	Ministry of Higher Education and Scientific Research - Iraq University of Technology Department of Computer Science Computer and Cyber security Branch	

MODULE DESCRIPTOR FORM
نموذج وصف المادة الدراسية

Module Information
معلومات المادة الدراسية

Module Title	BLOCK CIPHER	**Module Delivery**	
Module Type	Core	-Theory Lecture -Lab -Practical Seminar	
Module Code	BLCI224		
ECTS Credits	5.00		
SWL (hr/sem)	78		
Module Level	4	**Semester of Delivery**	
Administering Department	computer security and cyber security branch	**College**	Computer sciences department
Module Leader	Prof.dr.Alaa Kadhim Farhan	**e-mail**	Alaa.k.Farhan@uotechnologu.edu.iq
Module Leader's Acad. Title	Prof	**Module Leader's Qualification**	
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	Stream Cipher	**Semester**	3
Co-requisites module	Public Key Cryptography	**Semester**	5
Module Aims, Learning Outcomes and Indicative Contents أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية			
Module Aims أهداف المادة الدراسية	1-Understand Block Cipher Fundamentals: Grasp the basic concepts of block ciphers, including data processing in fixed-size blocks. 2- Study Encryption and Decryption: Learn how block ciphers encrypt and decrypt data, understanding the importance of key management. 3- Explore Different Modes of Operation: Examine various modes of operation (e.g., ECB, CBC, CFB, OFB, CTR) and their implications for security and performance. 4- Analyze Security Properties: Investigate the security properties such as confusion, diffusion in S-Box and IP-permutation Boxes for contribute to cryptographic strength. 5- Learn About Key Sizes and Algorithms: Get familiar with common block cipher algorithms (e.g., AES, DES, cast,Gost,…) and their key sizes, strengths, and weaknesses. 6-Implement Block Ciphers: Gain practical experience by implementing block ciphers and evaluating their performance and security features. 7- Examine Attacks on Block Ciphers: Identify possible cryptographic attacks (like differential and linear cryptanalysis) and how they affect block cipher security.		
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	1-**Comprehension of Basic Concepts** • Understand the fundamental principles of block ciphers, including encryption and decryption processes. 2-**Knowledge of Common Algorithms** • Identify and describe various block cipher algorithms (e.g., AES, DES,		

	Cas,….t) and their operational differences. 3- **Analysis of Security Features** • Analyze the security attributes of block ciphers, such as strength against various cryptographic attacks. 4- **Implementation Skills** • Implement block cipher algorithms in a programming environment and evaluate performance metrics. 5-**Evaluation of Key Management** • Assess key management practices, including key generation, distribution, and storage in the context of block ciphers. 6-**Understanding of Cryptographic Protocols** • Explain the role of block ciphers in broader cryptographic protocols and their integration with other cryptographic components. 7-**Awareness of Contemporary Issues** • Stay informed about current trends and developments in cryptography and the implications for block cipher algorithm
Indicative Contents المحتويات الإرشادية	1. Introduction to Block Ciphers** - Definition and significance in cryptography - Overview of symmetric vs. asymmetric encryption 2. Basic Principle - Structure and function of block ciphers - Key concepts: plaintext, ciphertext, keys, and blocks 3. Common Block Cipher Algorithms - Detailed study of popular algorithms: - Data Encryption Standard (DES)

	- Triple DES (3DES) - Advanced Encryption Standard (AES) - Cast and Gost algorithm 5. Cryptographic Security and Analysis - Importance of confusion and diffusion principles 6. Key Management - Key generation techniques - Key distribution and storage strategies - Best practices for secure key lifecycle management 7. Implementation Considerations - Practical programming exercises for implementing block ciphers - Evaluation of performance and efficiency

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 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	102	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	7
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	98	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	7
Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	200		

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**	2 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	Symmetric Cipher Model.
Week 2	Confusion and Diffusion
Week 3	Feistel Mode
Week 4	DataEncryption Standard DES
Week 5	Key of DES algorithm
Week 6	Example of DES
Week 7	Type of DES
Week 8	Cast algorithm
Week 9	Gost Algorithm
Week 10	Key generation of Gost
Week 11	Example of Gost
Week 12	Feal Algorithm
Week 13	Key Generation of Feal
Week 14	RC4 Algorithm
Week 15	Serpant algorithm
Week 16	**Final Exam**

Delivery Plan (Weekly Lab. Syllabus)
المنهاج الاسبوعي للمختبر

Week	

Week 1	Designing simple vb.net program
Week 2	Designing simple vb.net program.
Week 3	S-P-Box
Week 4	f-Function in DES
Week 5	Permutation tables of DES algorithm
Week 6	DES algorithm
Week 7	Key of DES algorithm
Week 8	CAST algorithm program
Week 9	Key generator of cost program
Week 10	GOST algorithm program
Week 11	Key generator of Gost program
Week 12	Key generator of Gost
Week 13	Functions algorithm program

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*	yes
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.