|  |  |  |
| --- | --- | --- |
| **1** | Course title | Information Security and Privacy |
| **2** | Course number | 5401322 |
| **3** | Credit hours (theory, practical) | 3 |
| Contact hours (theory, practical) | 48 (theory 30, practical 15, exams, 3) |
| **4** | Prerequisites/corequisites | Theory of Algorithms (5401341) |
| **5** | Program title | Computer Information Systems (CIS) |
| **6** | Program code | 01 |
| **7** | Awarding institution | The University of Jordan |
| **8** | Faculty | Systems and Information Technology |
| **9** | Department | Computer Information Systems |
| **10** | Level of course | Senior |
| **11** | Year of study and semester (s) | Third year-second semester, Furth year- first semester |
| **12** | Final Qualification | Bachelor (BS.c.) |
| **13** | Other department (s) involved in teaching the course | Business Information Technology (BIT) |
| **14** | Language of Instruction | English |
| **15** | Date of production/revision | 04/02/2020 |

16. Course Coordinator:

|  |
| --- |
| Dr. Ismail AL-Taharwa  Rank: Assistant professor  Office No.:322  Office hours: Sun, Tue, Thr: 10:00 – 11:00, Mon: 9:30-10:30,  Phone numbers :35118  Email addresses: i\_taharwa@ju.edu.jo |

17. Other instructors:

|  |
| --- |
|  |

**18. Course Description:**

|  |
| --- |
| This is an introductory course to information security that gives an overview of information security principles and practices. Course emphasizes on the basic security services, Confidentiality, Authentication, and Integrity. Underlying theoretic and practical are investigated too. Key topics covered includes, but not limited to: classical encryption and block ciphers,  modern symmetric ciphers (DES, AES, Triple DES), confidentiality using symmetric ciphers, public-key cryptosystems and key management (RSA), message authentication and hash functions, digital signatures (DSS), IP and Web security, firewalls and trusted systems, and security threats (Viruses, Worms, ...). |

1. 19. Course aims and outcomes:

|  |
| --- |
| A- Aims: |
| **B- Intended Learning Outcomes (ILOs):** Upon successful completion of this course students will be able to … |
| **B.1. Knowledge and Understanding (students should):** |
| B.1.1 Understand the meaning of information security. |
| B.1.2 Understand security threats, Security models, and building security functions. |
| B.1.3 Understand the Public key cryptography schema. |
| B.1.4 Understand the private key cryptography schema. |
| B.1.5 Understand the cryptographic hash functions. |
| B.1.6 Understand the steganography, watermarking and information hiding. |
| B.1.7 Understand database security. |
| **B.2. Intellectual ILOs:** |
| B.2.1 Distinguish between different security models. |
| B.2.2 Distinguish between public key and private key cryptography |
| B.2.3 Explain some classical encryption methods. |
| B.2.4 Explain the Hash functions, cryptographic hash functions with applied examples. |
| B.2.5 Distinguish between different information hiding schema. |
| **B.3 Practical skills ILOs** |
| B.3.1 Analyze simple mathematical formulae. |
| B.3.2 Analyze some computational aspects related to public cryptography schema. |
| B.3.3 Analyze some computational aspects related to Private cryptography schema. |
| **B.4 Transferable Skills with ability to** |
| B.4.1 Display an integrated approach to the deployment of communication skills. |
| B.4.2 Work effectively with dataset owners and for dataset users. |
| B.4.3 Strike the balance between self-reliance and seeking help when necessary. |
| B.4.4 Show personal responsibility by working to multiple deadlines with respect to the course requirements. |
|  |

