KINGDOM OF SAUDI ARABIA
MINISTRY OF EDUCATION
KING FAISAL UNIVERSITY
COLLEGE OF COMPUTER SCIENCE
& INFORMATION TECHNOLOGY

Master of Science In Cybersecurity

Computer Networks and Communications Department
College of Computer Sciences and Information Technology

Study Plan

2019/2020

KINGDOM OF SAUDI ARABIA
MINISTRY OF EDUCATION
KING FAISAL UNIVERSITY

Master of Science
In
Cybersecurity

Computer Networks and Communications Department
College of Computer Sciences and Information Technology

Study Plan

2019/2020

1. DEPARTMENT OFFERING THE PROGRAM

Department: Computer Networks and Communications

College: College of Computer Sciences and Information Technology

2. PROGRAM TITLE

Master of Science in Cybersecurity
ماجستير العلوم في الأمن السيبراني

3. INTRODUCTION

Over the last few decades, information flow and processing through extensive use of computer systems and communication technology, has increased many fold. There has been a revolutionizing growth and development in various sectors including government and business operations, organizational policies, and decision-making. In addition, the growing use of Internet, social media, mobile and wireless technology has had a huge impact on public service delivery and social interaction. However, use of sophisticated techniques for information breaches and cyber-attacks has grown in parallel. Accordingly, there is a growing demand of information security professionals to keep information, systems and networks of an organization secure from various attacks within and outside the organizations. To cater the need of such professionals, the College of Computer Sciences and Information Technology is proposing an MS program in Cybersecurity. The nature and content of the proposed program is multidisciplinary to cover system security, information assurance and network security. In addition, the proposed program satisfies the need of the job market.

4. VISION

To be an internationally recognized interdisciplinary leader in cybersecurity education and research producing information security professionals.

5. MISSION

To offer a high quality, multidisciplinary graduate curriculum that prepares information security professionals to protect systems, information and network infrastructure of organizations against information breaches, cybercrime and attacks; To create professionals with an aim to develop and implement IT security plans and policies of an organization.

6. OBJECTIVES OF THE PROGRAM

The main objectives of the Master of Science program in Cybersecurity are to:

1. Prepare individuals with relevant technical knowledge and skill based in cybersecurity that equips them to protect and defend computer networks and systems.
2. Develop individuals capable of leading teams of technology specialists tasked with handling information security analysis, architecture, operations and monitoring for organizations.
3. Prepare individuals who can formulate long-term and near-term security strategies for an organization.

Upon completion of the degree, graduates of the program would be able to:

A. Explain concepts and theories related to the domain of cybersecurity.
B. Assess, analyze and evaluate the security requirements of an organization and discover security-related vulnerabilities.
C. Analyze, evaluate and implement appropriate solutions to meet the organizational security needs.
D. Formulate a comprehensive security architecture, devise and manage security policies, plans and procedures for effective and efficient management of security.
E. Use state of the art cybersecurity tools and technologies that assist in identification, analysis, and recovery from security breaches.

7. RATIONALE

According to the Saudi National Cyber Security Centre (NCSC), Saudi Arabia had suffered almost 1,000 cyberattacks last year that targeted infrastructure and intellectual property. As the Kingdom embarks towards its Vision 2030 plan, a great deal of consideration has been shifted to the national cybersecurity strategy. Technology will play a crucial role in facilitating the vision and the digitization of sensitive data will inevitably make it more vulnerable to cybercriminals. Security and threats have been evolving together, making the burden of security and information assurance a continuous challenge that only highly skilled professionals can handle. According to several reports, the demand for cybersecurity professional in local and international market is expected to grow exponentially in the coming years. The proposed master degree program in cybersecurity provides a rich and multidisciplinary curriculum that emphasizes on information security and its underlying technologies and vulnerabilities, while at the same time covering critical topics such as network security, cryptography, enterprise security analysis, legal and ethical issues etc. Graduates of this program will learn to stay current on rapidly changing technology, adapt and control new threats and start a successful career in enterprise security.

8. ADMISSION REQUIREMENTS

The eligibility criteria for candidates applying for admission to the Master program in Cybersecurity is listed below:

1. Fulfil the conditions stated in the graduate studies rules for Saudi Universities.
2. Have a bachelor degree in Computer Sciences Domain from a recognized university by the Ministry of Education.
3. Have a minimum CGPA of 3.75/5.00 or equivalent in the bachelor degree. A minimum CGPA of 3.5/5.00 and less than 3.75/5.00 might be accepted based on the university regulations.
4. Demonstrate English language proficiency through one of the following:
    i. A Band 5 in the International English Language Testing System (IELTS); or equivalent.
    ii. Earning a bachelor degree with English language as medium of instruction.
5. Provide two letters of recommendation.
6. Provide a certificate of good character (behavior).
7. Provide a letter of approval from the employer if the candidate is currently employed.
8. Pass entry test or interview conducted by the department or the college.
9. Meet any other criteria recommended by the department or the college.

9. GRADUATION REQUIREMENTS

The requirements needed to be fulfilled by students enrolled in the Master Degree Program in Cybersecurity to successfully graduate from the College of Computer Sciences and Information Technology, King Faisal University are:

1. Successful completion of 36 credits including a 9-credit Dissertation (Thesis Track) or 42 credits including a 9-credit Project (Coursework Track).
2. A Thesis or a Project is mandatory for successful completion of the Master's degree.
3. The minimum CGPA required for graduation is 3.75 out of 5.00.

10. BENCHMARKS

King Faisal University ranks in the 751-800 range in the QS World University Rankings for the year 2018. A list of universities selected from local, regional and international locations ranked higher than KFU and offering similar programs were selected for benchmark comparison. Please note that a few unlisted local and regional universities were considered to account for the lack of listed universities offering a program in information security or cybersecurity in these regions.

