MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

| **Module Information**  **معلومات المادة الدراسية** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Module Title** | Information security | | | | **Module Delivery** | | |
| **Module Type** | Core | | | | * **☒Theory** * **☐ Lecture** * **☒ Lab** * **☐ Tutorial** * **☐ Practical** * **☐ Seminar** | | |
| **Module Code** | BMI422 | | | |
| **ECTS Credits** | 5 | | | |
| **SWL (hr/sem)** | 125 | | | |
| **Module Level** | | 4 | **Semester of Delivery** | | | | 8 |
| **Administering Department** | | Bioinformatics | **College** | BMIC | | | |
| **Module Leader** | Sanaa Ahmed Kadhim | | **e-mail** | Dr.sanaa.ahmed@uoitc.edu.iq | | | |
| **Module Leader’s Acad. Title** | | Ass. Professor | **Module Leader’s Qualification** | | | | Ph.D. |
| **Module Tutor** | Sanaa Ahmed Kadhim | | **e-mail** | Dr.sanaa.ahmed@uoitc.edu.iq | | | |
| **Peer Reviewer Name** | | Omar. A Abdulmajeed | **e-mail** | omara.m@uoitc.edu.iq | | | |
| **Scientific Committee Approval Date** | | 08/06/2023 | **Version Number** | | | 1.0 | |

| **Relation with other Modules**  **العلاقة مع المواد الدراسية الأخرى** | | | |
| --- | --- | --- | --- |
| **Prerequisite module** | Mathematics II, BID121 | **Semester** | 2 |
| **Co-requisites module** | None | **Semester** |  |

| **Module Aims, Learning Outcomes and Indicative Contents**  **أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية** | |
| --- | --- |
| **Module Objectives**  **أهداف المادة الدراسية** | 1. To develop problem solving skills and understanding of Security issues through the application of security techniques. 2. To understand the concept of cyber and cyber security. 3. To understand Encryption, Decryption and Key. 4. This course deals with the basic concept of secrecy methods. 5. To understand Authentication, Verification, and Confidentiality. 6. To understand type of cyber \_attacks and threats. 7. To perform different traditional cryptosystems to secure cyber data transfer. 8. This is the basic subject for all cyber and network transmission. |
| **Module Learning Outcomes**  **مخرجات التعلم للمادة الدراسية** | 1. Recognize the basic idea of security. 2. Understand the concepts of cyber security. 3. Learning the concept of attack and threats. 4. List the various types of traditional cryptosystems to secure data transmission. 5. Learn some basic methods of Monophonic encryption that using one element key. 6. Learn some basic methods of encryption that using more than one key. 7. Learn some basic methods of Homophonic encryption. 8. Learn the pros and cons of using one time pad key OTP. 9. Define Feistel method and DES method. 10. Identify the basic tables and key generation of DES. 11. Define DEA method and compared with DES method. 12. Discuss the concept of cryptanalyst, cyberattack and defense. 13. Explain the basic steps of cryptanalysis. The difference between attacker and cryptanalyst. |
| **Indicative Contents**  **المحتويات الإرشادية** | Indicative content includes the following.  Part A – Main concepts  The main concepts of security: encryption, decryption, keys and key generation and choosing, authentication, verification, confidentiality.  The main concepts of cyberattacks: cyber security, cyber threats, and different types of data to be transmitted in cyber world.  Part B - Cryptosystems  Fundamentals of cryptosystems: types of cryptosystems, symmetric and asymmetric cryptosystem, block and stream cipher, some traditional cryptosystems.  Fundamentals of cryptosystems: types of transferred data through net, types of alterations of data, types of cyber war.  Part C – Concepts of security system parts  Fundamentals of security parts: Steganography, watermarking, cryptography, data hiding for verification and ownership rights.  Part C – Stream cipher  Fundamentals of stream cipher: private key, monophonic and homophonic method.  Part D – Block cipher  Fundamentals of block cipher: Feistel method, DES, triple DES, DEA.  Part E - Cryptanalysis  Fundamentals of cryptanalysis, types and steps of encrypted code breaking, statistical analysis of cipher texts, cryptanalyst and attackers. |