20. Topic Outline and Schedule:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Topic** | **Week** | **Instructor** | **Achieved ILOs** | **Evaluation Methods** | **Reference** | | **Overview**  Introduction to data security, attacks, services, Security models, Cryptology, and digital signature | 1,2 | Ismail AL-Taharwa | B.1.1, B.1.2, B.2.1 , B.2.2 | **Homework** | Text: chapter 1 | | **SymmetricCiphers**  Symmetric cipher model, Caesar cipher, Monoalphabatic cipher, Polyalphabatic cipher,  Playfair cipher, Hill cipher, Vigenere Cipher, Transposition Cipher and ROTOR Machines | 3, 4 | Ismail AL-Taharwa | B.2.3, B.3.1 | Quiz + Homework | Text: Chapter 3 | | **Block ciphering andData Encryption Standard (DES)**  Ideal Block cipher,  Feistel network  DES encryption and decryption  Avalanche effect | 5,6 | Ismail AL-Taharwa | B.1.2, B.1.3, B.2.3, B.3.2 | Exam | Text: Chapter 4 | | **Finite Fields**  Group, Ring and field  Finite fields and GF(2n) | 7 | Ismail AL-Taharwa | B.3.1, | Homework | Text: Chapter 5 | | **Midterm exam** |  | Ismail AL-Taharwa |  |  |  | | **Advanced Encryption Standard**  Key creation, Encryption, Decryption | 8, 9 | Ismail AL-Taharwa | B.3.1, B.2.3, B.3.2 | Exam + HW | Text: Chapter 6 | | **Public key encryption**  Public key ciphering requirements  RSA cipher:  Key generation  Encryption/decryption  Fast exponent algorithm,  Cryptanalysis  quiz | 10, 11, 12 | Ismail AL-Taharwa | B.1.3, B.1.4, B.2.2, B.3.1, B.3.3 | Quiz + exam | Text: Chapter 9 | | **Public key Cryptosystem**  Diffie-Hellman key exchange | 13 | Ismail AL-Taharwa | B.1.4, B.2.2, B.3.3 | Exam | Text: Chapter 10 | | **Hashing**  Hash function, One-way functions,SHA1, MDs and Digital Signature | 14, 15 | Ismail AL-Taharwa | B.1.5, B.2.4, | Exam+ HW + quiz | Text: Chapter 11 | | **Security threats**  Malware  Viruses  Warms  Heap spraying  SQL-injection  ... |  | Self read | B.1.7, B.4.1, B.4.2, B.4.3, B.4.4 | Presentation | Suggested paper reading | | **Final Exam** | 16 | Ismail AlTaharwa |  |  |  | |

21. Teaching Methods and Assignments:

|  |
| --- |
| Development of ILOs is promoted through the following teaching and learning methods:   * Presentation and discussion in class * Practical classes * Reading materials * Handouts * External material * Online resources (encryption/decryption simulators) |

22. Evaluation Methods and Course Requirements:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Opportunities to demonstrate achievement of the ILOs are provided through the following assessment methods and requirements:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Method | Lecture | Demo | Laboratory | Paper reading | | Intended Learning Outcomes (ILO) | B.1.1, B.1.2, B.1.3, B.1.4, B.1.6, B.2.2, B.2.4 | B.1.4, B.2.4, B.1.6 | B.1.2, B.1.3, B.1.4, B.2.3, B.3.1, B.3.2, | B.1.6, B.1.6, B.2.5, B.4.1, B.4.2, B.4.3, B.4.4 | | Assessment | Exams + Assignments | Quiz + Homework | Exams + Assignments | Presentation and discussion | |

