



Academic Course Specification Form

استمارة توصيف المقرر الأكاديمي

القسم الخاص بالطالب Section Concerning the Student

1. Course Code:	MATHS 353	1. رمز المقرر:
2. Course Title	Introduction to Mathematical Cryptography	2. اسم المقرر:
3. College:	College of Science	3. الكلية:
4. Department:	Department of Mathematics	4. القسم:
5. Academic Program:	Bachelor of Science in Mathematics	5. البرنامج الأكاديمي:
6. Course Credits:	3-0-3	6. عدد الساعات المعتمدة:
7. Course NQF Level	7	7. مستوى المقرر وفقاً للإطار الوطني للمؤهلات:
8. Notional Hours:	133	8. عدد الساعات الافتراضية:
9. NQF Credits	13	9. عدد الساعات المعتمدة للمقرر وفقاً للإطار الوطني للمؤهلات:
10. Prerequisite:	MATHS 254	10. المتطلب المسبق للمقرر:
11. Lectures Timing & Location:	TBA	11. وقت المحاضرة ومكانها:
12. General Mode of Teaching and Learning	Traditional تقليدي	12. النمط العام للتعليم والتعلم:
13. Course Coordinator:	TBA	13. منسق المقرر:
14. Course Instructor:	TBA	14. مدرس المقرر:
15. Office Hours and Location:	TBA	15. الساعات المكتبية ومكانها:
16. Instructor's Email:	TBA	16. البريد الإلكتروني لمدرس المقرر:
17. Academic Year:		17. السنة الأكاديمية:
18. Semester:	First Semester الفصل الأول	18. الفصل الدراسي:

19. Textbook(s):		19. الكتب الدراسية للمقرر:
An Introduction to Mathematical Cryptography (Second Edition) by Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman Undergraduate Texts in Mathematics Springer-Verlag 2014		
20. References:		20. المراجع:
- Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, CRC Press, 1996. - A Course in Number Theory and Cryptography by Neal Koblitz Springer-Verlag, 1994. - Cryptography made Simple by Nigel Smart Springer-Verlag, 2016.		
21. Other learning resources used (e.g. e-Learning, field visits, periodicals, software, etc.):		21. مصادر أخرى (مثال : التعلم الالكتروني، زيارات ميدانية، دورات، برامج كمبيوتر، الخ....)
University Official Platforms (BB & MT)		
22. Course Description (as published in the College Catalogue):		22. توصيف المقرر (حسبما ورد في دليل الكلية):
Modular Arithmetic and Prime Numbers. Classic Ciphers and Accompanying Attacks. Public Key Cryptography. Primality Tests. Elliptic Curve Cryptography. Historical and Social Consequences with Applications of Cryptography.		
23. Course Intended Learning Outcomes (3 to 5 CILOs):	23. مخرجات التعلم للمقرر (CILOs) (3 إلى 5 مخرجات تعليمية):	
1. Explain the idea of public-key cryptography and the common algorithms used.		
2. Describe the basic issues around finding large prime numbers and factoring large composite numbers		
3. Explain the significance of some number theory problems to public key cryptography.		
4. Construct elliptic curves and explain their use in cryptography		
5. Construct cryptographic hash functions		
24. Course Assessment Percentages (As per Regulations of Study and Examination at the University of Bahrain):	24. أساليب التقويم ونسبها المئوية (بحسب نظام الدراسة والامتحانات في جامعة البحرين):	
OTHERS	20%	
TEST#1	20%	
TEST#2	20%	
EXAM	40%	
Total	100%	
This assessment includes regular assignments, homework, or quizzes with a minimum of two assessments per semester. These assessments are usually conducted using e-learning tools such as Blackboard, WebAssign, and ALEKS.		
25. Description of Topics Covered:	25. وصف الموضوعات التي ينبغي تناولها:	
Topic Title (e.g. chapter/experiment title) الموضوع	Description التفصيل	
Chapter 1	An Introduction to Cryptography	
Chapter 2	Discrete Logarithms and Diffie Hellman	
Chapter 3	Integer Factorization and RSA	
Chapter 4	Digital Signatures	
Chapter 6	Elliptic Curves and Cryptography	
Chapter 8	Additional Topics in Cryptography	