University	Country	Program Title	Multidisciplinary	QS Ranking
Local University Benchmarks				
KFUPM	KSA	MSc in Information Assurance and Security	Yes	173
Saudi Electronic University	KSA	MSc in Cybersecurity	Yes	Not Listed
Prince Sattam bin Abdulaziz University	KSA	MSc in Cybersecurity	Yes	Not Listed
Regional University Benchmarks				
Heriot-Watt University	UAE	MSc in Network Security	No	312
United Arab Emirates University	UAE	MSc in Information Security	Yes	390
Khalifa University	UAE	MSc in Information Security	No	451-460
NYIT - Abu Dhabi	UAE	MSc in Cybersecurity (Information, Network, & Computer Security)	Yes	Not Listed
International University Benchmarks				
University of Oxford	UK	MSc in Software and Systems Security	No	6
University College London	UK	MSc in Information Security	No	7
Johns Hopkins University	USA	MSc in Cybersecurity	Yes	17
Carnegie Mellon University	USA	Master of Science in Information Security	Yes	47
Georgia Institute of Technology	USA	M.S. In Cybersecurity (Technology Specialization)	Yes	70
University of Southampton	UK	MSc in Cyber Security	Yes	102
Eindhoven University of Technology	Netherlands	MSc in Information Security Technology	Yes	104

11. FACILITIES AND HUMAN RESOURCES

11.1 Human Resources:

Human resource requirement for the program is included in the table below. Please note that the information furnished in the table includes human resources that are available at the college with some recruitment needed in the future.

Academic Rank	Number
Professor	1
Associate Professor	2
Assistant Professor	8
Lab Administrators	2

11.2 Facilities:

11.2.1 Lecture Rooms:

The college has sufficient lecture rooms equipped with smart boards and two-way communication system to deliver lectures to male and female students at the same time.

11.2.2 Laboratories:

A dedicated lab for Cybersecurity. Some specifics for the lab are provided in the table below:

Resource	Minimum Quantity	Purpose	Availability in the College
Desktop Computers	30	Students will use them to perform hands-on training and exercises	Yes
Server	2	This system will host the vulnerable system	No
Small Experimental Wired and Wireless Network (includes LAN Switch, cables and Wi-Fi router)	-	An experimental network is made available either as cloud or a single instance for students to practice network security and penetration testing	Yes
Kali Linux	Installed on the Desktop Computers	The Operating System of choice	(Free)
Windows, Linux and Mobile Operating Systems	Different Operating system images installed on student machines	Students will work with different operating system vulnerabilities through the virtual machines	Yes

11.2.3 Other Requirements:

A dedicated library (or a section within the existing library) is needed with books from the Information Security domain. The library is expected to be populated with books from popular publishers such as Wiley, Syngress, Wrox, Elsevier and so on. These books will be main and reference texts for the courses included in the program. Digital copies of additional references and subscriptions to scientific journals (not included in the Saudi Digital Library) should also be made available to account for new and updated publications in the InfoSec area. It is expected that students in the Cybersecurity program will be eligible to appear for professional certification exams. Hence, subscriptions to resources provided by certifying organizations such as ISACA, ISC2, SANS etc. should be made available in the library.

12. PROGRAM DESCRIPTION

12.1 Title: Master of Science in Cybersecurity

12.2 Department Offering the Program: Computer Networks and Communications

12.3: Period: 2 Years (4 Semesters)

12.4: Language of Study: English

12.5: Total Credit Hours:

The Master program in Cybersecurity has two tracks: Thesis track and Coursework track. The total credit hours required to be completed for these tracks and their distributions is shown in the table below:

CATEGORY	MS THESIS TRACK		MS COURSEWORK TRACK	
	NUMBER OF COURSES	UNITS	NUMBER OF COURSES	UNITS
Core Courses	5	15	6*	18
Elective Courses	4	12	6	18
Thesis / Project	1	09	1	06
Total	**10**	**36**	**13**	**42**

** Includes Project Proposal as a core course*

13. COURSE CONTENTS

13.1 Core Courses

The list of core courses for the **Thesis Track** are:

Course Code	Course Title	Units		
		Lecture	Lab	Total
0914611	Foundations of Cybersecurity	3	0	3
0911622	Cryptography	3	0	3
0914612	Network Security	3	0	3
0912614	Information Security Management	3	0	3
0912615	Research Methodology	3	0	3
0914700	Thesis	0	9	9
	Total	15	9	24

The list of core courses for the **Coursework Track** are:

Course Code	Course Title	Units		
		Lecture	Lab	Total
0914611	Foundations of Cybersecurity	3	0	3
0911622	Cryptography	3	0	3
0914612	Network Security	3	0	3
0912614	Information Security Management	3	0	3
0912615	Research Methodology	3	0	3
0914690	Project Proposal	0	3	3
0914695	Project Implementation	0	6	6
	Total	15	9	24

13.2 Elective Courses

Course Code	Course Title	Units		
		Lecture	Lab	Total
0913631	Hardware Security	3	0	3
0911632	Incident Response and Digital Forensics	3	0	3
0911633	Malware Analysis	3	0	3
0914634	Security in IoT and Wireless Networks	3	0	3
0912635	Security Risk Analysis and Management	3	0	3
0912636	Security Audit and Compliance Testing	3	0	3
0912637	Web Server and Application Testing	3	0	3
0912638	Future Trends in Information Security Research	3	0	3
0914639	Cloud Computing Security	3	0	3
0914640	Network Penetration Testing	3	0	3
0913641	Image Analysis with Security Applications	3	0	3

14. APPLIED EXAMPLE FOR THE PROGRAM

MS with Thesis Track

*(Total **36** Credit Hours)*

TITLE	UNITS		TITLE	UNITS
First Semester			**Second Semester**	
0914611: Foundations of Cybersecurity	3		0911622: Cryptography	3
0912614: Information Security Management	3		0912615: Research Methodology	3
0914612: Network Security	3		Elective I	3
			Elective II	3
	9			12

TITLE	UNITS		TITLE	UNITS
Third Semester			**Fourth Semester**	
Thesis*	0		0914700: Thesis	9
Elective III	3			
Elective IV	3			
	6			9

** Thesis proposal should be started in the third semester*

MS with Coursework Track

*(Total **42** Credit Hours)*

TITLE	UNITS		TITLE	UNITS
First Semester			**Second Semester**	
0914611: Foundations of Cybersecurity	3		0911622: Cryptography	3
0912614: Information Security Management	3		0912615: Research Methodology	3
0914612: Network Security	3		Elective I	3
			Elective II	3
	9			12

TITLE	UNITS		TITLE	UNITS
Third Semester			**Fourth Semester**	
0914690: Project Proposal	3		0914695: Project Implementation	6
Elective III	3		Elective V	3
Elective IV	3		Elective VI	3
	9			12

