

Course Syllabus

1.	Course title	Computer Security
2.	Course number	1901463
3.	Credit hours (theory, practical)	3
	Contact hours (theory, practical)	3
4.	Prerequisites/corequisites	Computer Networks (1901361)
5.	Program title	Computer Science
6.	Year of study and semester (s)	Fourth year
7.	Final Qualification	Bachelor degree
8.	Other department (s) involved in teaching the course	None
9.	Language of Instruction	English
10.	Date of production/revision	September 1, 2019
11.	Required/ Elective	Required

12. Course Coordinator:

Dr. Khair Eddin Sabri
Office numbers: KASIT 117, Phone number: 22557
Office hours:
Sun, Tue: 9:00 – 10:00, Wed: 9:30-11
Email addresses: k.sabri@ju.edu.jo

13. Other instructors:

N/A

14. Course Description:

This course explains Security protocols, authentication protocols, data integrity, digital signatures, intrusion detection, key management and distribution, viruses and other malicious codes, information flow, mobile code and agent security. Cryptographic algorithms: Secret Key Encryption (DES), Public Key Encryption (RSA), Message Digest Algorithm (MD5); Attacks and countermeasures: Packet sniffing, Spoofing and denial of service; Application layer security: HTTPS, secure email; Transport layer security: TLS, SSL; Network layer security: IP security (IPSec), AH protocol, ESP protocol; access control and Firewalls: Filter-based firewalls, Proxy-based firewalls; wireless networks security, security in IEEE 802.11, WEP protocol, EAP protocol

15. Course aims and outcomes:

Aims:

Enable students to understand the computer methods of security and cryptography. Students learn introduction to computer security, aspects of security, threats and method of data protections, encryption and decryption methods, authentication systems, data integrity and digital signature.

B- Intended Learning Outcomes (ILOs): Upon successful completion of this course students will be able to ...

A- Knowledge and Understanding: Students should ...

A1) Learn the basic concepts involved with computer security.

A2) Understand the features of cryptographic systems.

A3) Understand number theory concepts related to Security

A4) Understand the importance of having a secure network.

A5) Identify the security protocols applied in different network layers.

A6) Understand blockchain concepts and its implication on organizations and individual.

B- Intellectual skills: with the ability to ...

B1) Encrypt and decrypt messages using classical encryption techniques

B2) Encrypt messages using modern encryption techniques

B3) Analyze and compare the advantages/disadvantages of different security mechanisms and identify the set of security services they can provide.

B4) Classify different types of security attacks

B5) Design a new simple security protocol.

B6) Analyze existing security protocols applied in different network layers.

B7) Security analysis of blockchain

C- Subject specific skills – with ability to ...

C1) Design security protocols that satisfy predefined requirements.

C2) Apply techniques and design principles underlying security solutions, including aspects of cryptography and security protocols;

D- Transferable skills – with ability to

D1) Discuss and work in a group in order to design and write the specification of a new security protocol.

D2) Implement and present security programs.

D3) Use security tools

16. Topic Outline and Schedule:

Topic	Week	ABET outcome	ILO	Teaching methods and evaluation
Computer and Network Security Concepts	1	1, 4	A1, A4	T: Lecture L: Reading CH 1, Handout A: Midterm, Assignment, Final
Classical Encryption Techniques	2	1	A2, B1, B3, B4	T: Lecture and discussion L: Reading CH03 A: Midterm, Assignment, Final
Block Ciphers and the Data Encryption Standard	3	1, 2	A2, A3, B2, B3, B4	T: Lecture and discussion L: Reading CH04 A: Midterm, Assignment, Final
Advanced Encryption Standard	4	1, 2	A2, A3, B2, B3	T: Lecture and discussion L: Reading CH06 A: Midterm, Assignment, Final
Block Cipher Operation Random Bit Generation and Stream Ciphers	5	1	A2, A3, B2, B3	T: Lectures and discussion L: Reading Sections from CH07 and CH08 A: Midterm, Assignment, Final
Public-Key Cryptography and RSA	6	1, 2	A2, A3, B2, B3	T: Lecture and discussion L: Reading CH09 A: Midterm, Assignment, Final
Other Public-Key Cryptosystems	7	1	A2, A3, B2, B3	T: Lectures and discussion L: Reading Section from CH10 A: Midterm, Assignment, Final
Secret Sharing, Message Authentication (Hash Function, MAC, Digital Signature)	8	1, 2	A2, A3	T: Lecture and discussion L: Reading Sections from Chapters 11,12,13 A: Midterm, Assignment, Final
Key Management and Distribution	9	1, 2, 3, 6	A5, C1	T: Lecture and discussion L: Reading CH14 A: Project, Final
User Authentication	10	1, 2, 6	A1, B3, B4, C2	T: Lecture and discussion L: Reading CH15 A: Final
Transport-Level Security	11	1, 2, 6	A5, B5, B6, C1	T: Lecture, and discussion L: Reading CH17 A: Final
IP Security	12	1, 2, 6	A5, B5, B6, C1	T: Lecture and discussion L: Reading Sections 9.1, 9.3, 9.4, 9.5 A: Final Short test in Sections: 2.3, 2.4, 2.6, 4.1, 4.3, 5.1
Firewalls	13	1, 2	A1, B3, B4, C2	T: Lecture and discussion L: Reading Sections 10.1, 10.2, 10.3, 10.4

