level mechanisms and policies in investigating and defending against real-world attacks on computer systems, such as self-propagating worms, stealthy rootkits and large-scale botnets. It discusses basic OS security techniques such as authentication, system call monitoring, and memory protection. It introduces recent advanced techniques such as system-level randomization, hardware/software virtualization, and other hardware features.

- **Assessment methods.**

1. Quizzes.
2. Homeworks.
3. Midterm and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال٦٠٢	أمن الانظمة اللاسلكية والجوالة	٣	

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. اكتساب المعرفة الصلبة في مبادئ الأمن المدرجة في تصميم أجيال الشبكات المتنقلة.
٢. شرح نماذج الأمن لمختلف منصات الأجهزة المحمولة.
٣. توضيح المعايير الأمنية لخدمات المحمول والأنظمة اللاسلكية.

- **المحتوي:**

يقدم هذا المقرر نظرة عامة على المفاهيم المتعلقة بالمبادئ الأمنية المتضمنة في تصميم عدة أجيال من شبكات المحمول، من الجيل الثاني إلى الجيل الخامس. ويستكشف نماذج أمن الأنظمة الأساسية لمنصات الأجهزة المحمولة الشهيرة مثل نظام تشغيل المحمول أي فون والأندرويد وهاتف ويندوز. وهو يغطي أمن خدمات الهاتف المحمول، مثل الصوت عبر بروتوكول الإنترنت ، والرسائل النصية، وبروتوكول التطبيقات اللاسلكية ، ولغة ترميز النصوص التشعبية للمحمول. كما يقدم معايير الأمن في الأنظمة اللاسلكية الحالية: أمن واي فاي (الخصوصية المكافئة السلكية و الوصول المحمي لواي فاي والوصول المحمي لواي فاي المؤسسة)

- **وسائل التقويم:**

١. اختبارات قصيرة مفاجئة.
٢. واجبات منزلية.
٣. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CE602	Wireless and Mobile Security	3	

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Acquire solid knowledge on security principles incorporated in the design of mobile network generations.
2. Explain security models for various mobile device platforms.
3. Illustrate security standards for mobile services and wireless systems.

- **Content:**

This course provides a conceptual overview of the security principles incorporated in the design of several generations of mobile networks, from 2G to 5G. It explores platform security models of the popular mobile device platforms such as iphone operating system (IOS), Android and the Windows Phone. It covers the security of mobile services, such as voice over IP (VoIP), text messaging, Wireless Application Protocol (WAP) and mobile Hyper Text Markup Language (HTML). It also introduces security standards in current wireless systems: WiFi security (Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA-Enterprise).

- **Assessment methods.**

1. Quizzes.
2. Homeworks.
3. Midterm and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال ٦٠٣	أمن الحواسب والشبكات المتقدم	٣	

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. التعرف على نظرية الأعداد، إخفاء المعلومات، خوارزميات التشفير المتماثلة وغير المتماثلة.
٢. تطبيق وظائف التجزئة، ورموز مصادقة الرسالة، والتوقيعات الرقمية، وإدارة المفاتيح ومصادقة المستخدم.
٣. تقييم تقنيات وخوارزميات أمن الإنترنت.

- **المحتوي:**

في هذا المقرر ، يتم تعريف الطلاب بمتطلبات أمن الشبكات ، ونظرية الأعداد ، وإخفاء المعلومات ، ومبادئ تصميم التشفير ، والخوارزميات ، ومصادقة الرسائل ، ومبادئ التصاميم والتوقيع الرقمي ، وتصميم أمن أنظمة الشبكات.

- **وسائل التقويم:**

١. اختبارات قصيرة مفاجئة.
٢. واجبات منزلية.
٣. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CE603	Advanced Computer and Networks Security	3	

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Recognize number theory, steganography, symmetric and asymmetric encryption algorithms.
2. Apply hash functions, message authentication codes, digital signatures, key management and user authentication.
3. Appraise techniques and algorithms for Internetworking security.

- **Content:**

In this course, students are introduced to the network security requirements, number theory, steganography, encryption design principles and algorithms, message authentication and digital signature principles and designs, and network system security design.