15. COURSE DESCRIPTIONS

Course Name	*Foundations of Cybersecurity*		أساسيات الأمن السيبراني	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0914611	CS 611	3 (3-0-6)	None
Course Track	☒ Program Core ☐ Electives			

Course Description

Cybersecurity aims to protect the computer system's resources like hardware, software and information. This course This course provides students with understanding of the core concepts of cybersecurity: concepts for confidentiality, integrity and availability; threats, vulnerabilities, threat modeling, risks and access control. This course will also cover basic concepts of application security including secure software system development and operating system security focusing on Windows and Linux. Concepts in secure software development will include security architecture and models. Business continuity planning, disaster recovery, legal aspects of security, physical security and human aspects of cyber security will also be discussed in this course.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Describe** the concepts and theories related to the domain of cybersecurity including threats, vulnerabilities and threat modeling. [A]
2. **Select** appropriate security architectures and models for the system under consideration. [B]
3. **Describe** concepts related to access control and identity management. [A]
4. **Relate** and adapt secure practices for software development security and operating system security. [C]
5. **Identify** the role of physical security, laws and humans in cybersecurity. [A]
6. **Analyze** and **plan** for business continuity and disaster recovery in case of a failure. [C]

Assessment Policy	**Assignments**	15%	**Quiz**	15%	**Project**	-
	Midterm	30%	**Final**	40%	**Others**	-
Textbook	Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, "*Cybersecurity Essentials*", John Wiley & Sons, 2018. ISBN-13: 978- 119362395.					
References	1. Stuart Jacobs, "*Engineering Information Security*", 2nd Edition, Wiley-IEEE Press, 2015. ISBN-13: 978-1119101604. 2. Jason Andress, "*The Basics of Information Security, Understanding the Fundamentals of InfoSec in Theory and Practice*", 2nd Edition, Syngress, 2014. ISBN-13: 978-0128007440. 3. Ross J. Anderson, "*Security Engineering: A Guide to Building Dependable Distributed Systems*", 2nd Edition, Wiley, 2008. ISBN-13: 978-0470068526.					

Course Name	*Network Security*		أمن الشبكات	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0914612	CN 612	3 (3-0-6)	None
Course Track	☒ Program Core ☐ Electives			

Course Description

Most of the serious attacks on computer systems involve exploitation of the underlying network infrastructure, either as the target of attack or as a vehicle to launch attacks on end systems. This course provides an in-depth study of network attacks and corresponding defense mechanisms. The course covers three broad areas within network security: 1) Network Attacks: eavesdropping, distributed denial of service, malware, phishing, worm and virus propagation, social engineering 2) Countermeasures: demilitarized zones, firewalls, intrusion detection systems, deep packet inspection, secure routing protocols, domain name system, secure socket layer, IP security, virtual private networks, VoIP, and 3) Future Trends: security aspects of software-defined networks, Internet of Things, smart gird, cloud based systems and next generation cellular and wireless networks. The course involves reading, lectures, discussions and a term project.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Recall** fundamental network security concepts, techniques, and solutions in computer networks. [A]
2. **Describe** common attack techniques for different types of networks. [A]
3. **Analyze** the security aspects of networked systems to identify potential vulnerabilities. [C, E]
4. **Describe** the core issues and requirements in building secure and effective networks. [A]
5. **Explain** security threats and solutions in next generation networking technologies. [A]
6. **Prepare** reports on possible attacks and network defense mechanisms for given scenarios. [B, C]

Assessment Policy	**Assignments**	20%	**Quiz**	15%	**Project**	-
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	William Stallings, *Network Security Essentials: Applications and Standards*, 6th Edition, Prentice Hall, 2016. ISBN-13: 978-0134527338.					
References	1. Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World*, 2nd Edition, Prentice Hall, 2002. ISBN-13: 978-0130460196. 2. Behrouz A. Forouzan, *Cryptography and Network Security*, 1st Edition, McGraw-Hill Forouzan Networking, 2007. ISBN-13: 978-0073327532.					

Course Name	*Information Security Management*		إدارة أمن المعلومات	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0912614	IS 614	3 (3-0-6)	None
Course Track	☒ Program Core ☐ Electives			

Course Description

Organizations are open to vulnerabilities some of which are predictable and most of them unpredictable. Standard mechanisms may not work for unpredictable incidents. This course focuses on identifying the need for effective security management within organizations, developing knowledge and skills to assess security in organizations, and to incorporate appropriate levels of security in various stages of a system's lifecycle considering legal, cost, privacy and technology constraints. This course establishes a foundation for developing comprehensive and proactive security programs to ensure protection of an organization's information assets. Topics covering governance and security policy, threat and vulnerability management, information leakage, crisis management and business continuity, legal and compliance, security awareness and security implementation considerations are covered in the course. Standards such as the ISO/IEC 27001 which is well-known for providing requirements for an information security management system are briefly discussed.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Identify** and **discuss** the benefits of embedding security throughout an organization. [A, B]
2. **Analyze** information security risks, strategies and methods. [B]
3. **Evaluate** security management requirements. [B]
4. **Apply** the principles of information security management in a variety of contexts. [C]
5. **Relate** and adapt information systems and security solutions to specific business processes and requirements. [C, D]
6. **Identify** and **justify** technical and non-technical solutions to security problems. [C]

Assessment Policy	**Assignments**	15%	**Quiz**	10%	**Project**	10%
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	Mike Vasquez, David Seidl, Jeff T. Parker ,"*The Official (ISC)2 Guide to the CISSP CBK Reference*" , 5th Edition, Wiley, 2019. ISBN: 9781119423348.					
References	1. Adam Gordon, "*Official (ISC)2 Guide to the CISSP Complete Body of Knowledge*", 4th Edition, Auerbach Publications, 2015. ISBN-13: 978-1482262759. 2. David Alexander, Amanda Finch, David Sutton, Andy Taylor, "*Information Security Management Principles*", 2nd Edition, BCS - The Chartered Institute for IT, 2013. ISBN-13: 978-1780171753. 3. Harold F. Tipton, Micki Krause, "*Information Security Management Handbook*", 6th Edition, CRC Press, 2007. ISBN-13: 978-0849374951.					