| **Learning and Teaching Strategies**  **استراتيجيات التعلم والتعليم** | |
| --- | --- |
| **Strategies** | The main strategy that will be adopted in delivering this module is to encourage students’ participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering types of simple experiments involving some sampling activities that are interesting to the students. |

| **Student Workload (SWL)**  **الحمل الدراسي للطالب محسوب لـ ١٥ اسبوعا** | | | |
| --- | --- | --- | --- |
| **Structured SWL (h/sem)**  **الحمل الدراسي المنتظم للطالب خلال الفصل** | 64 | **Structured SWL (h/w)**  **الحمل الدراسي المنتظم للطالب أسبوعيا** | 4 |
| **Unstructured SWL (h/sem)**  **الحمل الدراسي غير المنتظم للطالب خلال الفصل** | 61 | **Unstructured SWL (h/w)**  **الحمل الدراسي غير المنتظم للطالب أسبوعيا** | 4 |
| **Total SWL (h/sem)**  **الحمل الدراسي الكلي للطالب خلال الفصل** | **125** | | |

| **Module Evaluation**  **تقييم المادة الدراسية** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **As** | | **Time/Number** | **Weight (Marks)** | **Week Due** | **Relevant Learning Outcome** |
| **Formative assessment** | **Quizzes** | 4 | 10% (10) | 3,7,11 and 13 | LO #1, #2; #3-#6, #7-#10, #11-#13 |
| **Assignments** | 6 | 10% (10) | Continuous | LO #2- #13 |
| **Lab** | 6 | 10% (10) | Continuous | All |
| **Report** | 1 | 10% (10) | 13 | All |
| **Summative assessment** | **Midterm Exam** | 2hr | 10% (10) | 7 | LO #1 - #7 |
| **Final Exam** | 3hr | 50% (50) | 16 | All |
| **Total assessment** | | | 100% (100 Marks) |  |  |

| **Delivery Plan (Weekly Syllabus)**  **المنهاج الاسبوعي النظري** | |
| --- | --- |
| **Week** | **Material Covered** |
| **Week 1** | Introduction to data security and cyber security (what is the difference..) |
| **Week 2** | Basics of data transmission, what are the threats, Kinds of breaches and attacks. |
| **Week 3** | Steganography, watermarking, and cryptography. |
| **Week 4** | Review of the various types of traditional cryptosystems and stream cipher. |
| **Week 5** | Learn some Monophonic encryption methods that use one key. |
| **Week 6** | Learn some methods of encryption that using more than one key. |
| **Week 7** | **Mid-term Exam** |
| **Week 8** | Learn some Homophonic encryption methods. |
| **Week 9** | Learn the pros and cons of using one time pad key OTP. |
| **Week 10** | Define block cipher: Feistel method and DES method. |
| **Week 11** | Identify the basic tables and key generation of DES. |
| **Week 12** | Define DEA method and compared with DES method. |
| **Week 13** | Multimedia secure transmission through cyber world. |
| **Week 14** | Discuss the concept of cryptanalyst steps of cryptanalysis. |
| **Week 15** | Explain the difference between attacker and cryptanalyst. |
| **Week 16** | **Preparatory week before the final Exam** |

