Master in Cyber Security – 2019

First Semester

	Course Code	Course Title	Credit Hours	Pre-Requisite
1	CS501	Research Methods in Computational Studies	3	None
2	CS507	Introduction to Cyber Security and Digital Crime	3	None
3	CS512	Cryptography Fundamentals	3	None
			9	

Second Semester

	Course Code	Course Title	Credit Hours	Pre-Requisite
1	CS564	Cyber Defense in Web Based Attacks	3/ Lab	CS507
2	CS566	Securing Enterprise Infrastructure using Cyber Security Techniques	3/ Lab	CS507
3	CS663	Digital Forensics and Investigations	3/ Lab	CS507
			9	

Third Semester

	Course Code	Course Title	Credit Hours	Pre-Requisite
1	CS613	Security Threats and Countermeasures in Complex Organizational Networks	3/ Lab	CS507
2	CS642	Innovative Solutions in Software Security	3/ Lab	CS507, CS564
3	CS645	Information Security Management, Legal and Ethical Issues	3	CS507
			9	

Fourth Semester

	Course Code	Course Title	Credit Hours	Pre-Requisite
1	CS666	Advanced Principles of Cyber Security	3/ Lab	CS507, CS564
2	CS683	Ethical Hacking and Penetration Testing	3/ Lab	CS564
3	CS698	Capstone Project in Cyber Security	3	Department Approval
			9	

SEU Master of Science in Cyber Security
Course description and Prerequisites

1. **CS501 Research Methods in Computational Studies**: This course provides an overview of the important concepts of research design, data collection, statistical and interpretative analysis, and final report presentation. The focus of this course is not on mastery of statistics but on the ability to use research in Computational Studies. Students will prepare a preliminary research design for projects in their subject matter areas and how to accurately collect, analyze and report data.
   Students will focus on the steps needed to design an individual research project or thesis. The course provides real world active learning assignments that seek to integrate the knowledge and skills gained through undergraduate course work. The course focuses on scientific writing, and oral, written, and graphical presentation of data and research results.
   Prerequisite: None

2. **CS507 Introduction to Cyber Security and Digital Crime:** This course provides an introduction to cyber security and digital crime. Students will learn about cyber security threats, dangers, and risks that organizations face and will develop the ability to analyze potential vulnerabilities that can have an adverse impact on digital assets.
   Prerequisite: None

3. **CS512 Cryptography Fundamentals:** This course provides students with a thorough review of cryptography and cryptographic techniques as they apply to the area of cyber and computer security. Students will learn about various cryptography techniques along with their advantages and disadvantages. Additionally, discussion will be provided on the various systems that are used to provide secure and encrypted end-to-end communications to include: pre-shared keys, hashing algorithms, certificates, public-key/private key infrastructures and shared secret keys.
   Prerequisite: None

4. **CS564 Cyber Defense in Web Based Attacks**: This course focuses on external cyber security threats including information networks and the World Wide Web. There will be a detailed view into search engines and current trends of integrating social media outlets into the enterprise as a mean of achieving strategic objectives.
   Prerequisite: CS507

5. **CS566 Securing Enterprise Infrastructure using Cyber Security Techniques**: This course gives the students the knowledge and hands on experience of protecting infrastructure services. It covers fundamentals and advanced topics in theoretical and practical infrastructure security. It explains mechanisms and policies. The course also covers types of malware and threats, and techniques used to defend against such threats. Students will have the opportunity to investigate recent research papers and existing technologies relevant to the course topics.
   Prerequisite: CS507

6. **CS663 Digital Forensics and Investigations:** This course provides students with insight to cyber security professional intrusion detection methods, cyber security tools, and preventative measures to cyber security risks. Students will learn how to respond to cyber breaches including the recovery, preservation, analysis of digital crime scene evidence, and proper incident response to cyber criminals.
   Prerequisite: CS507

7. **CS613 Security Threats and Countermeasures in Complex Organizational Networks:** The course details different network infrastructure security threats, attacks and countermeasures at different organizational network layers including perimeter security defenses, firewalls, virtual private networks, intrusion detection systems, wireless security, mobile network and network security auditing tools.
   The following topics will be covered: Network security protocols, Network threats and attacks, Malware, and Defense mechanisms and countermeasures.
   Prerequisites: CS507