- **Assessment methods.**

1. Quizzes.
2. Homeworks.
3. Midterm and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
عال٦١٧	مناهج واخلاقيات البحث العلمي	٣	

توصيف المقرر

- **الأهداف**:

بعد الانتهاء من دراسة هذا المقرر يكون الطالب قادرا على:

١. تحليل وتقييم الابحاث المنشورة ذات الصلة بمشروعه البحثي.
٢. اختيار الأساليب المناسبة لتحقيق اهداف للبحث .
٣. نقد مناهج البحث الكمية او النوعية ذات الصلة بمشروعه البحثي.
٤. تعريف المبادئ الأخلاقية للبحث العلمي.

- **المحتوي:**

	يقدم هذا المقرر المعرفة والمهارات البحثية لطلبة الدراسات العليا من خلال الاستكشاف النقدي للغة البحثية والأخلاقيات واساليب البحث. يقدم المقرر لغة البحث ، المبادئ والتحديات الأخلاقية ، وعناصر عملية البحث ومن ثم استخدام هذه الأسس النظرية للبدء في مراجعة نقدية للأدبيات ذات الصلة بمجالهم و تحديد كيفية الاستفادة من الابحاث السابقة في تكوين فهمهم لعملهم البحثي، كما يتضمن هذا المقرر تقديم الطلاب لعمل ندوات وحلقات دراسية عن البحوث المنشورة حديثا او المشاريع ذات الصلة. • **وسائل التقويم:** ١. الواجبات ، استعراض الأبحاث ، التقارير ، .. ٢. الاختبار الفصلي ٣. الامتحان النهائي

Course Code	Course Title	Credits	Prerequisite
CS617	Research Ethics and Methods	3	

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Analyze and critically evaluate published articles relevant to their research work.
2. Demonstrate the ability to choose methods appropriate to research aims and objectives.
3. Critique quantitative and/or qualitative research methodologies relevant to their research work.
4. Recognize and identify the ethical principles of research work.

- **Content:**

This course provides graduate students knowledge and research skills through critical exploration of research language, ethics, and approaches. The course introduces the language of research, ethical principles and challenges, and the elements of the research process. Graduate students will use these theoretical underpinnings to begin to critically review literature relevant to their field or and determine how research findings are useful in forming their understanding of their work. The student must present a seminar in one of the currents researches or projects in the area.

- **Assessment methods.**

1. Assignments, Reviews of Research Papers, Reports, …
2. Midterm Exam
3. Final Exam.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
عال ٦٥٥	التحليل الجنائي الحاسوبي	٣	هال٦٠٠

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. إنشاء طريقة لجمع وتقييم وتطبيق التشريعات الجديدة والقائمة والاتجاهات الصناعية المحددة لممارسة الطب الشرعي الرقمي.
٢. الالتزام بالمعايير الأخلاقية للمهنة وتطبيق تلك المعايير على جميع جوانب دراسة وممارسة الطب الشرعي الرقمي.
٣. تقييم فعالية أدوات الطب الشرعي الرقمية المتاحة واستخدامها بطريقة تعمل على تحسين كفاءة وجودة التحقيقات الجنائية الرقمية.

- **المحتوي:**

يُعنى هذا المقرر بالتحليل اللاحق لأنظمة الحاسب التي تم اختراقها بالفعل. تجمع أدوات وتقنيات التحليل الجنائي الحاسوبي المعلومات المتراكمة من أنظمة مختلفة لإعادة بناء سلوكيات واجراءات مجرمي الإنترنت. يركز التحليل الجنائي الحاسوبي على إعادة بناء الأحداث التي أدت إلى فساد النظام ، واستعادة البيانات المهمة ، ومساعدة السلطات في تعقب أولئك الذين ربما تسببوا في اختراق الانظمة ، ودراسة التقنيات التي يستخدمها المتسللون بغرض تحسين حماية الأنظمة ومنع انتهاكات مماثلة في المستقبل. • **وسائل التقويم:** ٤. الواجبات ، استعراض الأبحاث ، التقارير ، .. ٥. الاختبار الفصلي ٦. . الامتحان النهائي	

Course Code	Course Title	Credits	Prerequisite
CS655	Computer Forensics	3	**CE600**

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Create a method for gathering, assessing and applying new and existing legislation and industry trends specific to the practice of digital forensics.
2. Adhere to the ethical standards of the profession and apply those standards to all aspects of the study and practice of digital forensics.
3. Evaluate the effectiveness of available digital forensics tools and use them in a way that optimizes the efficiency and quality of digital forensics investigations.

