MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

1.	Name of Course	Applied Cryptography
2.	Course Code	TAC 3121
3.	Status of Course [Applies to (cohort)]	Specialisation Core for B.IT Security Technology
4.	MQF Level/Stage Note : *Certificate – MQF Level 3* *Diploma – MQF Level 4* *Bachelor – MQF Level 6* *Masters – MQF Level 7* *Doctoral – MQF Level 8*	Bachelor Degree – MQF Level 6
5.	Version (State the date of the Senate approval – history of previous and current approval date)	Date of previous version: June 2012 Date of current version: June 2014
6.	Pre-Requisite	TDS2111 Data Structures and Algorithms
7.	Name(s) of academic/teaching staff	Jaya Kumar Krishnan Tan Syh Yuan Low Cheng Yaw
8.	Semester and Year offered	Trimester 1, Year 3
9.	Objective of the course in the programme : To introduce the students to the definitions and constructions of various cryptosystems, and the underlying security issues.	
10.	Justification for including the course in the programme : The knowledge is important for Security Technology students because cryptography is the theoretical basis of computer and network security. This course covers the basic of cryptography; the basic of computational number theory; the constructions and security issues of various cryptosystems, such as symmetric encryption schemes (stream cipher and block cipher), message authentication codes and hash functions, asymmetric encryption schemes and digital signature schemes.	

11.	Course Learning Outcomes :	Domain	Level
	LO1: Recall the definitions of all the concepts and technical terms related to fundamental concepts of cryptography.	Cognitive	1
	LO2: Apply fundamental of cryptanalysis concepts in cryptographic applications.	Cognitive	3
	LO3: Appraise different security	Cognitive	6

	level of various cryptosystems between the various cryptographic schemes.		
	LO4: Analyse and assess the various cryptosystems and applications.	Affective	4
	LO5: Implement some simple cryptographic schemes.	Cognitive	3

12. Mapping of Learning Outcomes to Programme Outcomes :

Learning Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9
LO1		X							
LO2								X	
LO3							X		
LO4	X						X	X	
LO5	X						X	X	

13. Assessment Methods and Types :

Method and Type	Description/Details	Percentage
Test	Written Test	20%
Quiz	Written Quiz	5%
Assignment	Report & Presentation	15%
Final Exam	Written Exam	60%

14. Mapping of assessment components to learning outcomes (LOs)

Assessment Components	LO1	LO2	LO3	LO4	LO5
Test	23.53	23.53	23.53		
Quiz	5.88	5.88	5.88		
Assignment				100	100
Final Exam	70.59	70.59	70.59		

15. Details of Course

Topics	Mode of Delivery (eg : Lecture, Tutorial, Workshop, Seminar, etc.) Indicate allocation of SLT (lecture, tutorial, lab) for each subtopic	
	Lecture	Tutorial
1. Introduction a. Overview of Symmetric and Public-Key Cryptography b. Basic Terminology	2	1

SUMMARY OF INFORMATION ON EACH COURSE

	c. Cryptanalysis – Brute Force and Cryptanalytic Attacks		
	2. Finite Fields and Computational Number Theory a. Groups, Rings, Fields b. Modular Arithmetic c. Finite Fields of the Form GF(p) and GF(2n) d. Prime Numbers, the Greatest Common Divisor, the Euclidean Algorithm, Multiplicative Inverse e. Euler's Phi Function, Fermat's and Euler's Theorem, the Chinese Remainder Theorem f. Discrete Logarithm Problem and Diffie-Hellman Problem	4	2
	3. Classical Ciphers a. Symmetric Cipher Model b. Substitution Ciphers c. Transposition Ciphers d. The Security of Classical Ciphers	2	1
	4. Symmetric Encryption a. The Feistel Networks b. The Data Encryption Standard (DES) c. The Security of DES d. Triple DES e. The Advanced Encryption Standard (AES) f. Block Cipher Modes of Operation - ECB, CBC, CFB, OFB, CTR g. Stream Ciphers and RC4	5	3
	5. Message Authentication and Hash Functions a. Authentication Requirements and Functions b. Message Authentication Codes (MAC) c. Hash Functions d. Security of Hash Functions and MAC	3	1

SUMMARY OF INFORMATION ON EACH COURSE

	e. Specific MACs - HMAC, CBC-MAC, CMAC f. Specific Hash Functions – SHA-1		
	6. Asymmetric (Public-Key) Encryption a. Asymmetric Encryption Model b. The RSA Encryption c. The Rabin Encryption d. The ElGamal Encryption e. The insecurity of the "textbook version" of RSA, Rabin and ElGamal Encryptions f. Introduction to Elliptic Curve Cryptosystems	6	3
	7. Digital Signature a. Security Requirements for Signature Schemes b. The RSA Signature c. The ElGamal Signature d. The Digital Signature Algorithm (DSA) e. The security of RSA and ElGamal signature schemes, and DSA	4	2
	8. Key Establishment and Key Management a. Key Establishment – Symmetric Techniques (KDC) and Asymmetric Techniques (Diffie-Hellman Key Exchange) b. Digital Certificates, Certification Authority (CA), Public Key Infrastructure (PKI)	2	1
	Total	**28**	**14**

Total Student Learning Time (SLT)	Face to Face / Guided Learning	Independent Learning
Lecture	28	28
Tutorials	14	14
Laboratory/Practical	0	0
Presentation	0	0
Assignment	0	10
Mid Term Test	1	5
Final Exam	2	16

SUMMARY OF INFORMATION ON EACH COURSE

	Quizzes	2 times	2
	Sub Total	45	75
	Total SLT	**120**	
16.	Credit Value	**120/40 = 3**	
17.	Reading Materials :		
	Textbooks		
	William Stallings, (2013). Cryptography and Network Security - Principles and Practices, 6th Edition, Prentice Hall. Wenbo Mao, (2003). Modern Cryptography: Theory and Practice, Wiley 2003.		
	Reference Material (including 'Statutes' for Law)		
	D. Stinson, (2002). Cryptography: Theory and Practice, CRC Press Inc., 2nd Edition. ISBN 1-58488-206-9. Bruce Schneier. Applied Cryptography, 2nd Edition - Protocols, Algorithms and Source Code in C, John Wiley & Sons. ISBN:0-471-12845-7 Alfred J. Menezes, Paul C. van Oorshot and Scott A. Vanstone, (2001). Handbook of Applied Cryptography, CRC Press. WadeTrappe, Lawrence Washington. Introduction to Cryptography with Coding Theory, Second Edition, Prentice Hall. ISBN : 0-13-186239-1. M. G. Luby, (1996). Pseudorandomness and Cryptographic Applications, Princeton University Press. R. E. Smith, (1997). Internet Cryptography, Addison-Wesley.		

Appendix (to be compiled when submitting the complete syllabus for the programme) :

1. Mission and Vision of the University and Faculty
2. Programme Objectives or Programme Educational Objectives
3. Programme Outcomes (POs)
4. Mapping of POs to the 8 MQF domain
5. Summary of the Bloom's Taxonomy's Domain Coverage in all the Los in the format below :

Subject	Learning Outcomes (please state the learning 0utcomes)	Bloom's Taxonomy Domain		
		Affective	Cognitive	Psychomotor
ABC1234	Learning Outcome 1			
	Learning Outcome 2			
	Learning Outcome 3			
	Learning Outcome 4			
DEF5678	Learning Outcome 1			
	Learning Outcome 2			
	Learning Outcome 3			
	Learning Outcome 4			

MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

6. Summary of LO to PO measurement
7. Measurement and Tabulation of result for LO achievement
8. Measurement Tabulation of result for PO achievement