8. **CS642 Innovative Solutions in Software Security:** This course discusses how to construct secure innovative programs. The course explores secure software development through the use of secure coding, program analysis, and advanced testing. The course details secure programming techniques to defend against source code software vulnerabilities such as overwriting, buffer overflow and code injection. Overview is given for secure web application development against web attacks such as SQL injection, Cross-Site Scripting (XSS), secure session management, and secure authentication.
   Prerequisite: CS507, CS564

9. **CS645 Information Security Management, Legal and Ethical Issues:** This course examines security governance and policies and how law, ethics, and technology intersect in organizations that rely on information technology. Students will gain an understanding and insight into issues arising from privacy, secrecy, access control, and policy management and enforcement, as well as other legal, and ethical dilemmas prevalent in today's organizations. Special module(s) will be dedicated to study Saudi Laws related to information management and security.
   Prerequisite: CS507

10. **CS666 Advanced Principles of Cyber Security:** This course provides students with an overview of cyber security access control to protect resources against unauthorized viewing, tampering, or destruction to ensure privacy, confidentiality, and prevention of unauthorized disclosure. Access Control, Authentication, and Public Key Infrastructure define the components of access control, provide a business framework for implementation, and discuss legal requirements that impact access control programs. The course looks at the risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them.
    Prerequisite: CS507, CS564

11. **CS683 Ethical Hacking and Penetration Testing:** This course provides students with the experience needed to secure information systems against attacks such as viruses, worms, as well as other system weaknesses that pose significant danger to organizational data. Students learn ethical hacking and penetration testing to uncover common techniques used by cyber criminals to exploit system vulnerabilities.
    Prerequisite: CS564

12. **CS698 Capstone Project in Cyber Security.** In the capstone project students explore the literature, conduct research and develop solutions to help analyze organizations security needs related to continuously evolving security challenges. Students will analyze organizational objectives and propose solution(s) and implementation plan(s). The proposed solution must address strategies to overcome challenges of cyber security related projects such as assessing risks, reduction of fund, and keeping the support of executive management. Students will utilize skills gained throughout the program to demonstrate the ability to design a cyber security project from conception to publishing/deployment.
    Prerequisite: Department Approval

ماجستير الأمن السيبراني
توصيف المقررات والمتطلبات السابقة

1. CS501 - Research Methods In Computational Studies (3 Credits)

عال 501 منهجية البحث في الدراسات الحاسوبية

يقدم هذا المقرر لمحة عامة عن المفاهيم الهامة لتصميم البحوث، جمع البيانات ، التحليل الإحصائي، تفسير النتائج، وكتابة التقرير النهائي. لا يركز هذا المقرر على المهارات الإحصائية ولكن على القدرة على القيام ببحوث الدراسات العليا في مجال الحاسب الآلي. خلال هذا المقرر سيقوم الطلاب بإعداد تصميم البحوث الأولية للمشاريع في مجال التخصص وكيفية جمع وتحليل البيانات بدقة.

سيركز الطلاب على الخطوات اللازمة لتصميم مشروع بحث أو أطروحة حيث يقدم المقرر مهارات التعلم ضمن سيناريوهات حقيقية تسعى إلى دمج المعرفة والمهارات التي اكتسبها الطلبة في مرحلة الدراسة الجامعية الأولى. يركز المساق على الكتابة العلمية، والعرض الشفهي والكتابي ورسم البيانات ونتائج البحوث.

المتطلب السابق: لا يوجد

2. CS507 - Introduction to Cyber Security and Digital Crime (3 credits)

عال 507 مقدمة في الأمن السيبراني والجريمة الرقمية

يقدم هذا المقرر مقدمة لأمن الفضاء الإلكتروني والجريمة الرقمية. يتعرف الطلاب من خلال هذا المقرر على التهديدات والمخاطر التي تواجه الأمن السيبراني، والمخاطر التي تواجه المنظمات وتحتاج إلى تطوير القدرة على تحليل نقاط الضعف المحتملة التي يمكن أن يكون لها تأثير سلبي على الأصول الرقمية.

