Al-Al Bayt University
Prince Hussein bin Abdullah Faculty of Information Technology
Computer Science

Course Syllabus

Course Title	**Data Security & Authentication**	**Course Code**	**901480**
Coordinator	Rabah Alshboul	**Prerequisite(s)**	**901325 or 904460**
E-mail	Rabahshboul@aabu.edu.jo	**Credit Hours**	3
Course Is	**√ Required**		

Course Description:

Introduction to encryption techniques used in computer security. Encryption (using single and publick key), Steganography and watermark, digital signature, reliability, e-commerce (Monetary unknown, trace amounts of payment), key management, security protocols, and safe operating systems, firewall, Malicious software.

Course Learning Outcomes (CLO):

1. It is expected from the students to understand the principles and practice of cryptography and network security.
2. understanding different types of security mechanisms to protect management information systems
3. The objective is to provide an up-to-date survey of developments in computer security. Central problems that confront security designers and security administrators include defining the threats to computer and network systems, evaluating the relative risks of these threats, and developing cost-effective and user-friendly countermeasures.

Tentative Topics Covered

Week No	Topic
1	Computer Security Concepts, The OSI Security Architecture, Security Attacks,
2	Security Services, Security Mechanisms , A Model for Network Security

3	Classical Encryption Techniques, Symmetric Cipher Model,
4	Substitution Techniques
5	Substitution Techniques
6	Transposition Techniques
7	Rotor Machines, Steganography
8	Cryptographic Tools, Confidentiality with Symmetric Encryption
9	Message Authentication and Hash Functions, Public-Key Encryption, Digital Signatures and Key Management, Random and Pseudorandom Numbers, Practical Application: Encryption of Stored Data
10	User Authentication, Means of Authentication, Password-Based Authentication,
11	Token-Based Authentication, Biometric Authentication, Remote User Authentication, Security Issues for User Authentication
12	Malicious Software, Types of Malicious Software (Malware), Propagation—Infected Content—Viruses
13	Propagation—Vulnerability Exploit—Worms, Propagation—Social Engineering—SPAM E-mail, Trojans, Payload—System Corruption, Payload—Attack Agent—Zombie, Bots, Payload—Information Theft—Key loggers, Phishing, Spyware, Payload—Stealthing—Backdoors, Rootkits, Countermeasures
14	Firewalls and Intrusion Prevention Systems, the Need for Firewalls, Firewall Characteristic
15	Types of Firewalls, Firewall Basing, Firewall Location and Configurations, Intrusion Prevention Systems
16	Final exam

Textbook(s)

Title	Cryptography and Network Security*: Principles and Practice*		
Author(s)	**William Stallings**	**Publisher**	**Prentice-Hall**
Edition	6th	**Year**	2011

References

Book Titles (Author(s), Title, Edition, Publisher, Year)	Website URL (if available)
1. Computer security principles and practice, William Stallings, Lawrie Brown, third edition, Prentice-Hall, 2011 **2. Lecturers Notes and Handouts**	WilliamStallings.com/Crypto/Crypto5e.html.

Evaluation

Assessment Tool	Marks

- First Exam	20
- Second Exam	20
- Assignments (Reports, Quiz, Seminar, Tutorial, etc.) **- Discipline, presence and participation**	10
- Lab	-
- Final Examination	50