- **Content:**

Computer forensics is concerned with the post-analysis of computer systems that have already been compromised. Forensic tools and techniques combine information accumulated from various systems to reconstruct the behaviors and actions of cyber criminals. Computer forensics focuses on the reconstruction of events that have led to system corruption, with the goals of recovering critical data, aiding authorities in tracking those who may have caused the security breach, and learning techniques used by hackers to improve the protection of systems and prevent similar breaches in the future.

- **Assessment methods.**

4. Assignments, Reviews of Research Papers, Reports, …
5. Midterm Exam
6. Final Exam.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال ٦٠٦	أمن الحوسبة السحابية	٣	هال٦٠٣

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. التعرف على مفاهيم الأمان المتعلقة بالحوسبة السحابية.
٢. اكتساب المعرفة الصلبة في مبادئ تصميم الحوسبة السحابية الآمنة.
٣. تلخيص جوانب الخصوصية التي يجب أخذها بعين الإعتبار في السحابة.

- **المحتوي:**

يستعرض هذا المقرر الحالة الحالية لأمن البيانات وتخزينها في السحابة بما في ذلك السرية والسلامة والتوافر. يجب أن يتضمن المقرر الموضوعات التالية : ممارسة إدارة الهوية والوصول (IAM) من أجل التوثيق والتصريح والتدقيق للمستخدمين الذين يصلون إلى الخدمات السحابية ؛ أطر ومعايير إدارة الأمن ذات الصلة بالسحابة ؛ جوانب الخصوصية التي ينبغي النظر فيها في السحابة ؛أهمية وظائف التدقيق والامتثال داخل السحابة.

- **وسائل التقويم:**

١. اختبارات موجزة.
٢. واجبات.
٣. تقارير.
٤. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CE606	Cloud Computing Security	3	CE603

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Recognize the security concepts pertaining to cloud computing.
2. Acquire solid knowledge on the design principles of secure cloud computing.
3. Summarize the privacy aspects that should be considered in the cloud.

- **Content:**

This course reviews the current state of data security and storage in the cloud, including confidentiality, integrity, and availability. The topics should include: the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services; security management frameworks and standards that are relevant to the cloud; privacy aspects that should be considered in the cloud; importance of audit and compliance functions within the cloud.

- **Assessment methods.**

1. Quizes.
2. Assignments.
3. Reports.
4. Midterm and and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال ٦٠٧	أمن انترنت الأشياء	٣	هال٦٠٣

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:
١. التعرف على بنية أمن إنترنت الأشياء وإجراءاتها الأمنية المضادة.
٢. مقارنة بين التهديدات في إنترنت الأشياء والشبكات التقليدية المخصصة.
٣. توضيح التحديات والحلول الأمنية في إنترنت الأشياء.

- **المحتوي:**

يتناول هذا المقرر ضمان سلامة الأجهزة والشبكات المترابطة تحت نسيج إنترنت الأشياء(IoT). وهو يغطي أمن الأجهزة وأمن الشبكة وأمن البيانات وأمن نظام التشغيل وأمن الخادم. وهو يقدم موضوعات متقدمة حديثة مثل مصادقة إنترنت الأشياء، ومصادقة الخادم الفردي، ومخططات التوثيق متعددة الخوادم ، والهجمات والعلاجات ، والأدوات التحليلية.

- **وسائل التقويم:**

١. اختبارات موجز.
٢. واجبات.
٣. تقارير.
٤. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CE607	IoT security	3	CE603

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Recognize the security architecture of IoT and its security countermeasures.
2. Compare between the threats in IoT and traditional ad hoc networks.
3. Illustrate the security challenges and solutions in IoT.