Course Name	*Cryptography*		التشفير	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0911622	CS 622	3 (3-0-6)	None
Course Track	☒ Program Core ☐ Electives			

Course Description

The objective of this course is to develop a foundational understanding of cryptography as used in the real world. The course introduces the mathematical background required to understand the basics of cryptography. Topics on number theory, modular algebra and discrete log problems are covered. The course advances with classical cipher design and analysis, modern private key block cipher design, modes of use, stream ciphers and analysis. The course provides an extensive coverage of the techniques and methods needed for the proper functioning of the public key encryption algorithms. The key exchange problem and solutions using the Diffie-Hellman algorithm are discussed. The course defines one way functions and trap-door functions and presents the construction of Message Authentication Codes (MAC) and hash algorithms and schemes. The course includes key management and distribution including PKI.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Explain** cryptographic algorithms from classical substitution, transposition and product ciphers to modern ciphers. [A]
2. **Use** and **analyze** classical substitution and transposition ciphers. [B, C, E]
3. **Explain** and **analyze** authentication schemes used in cryptography. [A, B]
4. **Solve** simple number theory problems and compute trivial examples of public key algorithms. [C]
5. **Recognize** the uses, limitations, and appropriate selection of the various categories of cryptographic algorithms. [A]

Assessment Policy	**Assignments**	10%	**Quiz**	15%	**Project**	10%
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	William Stallings, *Cryptography and Network Security: Principles and Practice*, 7th Edition, Prentice Hall, 2017. ISBN-13: 978-0134444284					
References	1. Bruce Schneier, "*Applied Cryptography: Protocols, Algorithms, and Source Code in C*", 2nd Edition, Wiley Publications, 1996. ISBN-13: 978-0471117094 2. Joshua Holden, "*The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption*", 1st Edition, Princeton University Press, 2017. ISBN-13: 978-0691141756					

Course Name	*Research Methodology*		طرق البحث	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0912615	IS 615	3 (3-0-6)	None
Course Track	☒ Program Core ☐ Electives			

Course Description

Research Methodology is a graduate-level course that provides students with basic knowledge and insights into the theory of science, qualitative and quantitative research methodology and research ethics. The course will enable students to read and critically assess technical papers, identify and use criteria for good scientific practice, conduct literature review and use existing knowledge from literature to generalize and identify open areas. Students will be introduced to tools and techniques for selecting research topics, devising research questions, identifying hypotheses, planning and conducting research. Different types of research including case studies, survey, experimental, action and qualitative research are discussed. Statistical methods for data collection, sampling, measurement, data analysis and inference will be covered. Different forms of result analysis including quantitative, qualitative and mixed data analysis will also be covered in detail. The course also introduces students to ethical issues in research and appropriate documentation of research processes and outcomes. After completion of this course, students will have an overall understanding of quality in research and utilize this ability to reason in a critical manner, ensure quality control and further development of the knowledge present in the scientific literature.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Describe** approaches and methods used in the research process. [A]
2. **Conduct** literature search and acquire knowledge from scientific articles. [B]
3. **Formulate** research goals and hypotheses. [B]
4. **Analyze** data using sampling and measurement techniques to infer reliability and validity. [B]
5. **Apply** appropriate data analysis techniques using various statistical methods. [C]
6. **Document** and present research results and outcomes. [D]

Assessment Policy	**Assignments**	20%	**Quiz**	-	**Project**	30%
	Midterm	20%	**Final**	30%	**Others**	-
Textbook	John W. Creswell, "*Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*". 5th Edition, SAGE Publications, 2018. ISBN-13: 978-1506386706.					
References	1. Wayne Booth, Gregory Colomb and Joseph Williams, "*The Craft of Research*", 3rd Edition, University of Chicago Press, 2008. ISBN-13: 978-0226065663. 2. William Navidi, "*Statistics for Engineers and Scientists*", 2nd Edition, McGraw-Hill, 2010. ISBN: 978-0073376332.					

Course Name	*Hardware Security*		أمن الأجهزة	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0913631	CE 631	3 (3-0-6)	0911611
Course Track	☐ Program Core ☒ Electives			

Course Description

Computer Hardware is the most valuable and expensive property for the organizations and business. Problem in hardware components results into malfunction of system and lost or corruption of file. This course is designed to study the approaches for hardware security which enables the students for protection of computer hardware from the physical factors like fire, heat, incorrect voltage, dust or malicious activities. Upon completing the course, students will understand the vulnerabilities in current digital system design flow and the physical attacks to these systems. The students explore the secure processor architectures, and the concepts of channel attacks, Hardware Trojan and trusted integrated circuit (IC) design, Trust platform module (TPM), and physical unclonable function (PUF).

Course Outcomes

After the completion of this course, the student will be able to:

1. **Define** Intellectual Property Protection and **analyze** the social impact of intellectual property law and policy. [A]
2. **Discuss** and **analyze** the resilience of crypto implementations against side channel attacks. [A]
3. **Design, analyze** and **illustrate** reduction of logical expressions to implement sequential systems. [B]
4. **Evaluate** and **apply** digital watermarking for information security. [B]

Assessment Policy	**Assignments**	10%	**Quiz**	-	**Project**	20%
	Midterm	20%	**Final**	40%	**Others**	10%
Textbook	Bhunia, Swarup, and Mark Tehranipoor. Hardware Security: A Hands-on Learning Approach. Morgan Kaufmann, 2018.					
References	1. Mukhopadhyay, Debdeep, and Rajat Subhra Chakraborty. *Hardware Security: Design, Threats, and Safeguards.* Chapman and Hall/CRC, 2014. 2. Y. Younan, W. Joosen, and F. Piessens, "Runtime countermeasures for code injection attacks against C and C++ programs," ACM Computing Surveys 44(3):1-28, June 2012.					