				A: Final
Blockchain	14	1, 2	A6, B3, B4, B7, C2	T: Lecture and discussion L: Reading L: Handout and blockchain book A: Final
Revision	15			
Final	16			

17. Evaluation Methods and Course Requirements (Optional):

Opportunities to demonstrate achievement of the ILOs are provided through the following assessment methods and requirements:

There will be several assessment methods of evaluation the performance of the students such as attending and class participation, grading the quizzes; assignments; conducting the midterm, short test and the final exam.

18. Course Policies:

A- Attendance policies:

Deliberate abstention from attending 1901101 classes and any other similar acts will lead to student deprivation from the course according to the UJ regulations

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

If you miss the midterm or the short test, then a makeup exam will not be provided unless you submit a valid absence excuse, within three days from the midterm, to your lecturer. This excuse must be signed and stamped from the UJ hospital in order to be valid. If your lecturer accepts the excuse then you will be able to take the makeup. You need to follow up the departmental announcements regarding the makeup date and time. Please note that the lecturer may either accept or reject your excuse based on UJ regulations

C- Health and safety procedures:

N/A

D- Honesty policy regarding cheating, plagiarism, misbehavior:

All students in this course must read the University policies on plagiarism and academic honesty
http://registration.ju.edu.jo/RegRegulations/Forms/All_Regulations.aspx

E- Grading policy:

- Midterm Exam: 30%
- Quizzes, assignments and/or class participants 10%
- Presentation 10%
- Final Exam: 50%

F- Available university services that support achievement in the course:

N/A

G- Statement on Students with disabilities

Students with Disabilities: Students with disabilities who need special accommodations for this class are encouraged to meet with the instructor and/or their academic advisor as soon as possible. In order to receive accommodations for academic work in this course, students must inform the course instructor and/or their academic advisor, preferably in a written format, about their needs no later than the 4th week of classes.

19. Required equipment:

Class rooms with data shows

20. References:

A- Required book (s), assigned reading and audio-visuals:

- *Cryptography and Network Security Principles and Practices, William Stallings, Pearson: Prentice Hall, 7th Edition, 2016*

B- Recommended books, materials, and media:

- *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World. Don Tapscott and Alex Tapscott, 2018.*
- *Information Security: Principles and Practice, Mark Stamp, Wiley, 2th edition, 2011.*
- *Network Security Essentials Applications and Standards, William Stallings, Pearson: Prentice Hall, Fourth Edition, 2010.*
- *Cryptography and Network Security, Behrouz A Forouzan, McGraw-Hill Science, First Edition, 2007.*
- *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Bruce Schneier, Second Edition 1996.*
- *Practical Cryptography, Niels Ferguson and Bruce Schneier, Wiley, 2003.*
- *IEEE Security and Privacy magazine.*
- *ITU-T Recommendations X.800, X.805 and X.509.*

21. Additional information:

Course website:
elearning.ju.edu.jo

Date: -----

Name of Course Coordinator: -----Signature: -----

Head of curriculum committee/Department: ----- Signature: -----

Head of Department: ----- Signature: -----

Head of curriculum committee/Faculty: ----- Signature: -----

Dean: ----- -Signature: -----

Copy to:

Head of Department

Assistant Dean for Quality Assurance

Course File