- **Content:**

This course deals with ensuring the safety of devices and networks interconnected under the fabric of the Internet of Things (IoT). It covers device/physical security, network security, data security, operating system security, and server security**.** It introduces recent advanced topics such as IoT authentication, single-server authentication, multi-server authentication schemes, attacks and remedies, and analytical matrices and tools.

- **Assessment methods.**

1. Quizes.
2. Assignments.
3. Reports.
4. Midterm and and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال٦٠٨	أمن الأجهزة	٣	هال٦٠٠

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:
١. التعرف على نقاط الضعف في مراحل تصميم الأنظمة الرقمية الحالية.
٢. التفريق بين الأنواع المختلفة للهجمات المادية على الأنظمة الرقمية.
٣. توضيح التحديات والحلول الأمنية في الأجهزة الإلكترونية.

- **المحتوي:**

يقدم هذا المقرر للطلاب فهمًا شاملاً لأمن الأجهزة الإلكترونية بدءًا من الأساسيات إلى التطبيقات العملية. يجب أن يفهم الطلاب نقاط الضعف في مراحل تصميم الأنظمة الرقمية الحالية والهجمات المادية على هذه الأنظمة. يجب أن تتضمن الموضوعات ما يلي: أساسيات الهجمات المادية ، الإجراءات المضادة ضد الهجمات المادية ، هجمات القنوات الجانبية (الهجمات المخبأة ، هجمات تحليل الطاقة ، هجمات التوقيت ، هجمات سلسلة المسح) والتدابير المضادة ، هجمات طروادة المادية والتصميم الموثوق للدوائر المتكاملة، نموذج منصة الثقة، دالة عدم الاستنساخ المادية.

- **وسائل التقويم:**

١. اختبارات موجز.
٢. واجبات.
٣. تقارير.
٤. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CE608	Hardware Security	3	CE600

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Recognize the vulnerabilities in the current digital systems design flow.
2. Differentiate the different types of physical attacks on digital systems.
3. Illustrate the security challenges and solutions in the electronic hardware.

- **Content:**

This course gives students a comprehensive understanding of hardware security starting from fundamentals to practical applications. Students should understand the vulnerabilities in the current digital systems design flow and the physical attacks to these systems. The topics should include: fundamentals of physical attacks, countermeasures against physical attacks, Side channel attacks (cache attacks, power analysis attacks, timing attacks, scan chain attacks) and countermeasures, Hardware Trojan and trusted integrated circuit (IC) design, Trust platform module (TPM), physical unclonable function (PUF).

- **Assessment methods.**

1. Quizes.
2. Assignments.
3. Reports.
4. Midterm and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال٦٠٩	موضوعات مختارة في الأمن السيبراني ١	٣	موافقة المنسق

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. تعرف على أحدث المواضيع التي تنشأ في مجال الأمن السيبراني.
٢. تصنيف ووصف الثغرات وآليات الحماية لبروتوكولات الشبكة الشائعة ، وبروتوكولات الويب ، والبرمجيات وأنظمة الأجهزة.
٣. تحليل / وتعليل حول آليات الحماية الأساسية لأنظمة التشغيل الحديثة والبرمجيات والأجهزة.

- **المحتوي:**

في هذا المقرر ، سيتم تحديد موضوع أو موضوعات والموافقة عليها من قبل مجلس القسم لتعكس أحدث القضايا في مجال الأمن السيبراني التي قد تظهر بعد الموافقة على هذه الخطة الدراسية.

- **وسائل التقويم:**

١. اختبارات موجزة.
٢. واجبات.
٣. تقارير.
٤. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CE609	Selected Topics in Cyber Security 1	3	Coordinator approval

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. learn about the state of the art topics that arise in the cyber security field
2. classify and describe vulnerabilities and protection mechanisms of popular network protocols, web protocols, software and hardware systems
3. analyze / reason about basic protection mechanisms for modern OSs, software and hardware systems.

- **Content:**

In this course, a topic or a set of topics that will be determined and approved by the department to reflect the most recent issues in the field of cyber security that might appear after approval of the study plan.