Course Name	*Incident Response with Digital Forensics*		الاستجابة للحوادث مع التحليل الجنائي الرقمي	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0911632	CS 632	3 (3-0-6)	0914611, 0914612
Course Track	☐ Program Core ☒ Electives			

Course Description

Every organization, which uses computers to support their operations, are facing attacks. This course will equip the students to detect any attempt made to attack an organization and take appropriate actions to either stop that attack or take appropriate actions to mitigate its effect. The course starts with brief discussion on Intrusion Detection/Prevention systems (IDPS) architecture and all its components, and IDPS tools. After that, digital forensics process will be discussed in detail with focus on different tools to retrieve and analyze forensic data. Focus is then shifted to applying IDPS and concepts of forensics to handle security incidents in organizations. The course will discuss different elements in detail including incident response policy and incident team structure. The course will discuss the concepts for detecting and analyzing the incidents including attack vectors, incident analysis, containment and eradication strategy, handling, eradication and recovery and evidence retention. The coordination and information sharing between different teams will also be discussed to provide the flavor of actual working in organizations.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Explain** the detailed working of the forensics process. [A]
2. **Explain** all the components and workings of an Intrusion Detection / Prevention Systems. [A]
3. **Describe** the incident response process in Digital Forensics and Intrusion Detection / Prevention Systems. [A]
4. **Analyze** the logs obtained from monitoring the behavior of observed systems during attack. [B, E]
5. **Decide** and **Plan** the incident response for analyzed attacks. [C, D]

Assessment Policy	**Assignments**	10%	**Quiz**	10%	**Project**	15%
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	Ric Messier, "*Network Forensics*", 1st Edition, Wiley, 2017, ISBN-13: 978-1119328285.					
References	1. Jason T. Luttgens, Mathew Pepe and Kevin Mandia, "*Incident Response & Computer Forensics*", 3rd Edition, Mc-Graw Hill Education, 2014. ISBN-13: 978-0071798686. 2. Paul Cichonski, Tom Millar, Tim Grance and Karen Scarfone, "*Computer Security, Incident Handling Guide*", SP 800-61 R2, NIST US Dept. of Commerce, 2012. 3. Don Franke, "*Cyber Security Basics: protect your organization by applying the fundamentals*", 1st Edition, CreateSpace Independent Publishing Platform, 2016. ISBN-13: 978-1522952190.					

Course Name	*Malware Analysis*		تحليل البرمجيات الضارة	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0911633	CS 633	3 (3-0-6)	0911622
Course Track	☐ Program Core ☒ Electives			

Course Description

The increasingly networked nature of the world has also enabled the spread of various types of malicious software, from a simple adware to more sophisticated Cyber-weaponry. This course will provide the students with the knowledge and skills to detect, analyze, understand, control, and eradicate malware which is an increasingly important issue in information security. This course provides students with an understanding of the issues and techniques used in malware detection and classification. This course will introduce students to the detailed process of malware analysis, packing and unpacking of malwares, static and dynamic analysis of malware, and the malicious activities and techniques. The course also focusses on how to overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques. The course will equip the students with the skills needed to use advanced tools and methodologies that perform malware analysis.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Analyze** modern malware samples using both static and dynamic analysis techniques. [B]
2. **Explain** executable formats, Windows internals and API, and analysis techniques. [A]
3. **Identify** specific coding constructs in disassembly. [B]
4. **Apply** techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples. [E]
5. **Use** industry standard tools to perform Malware Analysis on existing Operating Systems. [E]

Assessment Policy	**Assignments**	10%	**Quiz**	10%	**Project**	15%
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	Christopher C. Elisan, "*Advanced Malware Analysis*", 1st Edition, McGraw-Hill/Osborne, 2015. ISBN-13: 978-0071819749.					
References	1. Michael Sikorski, Andrew Honig "*Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software*", 1st Edition, No Starch Press, 2012. ISBN-13: 978-1593272906. 2. Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard, "*Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*", 1st Edition, Wiley Publishers, 2011. ISBN-13: 978-0470613030.					

Course Name	*Security in IoT & Wireless Networks*		أمن إنترنت الأشياء والشبكات اللاسلكية	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0914634	CN 634	3 (3-0-6)	0914612
Course Track	☐ Program Core ☒ Electives			

Course Description

This course introduces the fundamentals and state of the art in wireless network security. The course will cover wireless vulnerabilities and attacks at various layers of the protocol stack, from the physical layer up to the application layer and include service security issues. The first part of the course addresses conventional wireless networks and begins by introducing the wireless security basics and physical layer security including wireless electronic warfare: jamming, anti-jamming, source localization and target-tracking. Subsequently, link-layer threats are discussed including wireless encryption, selfish and malicious behavior. Wireless multihop networks are explored from network security, privacy, trust, and reputation perspective along with attacks such as black hole, flooding, Sybil, and warm hole. The course briefly addresses security aspects in cellular networks. The second part of the course focuses on vulnerabilities, attacks and countermeasures for the Internet of Things (IoT) ecosystem including IoT security architecture, security classification, IoT privacy, authentication and authorization, cloud integration, attacks and mitigation strategies, and techniques for IoT communication and applications.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Describe** security architecture of different wireless networks. [A]
2. **Analyze** existing security mechanisms of enterprise wireless networks. [B]
3. **Propose** appropriate and efficient security mechanisms to secure enterprise wireless networks. [D]
4. **Describe** the security and privacy issues and threats for Internet of Things. [A]
5. **Identify** and **justify** security countermeasures against attacks in Internet of Things. [A]

Assessment Policy	**Assignments**	15%	**Quiz**	20%	**Project**	-
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	Matthew S. Gast, "*802.11 Wireless Networks: The Definitive Guide: Enabling Mobility with Wi-Fi Networks*", 3rd Edition, O'Reilly Media, 2018. ISBN-13: 978-1491963548.					
References	1. Lei Chen, Jiahuang Ji, Zihong Zhang, "*Wireless Network Security: Theories and Applications*", 1st Edition, Springer, 2013. ISBN-13: 978-3642365102. 2. Brian Russell, "*Practical Internet of Things Security*", 1st Edition, Packt Publishing, 2016. ISBN-13: 978-1785889639.					