المتطلب السابق: لا يوجد

3. CS512 - Cryptography Fundamentals (3 credits)

عال 512 أساسيات التشفير

يزود هذا المقرر الطلاب بأساسيات علم تشفير البيانات (التشفير) و تطبيقات هذا العلم في مجال أمن وسلامة المعلومات حيث يعتبر هذا الموضوع من الموضوعات والعلوم الاساسية في هذا المجال وذلك بسبب التطور السريع للكمبيوتر والنمو الكبير للشبكات وبخاصة الشبكة العالمية الإنترنت. وفي عصرنا الحالي باتت الحاجة ملحة لدراسة وفهم واستخدام علم التشفير وذلك لارتباط العالم ببعضه عبر شبكات مفتوحة. وحيث انه يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين او بين المنظمات الخاصة والعامة، ولذلك كان لابد من معرفة وايجاد الطرق المثلى لحفظ سرية هذه المعلومات بالاضافة الى امكانية تبادل البيانات بشكل امن. وسيتعرف الطالب من خلال دراسة هذا المقرر على أنظمة التشفير القديمة والحديثة والتقنيات والخوارزميات المستخدمة في تشفير البيانات بالاضافة لمعرفة المزايا والعيوب لهذه الانظمة كما سيتعرف الطالب من خلال هذا المقرر على الاتجاهات المعاصرة والحديثة في علم التشفير وتطبيقاتها في العديد من المجالات واستخداماتها في حياتنا اليومية.

المتطلب السابق: لا يوجد

4. CS564 - Cyber Defense in Web Based Attacks (3 credits)

عال 564 الدفاع السيبراني ضد الهجمات على شبكة الإنترنت

هذا المقرر يركز على تهديدات الأمن الإلكتروني الخارجية بما في ذلك شبكات المعلومات وشبكة الإنترنت العالمية. سوف يكون هناك عرض تفصيلي لوسائل التواصل الاجتماعي، محركات البحث، والاتجاهات الحالية التي تعمل على دمج وسائل التواصل الاجتماعي في المؤسسة كوسيلة لتحقيق الأهداف الاستراتيجية.

المتطلب السابق: CS507

5. CS566 - Securing Enterprise Infrastructure using Cyber Security Techniques (3 credits)

عال 566 تأمين البنية التحتية للمؤسسات باستخدام تقنيات الأمن السيبراني

هذا المقرر يعزز أساليب أمن الفضاء الإلكتروني في البنى التحتية الحساسة ويزود الطلاب بالمعرفة والخبرة اللازمتين لحماية خدمات البنية التحتية. سيكتسب الطلاب أيضا نظرة ثاقبة في تصميم ونشر وصيانة نظم الأمن السيبراني المعقدة.

المتطلب السابق: 507

6. CS663 - Digital Forensics and Investigations (3 credits)

عال 663 التحليل الجنائي الرقمي والتحقيقات

يزود هذا المقرر الطالب بنظرة داخلية عن التعليمات والتوجيهات ذات العلاقة بأمن الفضاء الالكتروني الاحترافي، وأدوات الأمن السيبراني، والتدابير الوقائية لمخاطر الأمن السيبراني. وسوف يتعلم الطلاب كيفية الرد على الانتهاكات الالكترونية بما في ذلك استرجاع البيانات، الحفاظ وتحليل الأدلة في مسرح الجريمة الرقمية، والاستجابة المناسبة للحوادث الصادرة عن مجرمي الإنترنت.

المتطلب السابق: CS507

7. CS613 - Security Threats and Countermeasures in Complex Organizational Networks (3 credits)

عال 613 التهديدات الأمنية والتدابير المضادة في شبكات الحاسوب المتطورة بالمؤسسات

يغطي هذا المقرر تفاصيل التهديدات والهجمات والتدابير المضادة الخاصة بأمن البنية التحتية المختلفة للشبكة في طبقات الشبكة التنظيمية المختلفة بما في ذلك دفاعات الأمن المحيطة، جدران الحماية، الشبكات الخاصة الافتراضية، أنظمة كشف التسلل، أمن الشبكات اللاسلكية، وأدوات تدقيق أمن الشبكات. ستتم تغطية المواضيع التالية: بروتوكولات أمان الشبكة، تهديدات الشبكة والهجمات، البرامج الضارة، وآليات الدفاع والتدابير المضادة.