- **Assessment methods.**

1. Quizes.
2. Assignments.
3. Reports.
4. Midterm and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال٦١٠	موضوعات مختارة في الأمن السيبراني٢	٣	موافقة المنسق

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. تعرف على أحدث المواضيع التي تنشأ في مجال الأمن السيبراني.
٢. تصنيف ووصف الثغرات وآليات الحماية لبروتوكولات الشبكة الشائعة ، وبروتوكولات الويب ، والبرمجيات وأنظمة الأجهزة.
٣. تحليل / وتعليل حول آليات الحماية الأساسية لأنظمة التشغيل الحديثة والبرمجيات والأجهزة.

- **المحتوي:**

في هذا المقرر ، سيتم تحديد موضوع أو موضوعات والموافقة عليها من قبل مجلس القسم لتعكس أحدث القضايا في مجال الأمن السيبراني التي قد تظهر بعد الموافقة على هذه الخطة الدراسية.

- **وسائل التقويم:**

١. اختبارات موجزة.
٢. واجبات.
٣. تقارير.
٤. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CE610	Selected Topics in Cyber Security 2	3	Coordinator approval

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. learn about the state of the art topics that arise in the cyber security field
2. classify and describe vulnerabilities and protection mechanisms of popular network protocols, web protocols, software and hardware systems
3. analyze / reason about basic protection mechanisms for modern OSs, software and hardware systems.

- **Content:**

In this course, a topic or a set of topics that will be determined and approved by the department to reflect the most recent issues in the field of cyber security that might appear after approval of the study plan.

- **Assessment methods.**

1. Quizes.
2. Assignments.
3. Reports.
4. Midterm and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال٦١١	أمن الشبكات وحماية المحيط	٣	هال٦٠٣

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. اكتساب المعرفة حول تصميم الشبكات الآمنة
٢. اكتساب المعرفة حول تقنيات الأمن المختلفة
٣. تحليل نقدي لتركيب الشبكات (باستخدام الأدوات المناسبة) من أجل تحديد مشاكلها الأمنية.
٤. صياغة توصيات لأصحاب المصلحة على مختلف المستويات داخل المنظمة ، لتقوية البنية التحتية للشبكة لتحقيق الوضع الأمني المنشود.

- **المحتوي:**

في هذا المقرر ، سيتم تعريف الطلاب بتصميم شبكات الحاسب الآمنة. يتم عرض ومناقشة نقاط الضعف في تصميم البنية التحتية للشبكة وعيوب الأمن في بروتوكولات الشبكة. تتم مراجعة أنظمة تشغيل الشبكات ومعماريات الشبكات بالإضافة إلى المشكلات المتعلقة بالأمان. سيتم أيضًا تناول المشكلات المتعلقة بأمن المحتوى والتطبيقات مثل رسائل البريد الإلكتروني و DNS وخوادم الويب. سيتم تحليل التقنيات الأمنية بما في ذلك كشف التسلل ، والتحليل الجنائي الحاسوبي ، والتشفير ، والتوثيق والتحكم في الوصول. سيتم تقديم مشكلات الأمان في بروتوكولات IPSEC و SSL / TLS و SSH.

- **وسائل التقويم:**

١. اختبارات موجزة.
٢. واجبات.
٣. تقارير.
٤. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CE611	Network Security and Perimeter Protection	3	CE603

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Acquire knowledge about the design of secure networks
2. Acquire knowledge about the different security techniques
3. critically analyze a network configuration (using tools as appropriate) in order to identify its security issues.
4. formulate recommendations for stakeholders at various levels within an organization, to harden network infrastructure to achieve a desired security situation.

- **Content**:

In this course, students are introduced to the design of secure computer networks. Exploitation of weaknesses in the design of network infrastructure and security flaws in network protocols are presented and discussed. Network operation systems and network architectures are reviewed, together with the respective security related issues. Issues related to the security of content and applications such as emails, DNS, web servers are also addressed. Security techniques including intrusion detection, forensics, cryptography, authentication and access control are analyzed. Security issues in IPSEC, SSL/ TLS and the SSH protocol are presented.