26. Weekly Schedule			26. الجدول الأسبوعي:	
Week الأسبوع	Date التاريخ	Topics Covered المواضيع المعروضة	CIOs المخرجات التعلمية للمقرر (CIOs)	Teaching/Assessment Mode and Method منهجية ونمط التدريس/التقييم
01		Substitution Ciphers	1,5	Traditional Teaching تدريس تقليدي
02		1.2 Divisibility and Greatest Common Divisors	1, 2, 3	
03		1.3 Modular Arithmetic	1, 2, 3	
04		1.4 Prime Numbers, Unique Factorization, and Finite Fields	1, 2, 3	
05		1.5 Powers and Primitive Roots in Finite Fields	1, 2, 3	
06		1.7 Symmetric and Asymmetric Ciphers	1, 5	
07		2.2 The Discrete Logarithm Problem 2.3 Diffie–Hellman Key Exchange	1, 3	
08		2.4 The El Gamal Public Key Cryptosystem 2.5 An Overview of the Theory of Groups	1, 3	
09		2.7 A Collision Algorithm for the DLP 2.8 The Chinese Remainder Theorem	1, 3	
10		3.1 Euler's Formula and Roots Modulo pq 3.2 The RSA Public Key Cryptosystem	1, 2, 3	
11		3.3 Implementation and Security Issues 3.4 Primality Testing	1, 2, 3	
12		4.1 Digital Signature 4.2 RSA Digital Signature 4.3 El Gamal Digital Signatures and DSA	1, 2, 3	
13		6.1 Elliptic Curves 6.2 Elliptic Curves over Finite Fields	3, 4	
14		6.3 The Elliptic Curve Discrete Logarithm Problem (ECDLP) 6.4 Elliptic Curve Cryptography	3, 4	
15		8.1 Hash Functions 8.2 Pseudorandom Number Generators (PRNGs) 8.3 Zero-knowledge Proofs	1, 5	

27. Academic Integrity Statement:	27. بيان النزاهة الأكاديمية:
Students are to observe the highest level of honesty and academic ethics in pursuit of their academic goals as per UOB Regulations of Student Conduct and Academic Integrity, Anti-plagiarism Policies , and Students' Rights and Responsibilities Handbook . The consequences for cheating, plagiarism, unauthorized collaboration, and other forms of academic dishonesty can be very serious and will be dealt with as per the aforementioned policies and regulations.	يعتبر الصدق والنزاهة عنصران أساسيان في العملية الأكاديمية. حيث يُتوقع من الطلاب خلال سعيهم لتحقيق أهدافهم الأكاديمية التحلي بالأمانة والأخلاق في جميع الأوقات، وذلك وفقاً للوائح والأنظمة الخاصة بطلبة جامعة البحرين، بالإضافة إلى دليل حقوق الطلبة وواجباتهم ، وكما جاء في سياسة الانتحال الخاصة بجامعة البحرين . حيث سيتم التعامل مع أي انتهاك للنزاهة الأكاديمية بحسب ما تنص عليه السياسات والأنظمة السابق ذكرها.
28. Attendance and Absence Regulations:	28. نظام الحضور والغياب:
Students are required to adhere to regular attendance for class lectures and practical sessions, as determined by the nature of the course, as per Article (33), of Regulations of Study and Examination at the University of Bahrain .	يُتوقع من الطلاب الالتزام بالحضور المنتظم للساعات الصفية والعملية بحسب طبيعة المقرر، وفقاً للمادة (33)، من نظام الدراسة والامتحانات في جامعة البحرين .