

UNIVERSITI TEKNOLOGI MARA

CSC669: CRYPTOGRAPHIC ALGORITHMS

Course Name (English)	CRYPTOGRAPHIC ALGORITHMS APPROVED		
Course Code	CSC669		
MQF Credit	3		
Course Description	Cryptography plays a key role in ensuring the privacy and integrity of data and the security of computer networks. The course will provide an overview of an introductory level of cryptography written from a modern, computer science perspective. This course will be blend of theory and practice, covering standardized cryptosystems widely used in practice without sacrificing rigor or an emphasis on foundations. The course also shed light on the entrepreneur and to prepare the students with the essence of entrepreneurship and business planning skills that is essential for the success of new ventures. The subject delivery combines both theoretical and practical aspects of cryptography algorithms		
Transferable Skills	Apply cryptography algorithms		
Teaching Methodologies	Lectures, Blended Learning, Lab Work		
CLO	CLO1 Compose a plan incorporating security properties and techniques CLO2 Explains systematically cryptography algorithms in application/software CLO3 Integrate the entrepreneurial mind in identifying business opportunities on application/software of cryptography algorithms		
Pre-Requisite Courses	No course recommendations		
Topics			
1. Introduction of cryptography algorithms 1.1) History 1.2) Definition term 1.3) Type of cryptography 2. Symmetric			
2.1) Block cipher 2.2) Stream cipher			
3. Asymmetric 3.1) Public key			
4. Hash functions 4.1) N/A			
5. Cryptosystems 5.1) N/A			
6. Recent developm 6.1) N/A	nent of cryptography algorithms		

Faculty Name : COLLEGE OF COMPUTING, INFORMATICS AND MATHEMATICS

Start Year : 2018

Copyright Universiti Teknologi MARA

Review Year : 2021

Assessment Breakdown	%
Continuous Assessment	100.00%

Details of				
Continuous Assessment	Assessment Type	Assessment Description	% of Total Mark	CLO
	Discussion	Presentation 1	10%	CLO2
	Discussion	Presentation 2	10%	CLO3
	Lab Exercise	Lab	20%	CLO2
	Reading Response	Reporting	20%	CLO3
	Test	Test 1	20%	CLO1
	Test	Test 2	20%	CLO1

Reading List	Recommended Text	Jonathan Katz,? Yehuda Lindell, , Introduction to Modern Cryptography: Principles and Protocols, 1st Ed., Chapman & Hall/ [ISBN: 978-158488551]			
	Reference Book Resources	Matt Bishop 2005, Introduction to Computer Security, Addison-Wesley Professional [ISBN: 0-321-24744-2]			
		Dieter Gollmann 2006, <i>Computer Security</i> , John Wiley & Sons [ISBN: 0470862939]			
		Charles P. Pfleeger,Shari Lawrence Pfleeger 2007, Security in Computing, Prentice Hall [ISBN: 9780132390774]			
		Christoph Kern,Anita Kesavan,Neil Daswani 2007, Foundations of Security, Apress [ISBN: 1590597842]			
		John Viega, Gary McGraw, Building Secure Software: How to Avoid Security Problems the Right Way, Addison-Wesley Professional [ISBN: 978032177495]			
Article/Paper List	This Course does not have any article/paper resources				
Other References	This Course does not have any other resources				

Faculty Name : COLLEGE OF COMPUTING, INFORMATICS AND MATHEMATICS

Start Year : 2018

Copyright Universiti Teknologi MARA

Review Year : 2021