Course Name	*Security Risk Analysis and Management*		تحليل وإدارة المخاطر الأمنية	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0912635	IS 635	3 (3-0-6)	0912614
Course Track	☐ Program Core ☒ Electives			

Course Description

Risk management processes assesses the overall security condition of organizations, analyses the collected data and plan to select appropriate security controls to implement it. The objective of this course is to enable students to understand the details of risk management and develop a basic risk management program for security of organization's information assets. The course will discuss in detail the phases of risk management lifecycle, the details of risk management process including risks and their components, risk assessment and risk mitigation, different risk assessment frameworks like COBIT, ISO/IEC standards, NIST framework etc., risk profiling, risk treatment strategies and risk monitoring. Security policies help to define the ways to implement the planned security in the form of written documents like security procedures, guidelines and recommendations. The course will also focus on understanding different types of security policies including general security policy, issue specific policy and systems policy. At the end, the course will focus on planning and building a risk management program in detail.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Describe** the importance and evolution of risk management for organization's information security. [A]
2. **Explain** the phases of risk management life cycle including risk assessment, risk mitigation and validation. [A]
3. **Evaluate** organization's information assets and identify risks for them. [B]
4. **Analyze** the identified risks to decide about their mitigation. [C]
5. **Decide** and **Plan** risk management program and security policies for organization. [C, D]

Assessment Policy	**Assignments**	10%	**Quiz**	10%	**Project**	15%
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	Freund, J., & Jones, J, "*Measuring and managing information risk: A FAIR Approach*", 1st Edition, Butterworth-Heinemann, 2015. ISBN-13: 9780127999326					
References	1. Evan Wheeler, "*Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*", 1st Edition, Syngress, 2011. ISBN-13: 978-1597496155 2. Thomas R. Peltier, "*Information security risk analysis*", 3rd Edition, Auerbach Publications, 2010. ISBN-13: 978-1439839560					

Course Name	*Security Audit and Compliance Testing*		تدقيق الأمن وفحص الامتثال	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0912636	IS 636	3 (3-0-6)	0912614
Course Track	☐ Program Core ☒ Electives			

Course Description

Organizations are compelled by state laws and business needs to implement cyber security and defined standards lay down the compliance requirements to achieve it. This course starts with focus on compliance topics including need of security compliance for information systems, compliance overview along with domestic and international compliance laws. The course then focuses on auditing modern computer systems, common frames of reference by establishing a baseline of technological understanding of risks, security control objectives and standards (e.g. COSO, SOx, ISACA COBIT, NIST framework) to perform IT audit function. The course provides analytical skills to apply audit planning process and management concepts to IT systems. The course discusses the evidence of audit success by deciding the criteria for success, statistical sampling and methods of evaluation by quantitative methods or simulations. The applied knowledge to perform auditing for different technological systems including IT infrastructure, application controls, operating systems and information systems will be discussed towards end including report writing that documents the findings uncovered during the auditing process.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Describe** the basic concepts and standards of information compliance. [A]
2. **Describe** the fundamental concepts of IT auditing and security controls to ensure acceptable security level for organizations. [A]
3. **Explain** the process and procedures to conduct audit according to different Auditing frameworks and standards. [A]
4. **Analyze** the compliance, legal and security policy requirements to implement security controls for security of organization. [B]
5. **Select** the most suitable and cost effective security controls according to risk management program strategy. [C]
6. **Plan** audit for different application level controls and systems. [D]

Assessment Policy	**Assignments**	10%	**Quiz**	10%	**Project**	15%
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	Martin Weiss, Michael G. Solomon, "*Auditing IT Infrastructures for Compliance (Information Systems Security & Assurance)*", 2nd Edition, Jones & Bartlett Learning, 2015. ISBN-13: 978-1284090703.					
References	1. Richard E. Cascarino, "*Auditor's Guide to IT Auditing*", 2nd Edition, Wiley, 2012. ISBN-13: 978-1118147610. 2. Robert R. Moeller, "*IT Audit, Control and Security*", 2nd Edition, Wiley, 2010. ISBN-13: 978-0471406761.					

Course Name	*Web Server and Application Testing*		فحص خوادم وتطبيقات الويب	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0912637	IS 637	3 (3-0-6)	0914611
Course Track	☐ Program Core ☒ Electives			

Course Description

Current technology has given us access to huge amounts of information on the web and simplified tasks. Web has become the primary vector for infecting computers. This course covers contemporary web application vulnerabilities and exploitation techniques based on the Open Web Application Security Project (OWASP). Students will be introduced to different methods and techniques that are used when attacking web servers including password cracking, SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) to name a few. Moreover, students will be provided with the knowledge and skills to implement protection against these attacks. Students will be familiarized with tools and techniques for performing attacks related to authentication, session management, access control, data stores, server-side components, and users. Finally, the students will be introduced to the web application hacker's methodology that provides a framework to check and implement protection schemes against popular web server and application attacks.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Define** common web infrastructure attack vectors and database vulnerabilities. [A]
2. **Apply** techniques to identify vulnerabilities existing in web servers and applications. [B, E]
3. **Use** tools and skills to attack web infrastructures. [B, E]
4. **Discuss** and **use** different procedures to check and implement protection schemes in web servers and web based applications. [C, D]

Assessment Policy	**Assignments**	25%	**Quiz**	-	**Project**	20%
	Midterm	25%	**Final**	30%	**Others**	-
Textbook	Juned Ahmed Ansari, "*Web Penetration Testing with Kali Linux*", 3rd Edition, Packt Publishing Ltd., 2018. ISBN: 9781788623377.					
References	1. Dafydd Stuttard and Marcus Pinto, "*The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*", 2nd Edition, Wiley, 2011. ISBN-13: 978-8126533404 2. Prakhar Prasad, "*Mastering Modern Web Penetration Testing*", 1st Edition, Packt Publishing Limited, 2016. ISBN-13: 9781785284588 3. Peter Kim "*The Hacker Playbook 2: Practical Guide to Penetration Testing*" 1st Edition, CreateSpace Independent Publishing Platform, 2015. ISBN-13: 978-1512214567					

Course Name	*Future Trends in Information Security Research*		الاتجاهات المستقبلية في أبحاث أمن المعلومات	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0912638	IS 638	3 (3-0-6)	0914611, 0912615
Course Track	☐ Program Core ☒ Electives			

Course Description

Cybersecurity is an evolving field wherein unpredicted emergence of disrupting innovations may radically change the existing information security landscape. The aim of this course is to provide students with near-future information security issues that are related to new technologies, services, and business models. Advancement in tools and techniques used for IT risk management, cybersecurity intelligence, securing networks, software systems and web applications will be discussed. Prominent topics of study may include use of Block chain technologies for information security solutions, expanding role of artificial intelligence in enhancing the resilience of computer infrastructure, use of crowdsourcing for reporting information security incidents and cybersecurity testing, and establishment of international legal framework to share information on cybersecurity incidents. The course is taught by delivering lectures, conducting group discussions on selected case studies and discussing peer-reviewed research articles published in reputed InfoSec journals.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Identify** the issues and trends in information security. [B]
2. **Recognize** the recent approaches, methods and tools used in the field of information security. [A]
3. **Identify** factors and attributes that affect the realization of the trends in information security. [B]
4. **Develop** skills to conduct independent research in contemporary topics in information security. [E]