- **Assessment methods.**

1. Quizes.
2. Assignments.
3. Reports.
4. Midterm and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال٦١٢	الهندسة العكسية للبرمجيات الخبيثة المتقدمة	٣	هال٦٠٠

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. تطبيق منهجية تحليل البرمجيات الخبيثة والتكنولوجيا.
٢. التعرف على التقنيات الهندسية المضادة العكسية وبعض وظائف البرمجيات الخبيثة المتقدمة.
٣. مناقشة المشاكل المهنية والتحليل والاستنتاجات في مجال تحليل البرمجيات الخبيثة ، سواء مع المهنيين أو مع الجمهور العام.

- **المحتوي:**

هذا المقرر يستعرض للطالب مختلف التقنيات والإجراءات المستخدمة في تحليل البرمجيات لاكتشاف وإزالة الكود المصاب. تميل المناطق التي يتم استكشافها نحو نمو الشفرات الخبيثة ، وناقلات الهجوم المشتركه ، والتحليل السطحي للبرامج الضارة ، وتحليل وقت التشغيل للبرامج الضارة ، ومراقبة النظام ، والمصححات ، والهندسة العكسية الثابتة للبرامج الضارة ، والمفككات لتحديد تقنيات التشويش وطرق منع الانعكاس.

- **وسائل التقويم:**

١. الواجبات ، استعراض الأبحاث ، التقارير ، ...
٢. الاختبار الفصلي
٣. الامتحان النهائي

Course Code	Course Title	Credits	Prerequisite
CE612	Advanced Malware Reverse Engineering	3	CE600

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Applying malware analysis methodology and technology
2. Identify known anti-reverse engineering techniques and some advanced malware functionality.
3. Discuss professional problems, analysis and conclusions in the field of malware analysis, both with professionals and with general audience.

- **Content:**

This course exposes the student to various techniques and procedures employed in the practice of software analysis to detect and remove affected code. The areas explored will consist of trends in malicious code growth, common attack vectors, surface analysis of malware, run-time analysis of malware, system monitoring, debuggers, static reverse engineering of malware, and disassemblers to identify obfuscation techniques and Anti-reversing methods.

- **Assessment methods.**

1. Assignments, Reviews of Research Papers, Reports, …
2. Midterm Exam
3. Final Exam.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال٦١٣	معالجات التشفير	٣	هال٦٠٠

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. اكتساب المهارات اللازمة لتنفيذ أنظمة التشفير على الأجهزة القابلة لإعادة التشكيل.
٢. استخدم أدوات البرامج والمعدات الملائمة لتطوير مسرعات أجهزة التشفير.
٣. المقارنة بين التنفيذات المختلفة لأنظمة التشفير باستخدام مقاييس التصميم المختلفة.

- **المحتوي:**

يهدف هذا المقرر إلى بناء المعرفة والمهارات اللازمة للتنفيذ الفعال لأوليات التشفير على الأجهزة القابلة لإعادة التكوين. وستكون منصة التنفيذ عبارة عن مصفوفة بوابات قابلة للبرمجة الميدانية (FPGA) تحتوي على معالج للأغراض العامة ونسيج إضافي قابل لإعادة التشكيل من أجل تطبيقات مسرعات الأجهزة المخصصة. تتطلب مشروعات الفريق تصميم بعض البدائل المشفرة المختارة متبوعة بالمقارنة والتباين بين البدائل المختلفة للتنفيذ، مثل البرمجيات، وأجهزة FPGA المخصصة، والتصميم المشترك المختلط لبرامج الأجهزة. يمكن أن تشمل الموضوعات حساب الحقل المتناهي الثنائي، وشفرات الكتلة، ووظائف هاش، ووضع العداد لتشغيل الأصفار، وأنظمة التشفير بالمفتاح العمومي، ومنهجيات التصميم المشترك للأجهزة البرمجيات مع FPGA ، وتطوير البرمجيات وتحديد ملامحها ، والتوليف عالي المستوى ، والحافلات على الشاشات ، واجهات الأجهزة / البرامج ، ومسرعات الأجهزة المخصصة والهجمات على القناة الجانبية.

- **وسائل التقويم:**

١. اختبارات موجز.
٢. مشروع.
٣. تقارير.
٤. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CE613	Cryptographic Processors	3	CE600

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Acquire the necessary skills to implement cryptographic primitives on reconfigurable hardware.
2. Use the proper software tools and hardware kits to develop cryptographic hardware accelerators.
3. Compare between the different implementations of cryptographic primitives using the different design metrics.

