جامعة الإسراء
ISRA UNIVERSITY

Course Syllabus

According to JORDAN National Qualification Framework (JNQF)

Course Name: Information Security protocols

Course Number: 06043254

General Course Information:

Course title	**Information Security Protocols**
Course number	**06043254**
Credit hours	**3 hrs.**
Education type	**[Face-to-Face] 3**
Prerequisites/corequisites	Introduction to Cyber Security (06042150)
Academic Program	Cyber Security
Program code	604
Faculty	Information Technology
Department	Cyber Security
Level of course	**3**
Academic year /semester	**3,2**
Awarded qualification	**Bachelor**
Other department(s) involved in teaching the course	**None**
Language of instruction	**English**
Date of production/revision	**2021/2022**

Course Coordinator:

Coordinator's name	**Dr. Ahmad alshanty**
Office No	**4225**
Office Phone extension number	**2504**
Office Hours	**TBA**
Email	**ahmad.alshanty@iu.edu.jo**

Other Instructors:

Coordinator's name	**Dr. Ahmad alshanty**
Office No	**4225**
Office Phone extension number	**2504**
Office Hours	**TBA**
Email	**ahmad.alshanty@iu.edu.jo**

Course Description *(English/Arabic)*:

English	*Reviews Contemporary Security Protocols and their Properties, Including Confidentiality, Authentication, Secure Group Communication, Privacy, and anonymity. Covers Cryptographic Primitives, as Well as Standard Formal Models and tools Used for Mechanized Verification of Secure Systems, Including Model Checking, Constraint Solving, Process Algebras, Protocol Logics, and Game theory.*
Arabic	بروتوكولات الأمان المعاصرة وخصائصها ، بما في ذلك السرية والمصادقة والتواصل الآمن للمجموعة والخصوصية وإخفاء الهوية. دراسة أساسيات التشفير، بالإضافة إلى النماذج والأدوات الرسمية القياسية المستخدمة للتحقق الآلي من الأنظمة الآمنة ، بما في ذلك فحص النموذج وحل القيود وعملية الجبر ومنطق البروتوكول ونظرية الألعاب.

Textbook: ***Author(s), Title, Publisher, Edition, Year, Book website.***

1- Internet Security Protocols: Protecting IP Traffic 1st Edition, Prentice Hall; 1st edition (July 24, 2000)
2- Cryptography and Network Security Principles and Practice Sixth Edition, William Stallings, Pearson; 6th edition, 2016

References: ***Author(s), Title, Publisher, Edition, Year, Book website.***

1- "CS 356- Lecture 27 Internet Security Protocols ", 2013.
2- Mohsen Toorani,"Security Protocols in a Nutshell",2016.
3- Christopher Kruegel, "Internet Security", Automation Systems Group (E183-1)
4- Online teching :"INTERNET SECURITY PROTOCOL"
5- Radia Perlman, "Network Security Protocols:A Tutorial", May 2005.
6- https://www.slideserve.com/elliot/internet-security-protocols 7- https://www.digicert.com/ssl/

Course Educational Objectives (CEOs):

1.	Understand the security protocols characteristics and specification for a particular system.
2.	Performing a detailed analysis of information security protocols properties.
3.	Extending an existing tool or method to support analysis of a new class of information security Protocols properties.
4.	Conducting a theoretical study of the relationship between several models.

Intended Learning Outcomes (ILO's):

	Subject Intended learning outcomes (ILOs) describe what students are expected to know and be able to do at the end of the course. These outcomes are related to the knowledge, skill and competence that students acquire:	**Relationship to CEOs**	**Contribution to PLOs**	**Bloom Taxonomy Levels***	**Descriptors****
A	**Knowledge and Understanding:**				
A1	Understand what Information Security Protocols.	**1**	**a, b**	**2**	**k**
A2	Know the fundamental strategies of developing and tracing information Security protocols.	**2,3**	**a**	**1**	**k**
A3	Ability to understand the functionality of Information security Protocols components, Architecture, and the interaction between them.	**2,3,4**	**b**	**2**	**k**
B	**Intellectual skills:**				
B1	Know the different types of skills required to analyze information Security protocols based on the key concepts.	**1,2,3,4**	**a,b**	**1**	**k**
B2					
B3					

C	**Subject specific skills:**				
C1	The ability to analyze the Information security Protocols challenges and proposed solutions.	**1,2,3,4**	**a,b,f**	**4**	**s**
D	**Transferable skills:**				
D1	Design and implement information Security protocols.	**1,2,3,4**	**a,b,c,f**	**3**	**c**

***Bloom Taxonomy Levels**

Level #	1	2	3	4	5	6
Level Name	Knowledge	Comprehension	Application	Analysis	Evaluation	Synthesis

**** Descriptor (National Qualification Framework Descriptors): K : Knowledge, S: Skill, C: Competency.**

Program Learning Outcome (PLOs):

Program Learning Outcomes describe what students are expected to know and be able to do by the time of graduation. These relate to the knowledge, skills, and behaviours that students acquire as they progress through the program. A graduate of the (_____) program will demonstrate:		Descriptors**		
		K	S	C
1.	Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.		✓	
2.	Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.		✓	
3.	Communicate effectively in a variety of professional contexts.			✓
4.	Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.	✓		
5.	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.		✓	
6.	Apply security principles and practices to maintain operations in the presence of risks and threats. [CY]			✓