Assessment Policy	**Assignments**	10%	**Quiz**	10%	**Project**	15%
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	No specific textbook for this course. Selected scientific papers, excerpts from case studies and books covering each topic will be used.					
References	1. Stamp, M., '*Introduction to Machine Learning with Applications in Information Security*', 1st Edition, CRC Press, 2017. ISBN-13: 978-1138626782 2. Resources provided by InfoSec certifying organizations such as ISACA, ISC2, SANS					

Course Name	*Cloud Computing Security*		أمن الحوسبة السحابية	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0914639	CN 639	3 (3-0-6)	0914612
Course Track	☐ Program Core ☒ Electives			

Course Description

As cloud computing increases its footprint throughout the world, unresolved issues related to security and privacy, data integrity and availability are raised. The fundamental question is how to protect the critical data that is increasingly being stored in the cloud? This course explores cloud computing models, thread models and security issues pertaining to cloud-based systems and explores how to build a security strategy that keeps data safe and mitigates risk. The major topics covered include infrastructure security, attacks and attack surfaces in a cloud, data security in clouds, secure computation and outsourcing, privacy in clouds, virtual machine security, trustworthy clouds, cloud forensics, cloud network security, cloud malware and regulatory compliances. The course also discusses industry best practices for cloud security and discusses how to architect and configure security-related features in a cloud platform.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Recall** fundamental security concerns in cloud computing systems. [A]
2. **Describe** the mechanisms used to ensure privacy and trust in cloud computing platforms. [A]
3. **Explain** key design considerations when architecting network infrastructure for cloud security. [A]
4. **Evaluate** and **prepare** reports on the threats and security countermeasures of given cloud computing systems. [C, D]

Assessment Policy	**Assignments**	15%	**Quiz**	20%	**Project**	-
	Midterm	25%	**Final**	40%	**Others**	-
Textbook	John R. Vacca, "*Cloud Computing Security: Foundations and Challenges*", 1st Edition, CRC Press, 2016. ISBN-13: 978-1482260946					
References	1. Vic (J.R.) Winkler, "*Securing the Cloud: Cloud Computer Security Techniques and Tactics*", 1st Edition, Syngress, 2011. ISBN-13: 978-1597495929 2. Ray A. Rothrock, Richard A. Clarke, "*Digital Resilience: Is Your Company Ready for the Next Cyber Threat?*", 1st Edition, AMACOM, 2018. ISBN-13: 978-0814439241 3. Tim Mather, Subra Kumaraswamy, Shahed Latif, "*Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*", 1st Edition, O'Reilly Media, 2009. ISBN-13: 978-0596802769					

Course Name	*Network Penetration Testing*		فحص اختراق الشبكات	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0914640	CN 640	3 (3-0-6)	0914612
Course Track	☐ Program Core ☒ Electives			

Course Description

Penetration testing enables ethical hackers to legally attempt to locate and exploit computer systems with the intention to make those systems secure. This course covers tools, techniques, and methodologies required for performing network penetration testing. It covers all phases of penetration testing as outlined by different standards such as the Penetration Testing Execution Standard (PTES). Students will be able to build their own penetration testing infrastructure that includes the hardware, software, network infrastructure, and tools needed to conduct penetration tests. The course discusses the tools and techniques required to retrieve sensitive information about a target environment; map the target environment's attack surface by creating a comprehensive inventory of machines, accounts, and potential vulnerabilities; understand different kinds of exploits that penetration testers use to compromise target machines, and post-exploitation activities including gathering information from compromised machines. High-level structure of a penetration test report to document findings will also be discussed in the course.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Recall** the penetration process from information gathering to an actual system penetration. [A]
2. **Perform** information gathering to facilitate effective network penetration. [B, E]
3. **Use** different approaches to compromise modern network infrastructures. [B, E]
4. **Describe** approaches to evade current attack detection mechanisms deployed in networks. [A]
5. **Present** results of a penetration test in the form of a report. [D]

Assessment Policy	**Assignments**	25%	**Quiz**		**Project**	20%
	Midterm	25%	**Final**	30%	**Others**	-
Textbook	Peter Kim, "*The Hacker Playbook 3: Practical Guide to Penetration Testing*", 3rd Edition, Independently published, 2018. ISBN-13: 978- 1980901754.					
References	1. Patrick Engebretson, "*The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*", 2nd Edition, Syngress, 2013. ISBN-13: 978-0124116443. 2. Georgia Weidman, "*Penetration Testing: A Hands-On Introduction to Hacking*" 1st Edition, No Starch Press, 2014. ISBN-13: 978-1593275648.					

Course Name	*Image Analysis with Security Applications*		تحليل الصور مع تطبيقات الأمن	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0913641	CE 641	3 (3-0-6)	0911622
Course Track	☐ Program Core ☒ Electives			

Course Description

This course aims to establish knowledge and skills necessary for efficient implementations of image analysis with security applications. The course is organized with image processing, pattern recognition and visual security issues, focusing on image acquisition, digitization, segmentation, shape representation and description. This will provide a solid foundation for students to apply image analysis techniques in image transformation, pattern recognition and security applications.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Describe** digital image acquisition with respect to sampling, quantization, and associated noise. [A]
2. **Define, describe** and **compare** different edge detection techniques for image analysis. [A, B]
3. **Apply** image enhancement techniques at the point and neighborhood level. [C]
4. **Evaluate** various machine learning architectures and algorithms used in image segmentation, clustering and classification. [C]
5. **Develop** an ability to explore and analyze the impact of potential development of image processing in digital watermarking. [C, E]
6. **Develop** skills and critical understanding of the principles of image analysis and processing, using the MATLAB/Visual C++ platform. [E]

Assessment Policy	**Assignments**	10%	**Quiz**	-	**Project**	20%
	Midterm	20%	**Final**	40%	**Others**	10%
Textbook	Rafael C. Gonzalez, Richard E. Woods, "*Digital Image Processing*", Pearson, 4th Edition, 2017, ISBN-10: 0133356728, ISBN-13: 978-0133356724.					
References	1. W. K. Pratt, "**Digital Image Processing**", J. Wiley, 2007, ISBN 0123797772. 2. Wilhelm Burger and Mark J. Burge, "**Digital Image: An Algorithmic Introduction Using Java**", 2nd Edition, Springer-Verlag London, 2016, ISSN 1868-095X.					