- **Content:**

The objective of this course is to build knowledge and skills necessary for efficient implementations of cryptographic primitives on reconfigurable hardware. The implementation platform will be a field programmable gate array (FPGA) containing a general-purpose processor and additional reconfigurable fabric for implementations of custom hardware accelerators. Team projects require design of selected cryptographic primitives followed by comparison and contrast of various implementation alternatives, such as software, custom FPGA hardware, and hybrid hardware-software co-design. Topics may include binary finite field arithmetic, block ciphers, hash functions, counter mode of operation for block ciphers, public key cryptosystems, hardware/software co-design methodologies with FPGAs, software development and profiling,

high level synthesis, on- chip buses, hardware/software interfaces, custom hardware accelerators and side channel attacks.

- **Assessment methods.**

1. Quizes.
2. Assignments.
3. Reports.
4. Midterm and and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
عال٦٥٦	القرصنة الأخلاقية والتدابير المضادة المتقدمة	٣	هال ٦٠٠

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. مناقشة تشريح هجمات الكمبيوتر والتدابير المضادة لحماية البيانات القيمة.
٢. استكشاف التقنيات المتقدمة والهجمات التي قد تكون جميع التطبيقات المعقدة الحديثة عرضة لها.
٣. التركيز على كيفية استخدام الأدوات والتقنيات المضادة.

- **المحتوي:**

يقدم هذا المقرر للطلاب أحدث أدوات وتقنيات القرصنة لفهم تشريح هجمات الكمبيوتر والتدابير المضادة لحماية البيانات القيمة. فهم المتجهات الهجومية المختلفة باستخدام تقنيات وأدوات يدوية يستخدمها الهاكر لمهاجمة أجهزة الكمبيوتر من أجل سرقة معلومات قيمة وخاصة.

- **وسائل التقويم:**

١. الواجبات ، استعراض الأبحاث ، التقارير ، ...
٢. الاختبار الفصلي
٣. الامتحان النهائي

Course Code	Course Title	Credits	Prerequisite
CS656	Advanced Ethical hacking and countermeasures	3	CE600

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Discuss anatomy of computer attacks and countermeasures to protect valuable data.
2. Explore advanced techniques and attacks to which all modern-day complex applications may be vulnerable.
3. Focus on how to use countermeasures tools and techniques.

- **Content:**

In this course we introduce the students to the latest hacking tools and techniques to understand the anatomy of computer attacks and countermeasures to protect valuable data. Understanding different attack vectors using hand-on techniques and tools that a hacker utilizes to attack computing devices in order to steal valuable and private information.

- **Assessment methods.**

1. Assignments, Reviews of Research Papers, Reports, …

	2. Midterm Exam 3. Final Exam.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال٦١٥	الامن السيبراني بكتلة البيانات المتسلسلة	٣	هال٦٠٠

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. وصف كيفية عمل سلاسل المعلومات الرقمية والتقنية الأساسية للمعاملات والكتل.
٢. إثبات انتشار سلاسل المعلومات الرقمية في المجال العام وكيفية الحفاظ على الشفافية والخصوصية والأمن دون أي سيطرة مركزية أو وكالة موثوق بها.
٣. استكشاف منصات لبناء التطبيقات على تكنولوجيا سلاسل المعلومات الرقمية مع تحديات ومستقبل الأمن السيبراني.

- **المحتوي:**

في هذا المقرر سيتم تعريف الطلاب بالمشهد المشترك للتهديدات السيبرانية والهجمات الشائعة مثل البرامج الضارة والتصيد الاحتيالي والتهديدات الداخلية و DDoS. فهم أعمال تقنية كتلة البيانات المتسلسلة ، الهندسة المعمارية Ethereum و Hyperledger وكيف تتناسب مع النظام البيئي للأمن السيبراني. كتابة التطبيق الموزع على كتلة البيانات المتسلسلة Ethereum وإطار Hyperledger Fabric. ثالوث الأمن وتكييفه مع كتلة البيانات المتسلسلة .المفاهيم الأساسية للأمن السيبراني ، مثل حماية DDoS ، والهوية القائمة على PKI ، و FA٢ ، وأمان DNS. دور كتلة البيانات المتسلسلة في تحويل حلول الأمن السيبراني. أمثلة النشر في العالم الحقيقي من كتلة البيانات المتسلسلة في الحالات الأمنية. تحديات على المدى القصير ومستقبل الأمن السيبراني مع كتلة البيانات المتسلسلة.