المتطلب السابق: CS507

8. CS642 – Innovative Solutions in Software Security (3 credits)

عال 642 الحلول المبتكرة لأمان البرمجيات

يناقش هذا المقرر كيفية بناء برامج آمنة مبتكرة. يستكشف المقرر تطوير برمجيات آمنة من خلال استخدام التشفير الآمن، تحليل البرامج، واختبارات البرمجيات المتقدمة. يقدم المقرر تفاصيل تقنيات البرمجة الآمنة للدفاع ضد الثغرات الأمنية لمصادر البرامج ومن هذه التهديدات الأمنية الكتابة فوق مواقع البيانات (overwriting)، تجاوز سعة المخزن المؤقت (buffer overflow) والحقن في الشفرة (code injection). يقدم المقرر أيضاً نظرة عامة على تطوير تطبيقات الويب الآمنة ضد هجمات الويب مثل حقن SQL ، البرمجة عبر المواقع (XSS) ، إدارة جلسات آمنة والمصادقة الآمنة.

المتطلب السابق: CS507 و CS564

9. CS645 - Information Security Management, Legal and Ethical Issues (3 credits)

عال 645 القضايا الإدارية والقانونية والأخلاقية في أمن المعلومات

يدرس هذا المقرر الحوكمة والسياسات الأمنية وكيف يتقاطع القانون والأخلاق والتكنولوجيا في المنظمات التي تعتمد على تكنولوجيا المعلومات. سيكتسب الطلاب فهماً للمسائل الناشئة عن الخصوصية والسرية والتحكم في الوصول وإدارة السياسات وتطبيقها فضلاً عن المعضلات القانونية والأخلاقية الأخرى السائدة في مؤسسات اليوم. سيخصص جزء من المقرر لدراسة القوانين السعودية المتعلقة بإدارة والأمن السيبراني.

المتطلب السابق: CS507

10. CS666 - Advanced Principles of Cyber Security (3 credits)

عال 666 مبادئ متقدمة في الأمن السيبراني

يقدم هذا المقرر طرق التحكم الآمن للوصول عبر الإنترنت لحماية الموارد من الوصول غير المصرح به أو العبث أو التدمير لضمان الخصوصية والسرية والحماية من الكشف غير المصرح به. يحدد التحكم في الوصول والمصادقة والبنية التحتية لمفتاح التشفير العام مكونات التحكم في الوصول ويوفر إطار عمل للتنفيذ ويناقش المتطلبات القانونية التي تؤثر على برامج التحكم في الوصول. ينظر المقرر أيضاً إلى المخاطر والتهديدات ونقاط الضعف السائدة في أنظمة المعلومات والبنى التحتية لتكنولوجيا المعلومات وكيفية التعامل معها.

المتطلب السابق: CS507 و CS564

11. CS683 - Ethical Hacking and Penetration Testing (3 credits)

عال 683 القرصنة الأخلاقية واختبارات الاختراق

يزود هذا المقرر الطالب بالخبرة اللازمة لتأمين نظم المعلومات ضد الهجمات مثل الفيروسات، والديدان الالكترونية، وكذلك نقاط الضعف الأخرى التي تشكل خطراً كبيراً على بيانات المنظمة ويتعلم الطلاب القرصنة الأخلاقية واختبار الاختراق للكشف عن التقنيات الشائعة التي يستخدمها مجرمو الإنترنت لاستغلال نقاط الضعف في النظام.

المتطلب السابق: CS564

12. CS698 - Capstone Project in Cyber Security (3 credits)

عال 698 مشروع التخرج في الأمن السيبراني

في هذا المقرر يتدارس الطلاب الدراسات الأدبية السابقة ويجرون الأبحاث ويطورون الحلول لمساعدتهم على تحليل احتياجات الأمن ذات الصلة بالتحديات الأمنية المتطورة الخاصة بالمؤسسات . سيقوم الطلاب بتحليل الأهداف التنظيمية واقتراح الحل وخطة التنفيذ. يجب أن يتناول الحل المقترح استراتيجيات للتغلب على تحديات المشاريع المتعلقة بالأمن السيبراني مثل تقييم المخاطر، الحد من التمويل والحفاظ على دعم الإدارة التنفيذية. سيستفيد الطلاب من المهارات المكتسبة طوال البرنامج لإثبات القدرة على تصميم مشروع الأمن السيبراني من مرحلة الفكرة المبدئية وحتى النشر/التنفيذ.

المتطلب السابق: موافقة القسم