Course Name	*Project Proposal*		مقترح المشروع	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0914690	CN 690	3 (0-3-3)	Department Approval
Course Track	☒ Program Core ☐ Electives			

Course Description

Project Proposal emphasizes on application of the theoretical concepts of software analysis and design learned during the course work. The analysis component comprises of preparing formal Software Requirements Specifications (SRS) document including problem statement, scope, justification, requirements, cost estimation, assumptions, limitations, methodology and tools to be used in project development. The assumption should be taken in such a way that scope of the problem becomes clear and well defined in the problem statement. All the functional and non-functional requirements of the system must be identified and analyzed in the proposal. The students will be encouraged to develop/describe logical model of the proposed system based on the requirements. The design component of the course includes prototype including input and output of the proposed system.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Identify** and **define** problem statement. [B]
2. **Define** and **justify** scope of the problem. [B]
3. **Gather** and **analyze** system requirements. [B]
4. **Propose** an optimized solution among the existing solutions. [C]
5. **Practice** software analysis and design techniques learned during the course work. [E]
6. **Prepare** and **present** a technical report. [D]

Assessment Policy	**Committee Evaluation**	**Report Evaluation**	35%	**Supervisor Evaluation**	30%
		Oral Examination	35%		
Textbook	There is no single textbook for this course. The students are encouraged to select and read various related texts under the recommendation of their supervisor.				
References	1. Jeremy T. Miner, Lynn E. Miner, "*Proposal Planning & Writing*", 4th Edition, Greenwood, 2008. ISBN-13: 978-0-313-35674-2. 2. Wayne Booth, Gregory Colomb and Joseph Williams, "*The Craft of Research*", 3rd Edition, University of Chicago Press, 2008. ISBN-13: 978-0226065663. 3. William Navidi, "*Statistics for Engineers and Scientists*", 2nd Edition, McGraw-Hill, 2010. ISBN: 978-0073376332.				

Course Name	*Project Implementation*		تنفيذ المشروع	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0914695	CN 695	6 (0-6-6)	0914690
Course Track	☒ Program Core ☐ Electives			

Course Description

In this course, the students will be required to implement proposed design of the project. The students will review the design specification and make any necessary enhancements to synchronize the implementation details. The students will identify and learn the use of tools required for the project implementation. The students will be expected to: prepare application architecture, code, debug, document, and test the application software within suggested timeframe. A key focus of the course is to emphasize the quality of software project through various evaluation aspects such as professional coding style, documentation of code, intuitive user interface design, input validation, verification and user guide. The students will be further required to evaluate the developed system by generating test cases of the critical components of the designed model.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Design**, **develop** and **evaluate** a computer-based system to meet a set of solution requirements. [C, D, E]
2. **Prepare** proper documentation of software projects following the standard guidelines. [D]
3. **Enhance** written and oral communications skills with a range of audience [E]
4. **Recognize** professional, ethical, legal and social issues related to IT. [E]
5. **Identify** the need for engaging in continuing professional development. [A]

Assessment Policy	**Committee Evaluation**	**Report Evaluation**	35%	**Supervisor Evaluation**	30%
		Oral Examination	35%		
Textbook	There is no single textbook for this course. The students are encouraged to select and read various related texts under the recommendation of their supervisor.				
References	1. Jeremy T. Miner, Lynn E. Miner, "*Proposal Planning & Writing*", 4th Edition, Greenwood, 2008. ISBN-13: 978-0-313-35674-2. 2. Wayne Booth, Gregory Colomb and Joseph Williams, "*The Craft of Research*", 3rd Edition, University of Chicago Press, 2008. ISBN-13: 978-0226065663. 3. William Navidi, "*Statistics for Engineers and Scientists*", 2nd Edition, McGraw-Hill, 2010. ISBN: 978-0073376332.				

Course Name	*Thesis*		الأطروحة (الرسالة)	
Course Information	**Course Code**	**Course No.**	**Credit Hour**	**Prerequisite(s)**
	0914700	CN 700	9 (0-9-9)	Department Approval
Course Track	☒ Program Core ☐ Electives			

Course Description

Student will choose a research topic under supervision of a faculty member. After approval of the dissertation subject, the student needs to define objectives of the research and prepare the research proposal. In the proposal, he/she will be required to (i) conduct an exhaustive survey (ii) identify and define the problem clearly (iii) decide scope of the problem and provide its assumptions and limitations (iv) ensure the originality of the research proposal (v) suggest the approach and methodology used in the research and (vi) present the expected results. At the successful presentation of the proposal, student will be asked to submit the proposal. The student will apply the proposed methodology to solve the problem. After completion, student will submit the dissertation and then student will defend the dissertation.

Course Outcomes

After the completion of this course, the student will be able to:

1. **Conduct** survey of research issues. [B, E]
2. **Practice** research techniques, tools and methodologies. [E]
3. **Work** independently and take initiatives in academic or professional environment. [E]
4. **Develop** writing and oral presentation skills. [D, E]

Assessment Policy	**Dissertation Evaluation**	40%
	Dissertation Oral Examination	60%
Textbook	There is no single textbook for this course. The students are encouraged to select and read various related texts under the recommendation of their supervisor.	
References	1. Wayne Booth, Gregory Colomb and Joseph Williams, "*The Craft of Research*", 3rd Edition, University of Chicago Press, 2008. ISBN-13: 978-0226065663. 2. William Navidi, "*Statistics for Engineers and Scientists*", 2nd Edition, McGraw-Hill, 2010. ISBN: 978-0073376332. 3. Berndtsson et al., "*Thesis Projects: A guide for Students in Computer Science and Information Systems*", 2nd Edition, Springer, 2008. ISBN-13: 978-1-84800-008-7	