23. Course Policies:

|  |
| --- |
| **Discipline and Active Participation Policy (If applicable as bonus, could be banned if it is insufficient):**  All together discipline and active participation will be rewarded. Attending the class by itself without any active participation doesn’t permit having the participation mark. **Refer to the JU’s regulations and legalizations regarding attendance.**   * + Participation frequency and relative grading percentage:   + participation is subject to 5% (good questions, valuable observations and effective answers )   + Semi-effective participation is subject to 3% (ineffective questions, observations and answers)   + Infrequent participation is subject to 2% (ineffective and show low level of preparation)   + Rare participation is subject to 1%   + Displaying no sign of life or long periods of absence is subject to 0%   Late presence to class (less than 10 minutes) will be recorded. If such behavior happens to be repeated, it will be accounted as absence. More than 10 minutes late presence are not allowed to attend the class.    A- Attendance policies:  Students are allowed up to 5 absences with excuses. If you exceed this number, you will fail the class.  B- Absences from exams and handing in assignments on time:  All projects and assignments are to be uploaded to the course website.   * Upload assignments to elearning.ju.edu.jo (Moodle) by 11:55 PM on its due date. * Everyone should check their e-mail and Moodle regularly. Students are responsible for information posted there. If critical information is posted in Moodle that you must read today, an announcement to check e-learning will be sent to the mailing list   C- Health and safety procedures:  D- Honesty policy regarding cheating, plagiarism, misbehavior:  Discussion of the concepts and principles between students is fine and very welcomed. Also, students are allowed to debug each other’s code. However, Student cooperation should not result in identical or near identical answers/code/documentation. **ALL THE MATERIAL SUBMITTED FOR GRADING MUST BE YOUR OWN EFFORT.** If this policy is violated then the following steps may be taken: (1) reduction of points by dividing by the number of students involved in an incident, (2) assignment of a grade of ZERO for all students involved in an incident.  E- Grading policy:  Midterm Exam 30% Quizzes and assignments 20% Final Exam 50%  **Evaluation Scale:**  Mark *≤* 34 *≤* 49 *≤* 54 *≤* 59 *≤* 64 *≤* 69 *≤* 74 *≤* 79 *≤* 84 *≤* 89 *≤* 94 *≤* 100  Scale F -D D +D -C C +C -B B +B -A A  F- Available university services that support achievement in the course:  **VERY IMPORTANT RULES AND REGULATIONS:**   * Attendance and participation are mandatory, absence may result in receiving an **ABSENT FAIL** grade or an equivalent fail grade * It preferable to have structured participation and **avoid random additions or interruptions** * When advised stick to the provided template for the deliverables, it would give more value to your piece of work * Any out of order behavior, as side talks or sleeping, during the lecture time will be reported and may result in an expel of the class room. * Disrespect toward colleagues while talking or discussing an issue is prohibited and **will result in an expel and a penalty**. * Late homework and assignments delivery may result in having ZERO grade for that particular deliverable * Cheating has no excuse at all, with no exceptions, it will result in **having a penalty**. **Refer to the JU’s regulations and legalizations regarding tests and exams.** * Disturbing the running of the exam for any reason (e.g., technical) by any behavior **is prohibited**, it will result in having **penalty. Refer to the JU’s regulations and legalizations regarding tests and exams.** In case the Instructor, lab supervisor or exam supervisor requested you to look in your monitor, to show your ID, or any other command**. Response to his order clammily and immediately. Definitely, it is your right to discuss such case after the exam.** * **Plagiarism** is **unethical** activity that may result in having a **penalty**, refer to [*www.plagiarism.org*](www.plagiarism.org) * Any feedback is welcomed while presented in a reasonable manner. However, **Disturbing the running of the class by making arguments** with classmates, lab supervisor, or instructor, or by any other behavior is **prohibited and will result in an expel and a penalty**. Nevertheless, any kind of **polite discussion and negotiation** regarding any issues related to the progress of the course is **welcomed at the instructor office**.   Carefully read the most recent copy of the **regulations statement** provided by the University of Jordan, as it applies to this course. |

24. Required equipment:

|  |
| --- |
| Personal Computer, Non-programmable calculator |

**25. References:**

|  |
| --- |
| Required book (s), assigned reading and audio-visuals:  TextBook:   1. Cryptography and network security, principles and practice, **7th** edition, **2017**, William Stallings.   Reference:   1. Computer security Basics, Deborah Russell and G.T.Gangemi.   Recommended books, materials, and media:  The following books are recommended for the student who wants more material in algebra and number theory:  1. Wenbo Mao, Modern Cryptography: Theory and Practice. Prentice Hall 2004.  2. Alfred Menezes, Paul van Oorschot and Scott Vanstone, Handbook of Applied Cryptography, CRC  Press, 2001. ISBN: 0-8493-8523-7. Published online free for personal usage as per the copyright notice. Available online at http://www.cacr.math.uwaterloo.ca/hac/  3. V. Shoup. A Computational Introduction to Number Theory and Algebra. An excellent source, written with  Cryptographic applications in mind. Available online: http://www.shoup.net/ntb/ntb-v1.pdf  4. D. Anglian: Lecture Notes on the Complexity of Some Problems in Number Theory. L.N. Childs: A Concrete  Introduction to Higher Algebra.  5. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Digital watermarking, Morgan Kaufmann, 2002  6. Behrouz A. Forouzan, Cryptography & Network Security, 1st ed., McGraw-Hill, 2008 |

26. Additional information:

|  |
| --- |
| None |

Name of Course Coordinator: --Dr. Ismail AL-taharwa---Signature: ------------------- Date: 04/02/2020

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