- **وسائل التقويم:**

١. اختبارات قصيرة مفاجئة.
٢. واجبات منزلية.
٣. مشاريع فى مجموعات.
٤. اختبارات فصلية ونهائية.

Course Code	Course Title	Credits	Prerequisite
CE615	Cybersecurity with Blockchains	3	CE600

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Describe how blockchains work and the underlying technology of transactions and blocks.
2. Demonstrate the deployment of blockchains in the public domain and how to maintain transparency, privacy and security without any central controlling or trusted agency.
3. Explore platforms to build applications on blockchain technology with challenges and future of cybersecurity.

- **Content:**

In this course, students are introduced to the common cyber threat landscape and common attacks such as malware, phishing, insider threats, and distributed denial-of-service (DDoS). Understand the workings of Blockchain technology, Ethereum and Hyperledger architecture and how they fit into the cybersecurity ecosystem. Write distributed application on Ethereum Blockchain and the Hyperledger Fabric framework. Security triad and its adaptation with Blockchain. Core concepts of cybersecurity, such as DDoS protection, public key infrastructure (PKI)-based identity, two-factor authentication (2FA), and Domain Name System (DNS) security. Role of Blockchain in

transforming cybersecurity solutions. Real-world deployment examples of Blockchain in security cases. Short-term challenges and future of cybersecurity with Blockchain.

- **Assessment methods.**
  1. Quizzes.
  2. Homeworks.
  3. Group projects.
  4. Midterm and Final Exams.

رمز ورقم المقرر	عنوان المقـــرر	عدد الوحدات	متطلب سابق
هال٦١٦	مشروع بحثي	٤	عال ٦١٧

توصيف المقرر

- **الأهداف**:

عند الانتهاء من دراسة هذا المقرر يتمكن الطالب من:

١. إثبات اكتساب التخصص والمهارات في جزء معين من مجال الأمان الإلكتروني.
٢. صياغة مشكلة متوسطة الحجم واختيار وتبرير نهج لحل المشكلة ضمن قيود معينة.
٣. مراعاة المبادئ الأخلاقية في جميع أنحاء العمل.
٤. إعداد تقرير مكتوب عن العمل المنجز.
٥. تقديم عرض تقديمي شفهي يوجز بدقة العمل المنجز.

- **المحتوي:**

يقوم الطالب في هذا المقرر باستخدام المهارات والمعارف التي اكتسبها خلال دراسته لإثبات القدرة على تصميم مشروع أمن معلومات بدءًا من مرحلة التصميم انتهاءًا إلى مرحلة التنفيذ والاختبار ويتم ذلك تحت اشراف أحد أعضاء هيئة التدريس بالقسم.

- **وسائل التقويم:**

١. عرض تقديمي للمشروع ومناقشة أمام لجنة مختصة
٢. تقييم تقرير المشروع

Course Code	Course Title	Credits	Prerequisite
CE616	Research Project	4	CS617

Course Description

- **Objectives:**

Upon completion of the course, a student will be able to:

1. Demonstrate that has acquired specialization and skills in a particular part of the cyber security field.
2. Formulate a moderate sized problem and select and justify an approach to solve the problem within certain constraints.
3. Be able to watch ethical principles throughout the work.
4. Prepare a written report on the work done
5. Make an oral presentation that should accurately summarize the work done.

- **Content:**

In this course, the student will use the skills and knowledge gained during his studies to demonstrate the ability to design an information security project from the design stage to the implementation and testing stage. This is done under the supervision of a faculty member in the department.

- **Assessment methods.**

	1. Project presentation and discussion in front of a Committee **2.** Evaluation of the project report