**** Descriptors according to the national qualifications framework (K: knowledge, S: skill, C: Competency)**

Weekly Schedule *(please choose the type of teaching)*

✓ Face to Face

□ Hybrid *(**2 Lectures** Face – To - Face **+1 Lecture** Asynchronous)*

□ Hybrid (*1 Lectures* Face – To - Face ***+1 Lecture*** Asynchronous)

□ Online *(**2 Lectures** Synchronous **+1 lecture Asynchronous**)*

Week	First Hour (*Face – To - Face*)	Second Hour (*Face – To - Face*)	Third Hour (*Face – To - Face*)	Ach. ILOs	Ach. PLOs	Descriptors**
1	Course outline	Introduction to protocols	Introduction to Murphi.	A1, A2, A3	1,2	k
2	SSL/TLS case study.	SSL/TLS case study.	SSL/TLS case study	A1, A2, A3	1,2	k
3	Overview of IP security. Internet Key Exchange (IKE) protocol	Overview of IP security. Internet Key Exchange (IKE) protocol	Overview of IP security. Internet Key Exchange (IKE) protocol	A1, A2, A3	1,2	k
4	Introduction to process algebra. Modeling security protocols	Introduction to process algebra. Modeling security protocols	Introduction to process algebra. Modeling security protocols	A1, A2, A3	1,2	k
5	Just Fast Keying (JFK) protocol.	Security as observational equivalence. JFK protocol in applied	Security as observational equivalence. JFK protocol in applied	A1, A2, A3	1,2	k

6	Protocols for anonymity	Probabilistic model checking.	Probabilistic model checking.	A1, A2, A3	1,2	k
7	Probabilistic contract signing.	Compositional protocol logic.	Compositional protocol logic.	A1, A2, A3	1,2	k
8	Inductive method. Analyzing SET with the inductive method.	Inductive method. Analyzing SET with the inductive method.	Inductive method. Analyzing SET with the inductive method.	A1, A2, A3	1,2	k
9	Symbolic constraint solving for security protocols.	Symbolic constraint solving for security protocols.	Symbolic constraint solving for security protocols.	A1, A2, A3	1,2	k
10	Formal definitions of security for symmetric ciphers.	Formal definitions of security for symmetric ciphers.	Formal definitions of security for symmetric ciphers.	A1, A2, A3	1,2	k
11	Formal model for secure key exchange. Simulatability based	Formal model for secure key exchange. Simulatability based	Formal model for secure key exchange. Simulatability based	A1, A2, A3, B1, C1, D1	1,2,3,4	K,C,S
12	Probabilistic polynomial-time process calculus	Probabilistic polynomial-time process calculus	Probabilistic polynomial-time process calculus	A1, A2, A3, B1, C1, D1	1,2,3,4	K,C,S
13	Computational soundness of formal models.	Computational soundness of formal models.	Computational soundness of formal models.	A1, A2, A3, B1, C1, D1	1,2,3,4	K,C,S
14	Fair exchange and contract signing protocols.	Fair exchange and contract signing protocols.	Fair exchange and contract signing protocols.	A1, A2, A3, B1, C1, D1	1,2,3,4	K,C,S
15	Game-based verification of contract signing protocols.	Game-based verification of contract signing protocols.	Game-based verification of contract signing protocols.	A1, A2, A3, B1, C1, D1	1,2,3,4	K,C,S
16		Final Exam				

* **K: Knowledge, S: Skills, C: Competency**

Teaching Methods and Assignments:

Development of ILOs is promoted through the following teaching and learning methods:

- **Interactive videos**
- **Practice Labs**
- **Discussion Forums**
- **Quizzes**
- **Other Interactive online activities**

- **Reports**

Course Policies:

A- Attendance policies:

The maximum allowed absences is 15% of the lectures.

B- Absences from exams and handing in assignments on time:

Midterm exam can be retaken based on approval of excuse by the instructor's discretion.

Not handing assignment on time will incur penalties.

C- Academic Health and safety procedures

D- Honesty policy regarding cheating, plagiarism, and misbehaviour:

Cheating, plagiarism, misbehaviour will result in zero grade and further disciplinary actions may be taken.

E- Grading policy:

- All homework is to be posted online through the e-learning system.
- Exams will be marked within 72 hours and the marked exam papers will be handed to the students.
- Online Activities (Course Videos, Practice labs, Discussion Forums, Quizzes) **20%**
- Midterm **30%**
- Final Exam **50%**

F- Available university services that support achievement in the course: **E-Learning Platform, Labs, Library.**

Required equipment:

- **PC / Laptop with webcam and mic**
- **Internet Connection**
- **Access to the IU E-Learning Platform at: https://elearn.iu.edu.jo/**
- **E-learning plan**
- Satisfaction questionnaires for online and face-to-face learning
- Software for e-learning
- Training

Assessment Tools implemented in the course:

X Final Exam
X Midterm Exam
X Quizzes
X Homework
- Practice Labs
- Discussion Forums
- Periodic reports for learning assessment
- Improvement plans for online or face-to-face teaching
- Others:…….

Responsible Persons and their Signatures:

Course Coordinator	**Dr. Ahmad Alshanty**	**Completed Date**	**23/6 /2022**
		Signature	

Received by (Department Head)	**Dr. Hasan Kanaker**	**Received Date**	/ /
		Signature	