| **Delivery Plan (Weekly Lab. Syllabus)**  **المنهاج الاسبوعي للمختبر** | |
| --- | --- |
| **Week** | **Material Covered** |
| **Week 1** | Lab 1: Introduction to encryption |
| **Week 2** | Lab 2: encrypt and decrypt small part of text file |
| **Week 3** | Lab 3: apply the methods of ceaser, multiplication and additive cipher |
| **Week 4** | Lab 4: apply the methods of columnar, keyword and keymixed cipher |
| **Week 5** | Lab 5: apply the methods of Vegener, Beafut cipher |
| **Week 6** | Lab 6: apply the methods of Hill cipher, play fair cipher |
| **Week 7** | Lab 7: apply the methods of OTP cipher |
| **Week 8** | Lab 8: design a model of black chamber table and encryption |
| **Week 9** | Lab 9: apply the methods of finding the modulation inverse |
| **Week 10** | Lab 10: apply initial key generation of one round of DES |
| **Week 11** | Lab 11: apply the methods of S-boxes generation |
| **Week 12** | Lab 12: apply the creation of IP and IP-1 |
| **Week 13** | Lab 13: finding the statistical information for cryptanalysis |
| **Week 14** | Lab 14: Continuation of the statistical information for cryptanalysis |
| **Week 15** | Lab 15: Discussion and Review |

| **Learning and Teaching Resources**  **مصادر التعلم والتدريس** | | |
| --- | --- | --- |
|  | **Text** | **Available in the Library?** |
| **Required Texts** | 1. [Cryptography and Network Security: Principles and Practice](https://www.amazon.com/Cryptography-Network-Security-Principles-Practice/dp/0136097049/ref=monarch_sidesheet), William Stallings, Publisher: Pearson , Edition 5, 2010. 2. [Cybersecurity Essentials](https://www.amazon.com/Cybersecurity-Essentials-Charles-J-Brooks/dp/1119362393/ref=sr_1_13?keywords=cyber+security&qid=1685775340&s=books&sr=1-13), [Charles J. Brooks](https://www.amazon.com/Charles-J-Brooks/e/B000APBBTY/ref=dp_byline_cont_book_1), [Christopher Grow](https://www.amazon.com/s/ref=dp_byline_sr_book_2?ie=UTF8&field-author=Christopher+Grow&text=Christopher+Grow&sort=relevancerank&search-alias=books) , [Philip A. Craig Jr.](https://www.amazon.com/s/ref=dp_byline_sr_book_3?ie=UTF8&field-author=Philip+A.+Craig+Jr.&text=Philip+A.+Craig+Jr.&sort=relevancerank&search-alias=books) , [Donald Short](https://www.amazon.com/s/ref=dp_byline_sr_book_4?ie=UTF8&field-author=Donald+Short&text=Donald+Short&sort=relevancerank&search-alias=books), publisher: Sybex, Edition 1, 2017 | Yes  No |
| **Recommended Texts** | Cryptography & Network Security, 1st Edition,by [Behrouz A. Forouzan](https://www.amazon.com/Behrouz-A-Forouzan/e/B001IOBDOE/ref=dp_byline_cont_book_1), Publisher: McGraw-Hill Education, 2007. | Yes |
| **Websites** | Recommended :   1. <https://insider.ssi-net.com/insights/what-is-the-difference-between-data-security-and-cyber-security>. 2. <https://www.secureworld.io/industry-news/cybersecurity-vs-data-security-definition> 3. <https://www.777networks.co.uk/data-security-vs-cyber-security-whats-the-difference/> | |

| **Grading Scheme**  **مخطط الدرجات** | | | | |
| --- | --- | --- | --- | --- |
| **Group** | **Grade** | **التقدير** | **Marks %** | **Definition** |
| **Success Group**  **(50 - 100)** | **A -** Excellent | **امتياز** | 90 - 100 | Outstanding Performance |
| **B -** Very Good | **جيد جدا** | 80 - 89 | Above average with some errors |
| **C -** Good | **جيد** | 70 - 79 | Sound work with notable errors |
| **D -** Satisfactory | **متوسط** | 60 - 69 | Fair but with major shortcomings |
| **E -** Sufficient | **مقبول** | 50 - 59 | Work meets minimum criteria |
| **Fail Group**  **(0 – 49)** | **FX –** Fail | **راسب (قيد المعالجة)** | (45-49) | More work required but credit awarded |
| **F –** Fail | **راسب** | (0-44) | Considerable amount of work required |
|  |  |  |  |  |
| **Note:** Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above. | | | | |