	Ministry of Higher Education and Scientific Research - Iraq University of Technology Department of Computer Sciences Information System Branch	

MODULE DESCRIPTOR FORM

نموذج وصف المادة الدراسية

Module Information

معلومات المادة الدراسية

Module Title	**Stream Cipher**	**Module Delivery**
Module Type	CORE	**-Theory Lecture** **-Lab** **-PracticalSeminar**
Module Code	STCI214	
ECTS Credits	6	
SWL (hr/sem)	150	

Module Level		**Semester of Delivery**	1
Administering Department		**College**	
Module Leader	Alaa Kadhim Farhan	**e-mail**	Alaa.k.farhan@uotechnology.edu.iq
Module Leader's Acad. Title	Professor Dr.	**Module Leader's Qualification**	PhD
Module Tutor	None	**e-mail**	None
Peer Reviewer Name		**e-mail**	
Review Committee Approval		**Version Number**	

Relation With Other Modules

العلاقة مع المواد الدراسية الأخرى

Prerequisite module	NUTH125	**Semester**	
Co-requisites module	BLCI224	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents
أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية

Module Aims أهداف المادة الدراسية	1. The aim of this subject is to teach the students how to program the algorithm of stream cipher 2. The basic principle to encryption the cipher text.
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	1. Understanding Cryptographic Fundamentals: . Explain the basic principles of cryptography, including the purpose and function of encryption and decryption. . Differentiate between symmetric and asymmetric encryption and identify where stream ciphers fit in this classification. 2. Stream Cipher Concepts: . Describe the key components and operation of stream ciphers, including keystream generation and XOR operation. . Explain the difference between synchronous and self-synchronizing stream ciphers. 3. Security Analysis: . Analyze the security properties of stream ciphers, including common vulnerabilities and attacks (e.g., keystream reuse, known-plaintext attacks). . Evaluate the robustness of different stream ciphers against various types of cryptographic attacks. 4. Implementation Skills: . Implement basic stream cipher algorithms in a programming language of choice (e.g., Python, C++). . Utilize cryptographic libraries to encrypt and decrypt data using stream ciphers. 5. Application and Use Cases: . Identify appropriate use cases for stream ciphers in real-world applications, such as securing data in transit or encrypting data streams. . Compare stream ciphers with block ciphers and determine the suitable use case for each type. 6. Performance Considerations: . Assess the performance characteristics of stream ciphers, including speed and resource consumption. . Optimize stream cipher implementations for efficiency in various environments, such as embedded systems or high-performance computing contexts. 7. Ethical and Legal Aspects: . Discuss ethical considerations in the use of cryptographic techniques, particularly in privacy and data protection.
Indicative Contents المحتويات الإرشادية	1. Introduction 2. Fundamental Concepts 3. Key Components 4. Classical Stream Ciphers

	5. Modern Stream Ciphers 6. Design Principles 7. Cryptanalysis of Stream Ciphers 8. Implementation 9. Applications 10. Case Studies 11. Future Trends and Research Directions

Learning and Teaching Strategies

استراتيجيات التعلم و التعليم

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 type of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL)

الحمل الدراسي للطالب

Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	93	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	57	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	
Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	150		

Module Evaluation

تقييم المادة الدراسية

		Time/Number	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	1	10% (10)	5	LO # 1 and 3
	Practical Seminar(Lab).	2	15% (15)	Continuous	LO # 2 , 4 and 5
Summative assessment	**Midterm Exam**	1 hr	15% (15)	14	LO # 1 to 5
	Final Exam	3hr	60% (60)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus) المنهاج الاسبوعي النظري	
	Material Covered
Week 1	Introduction Stream Cipher Structure
Week 2	Stream Cipher history
Week 3	Important element for design a stream cipher
Week 4	Types of stream ciphers
Week 5	Polynomial Equations
Week 6	Arithmetic of Polynomial
Week 7	Shift register
Week 8	Types of shift register
Week 9	Review
Week 10	Exam
Week 11	linear Shift Register
Week 12	Nonlinear Shift Register
Week 13	Five Basic Tests
Week 14	exam
Week 15	Review and Exam
Week 16	Final course Exam

Delivery Plan (Weekly Lab. Syllabus) المنهاج الاسبوعي للمختبر	
	Material Covered
Week 1	Program language V.B net
Week 2	Program language V.B net
Week 3	Program language V.B net
Week 4	Program to stream cipher
Week 5	Program to Polynomial
Week 6	Program to Arithmetic of Polynomial
Week 7	Program to Shift register
Week 8	Counties program to SR
Week 9	review
Week 10	linear Shift Register program

Week 11	**Nonlinear Shift Register program**
Week 12	**Five Basic Tests program**
Week 13	**Counties**

Learning and Teaching Resources
مصادر التعلم والتدريس

	Text	**Available in the Library?**
Required Texts	H. Boker & F. Piper, "Cipher System, The Protection of Communications ", Northwood Books, Landon, 1982.	Yes
Recommended Texts	B. Schneier, "**Applied Cryptography**", 2nd ed., John Wiley & Sons, Inc., 1996. ANSI X9.44, "**Public key cryptography using reversible algorithms for the financial services industry: Transport of symmetric algorithm keys using** RSA", 1994. Diffie: Whitfield Diffie and Martin Hellman, "New Directions in Cryptography'', IEEE Transactions on Information Theory, Nov 1976. William, S.," ***Cryptography and Network Security: Principles and Practice.", Three*** Edition. Prentice Hall, 2002.	No
Websites		

APPENDIX:

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	مقبول بقرار	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required
Note:				

NB 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.