1.	Name of Course/Module	Applied Cryptography
2.	Course Code	TAC2681
3.	Status of Subject	Major for B.IT Security Technology
4.	MQF Level/Stage	Bachelor Degree – MQF Level 6
5.	Version (state the date of the last Senate approval)	June 2012
6.	Requirement for Registration	TCS 1011 Data Structures and Algorithms
7.	Name(s) of academic/teaching staff	K.Jayakkumar Asrul Hadi b Yaacob Low Cheng Yaw
8.	Semester and Year offered	Trimester 2 (Gamma Level)

9. Objective of the course/module in the programme :

To introduce the students to the definitions and constructions of various cryptosystems, and the underlying security issues.

10. Learning Outcomes :

At the completion of the subject, students should be able to:

LO1: Recall the definitions of all the concepts and technical terms related to fundamental concepts of cryptography. (Cognitive, Level 1)
LO2: Apply fundamental of cryptanalysis concepts in cryptographic applications. (Cognitive, Level 3)
LO3: Appraise different security level of various cryptosystems between the various cryptographic schemes. (Cognitive, Level 6)
LO4: Analyse and assess the various cryptosystems and applications. (Affective, Level 4)
LO5: Implement some simple cryptographic schemes. (Cognitive, Level 3)

11. Synopsis:

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.

Kursus ini meliputi kriptografi asas, asas pengiraan dalam teori nombor dan pelbagai primitif kriptografi dan isu-isu keselamatan berkaitan seperti skema pengekodan simetri (tulisan rahsia arus dan tulisan rahsia blok), kod pengesahan mesej dan fungsi “hash”, skema pengekodan tak simetri dan tandatangan digital.

12. Mapping of Subject to Programme Outcomes :

Programme Outcomes	**% of Contribution**
PO1: Apply soft skills in work and career related activities	25.00
PO7: Demonstrate knowledge and understanding of essential facts, concepts, principles, and theories relating to security technology	37.50

	PO8: Apply principles and knowledge of security technology in relevant areas		37.50
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. Details of Subject

Topics	Mode of Delivery	
	Lecture	Tutorial
1. Introduction • Overview of Symmetric and Public-Key Cryptography • Basic Terminology • Cryptanalysis – Brute Force and Cryptanalytic Attacks	2	1
2. Finite Fields and Computational Number Theory • Groups, Rings, Fields • Modular Arithmetic • Finite Fields of the Form GF(p) and GF(2n) • Prime Numbers, the Greatest Common Divisor, the Euclidean Algorithm, Multiplicative Inverse • Euler's Phi Function, Fermat's and Euler's Theorem, the Chinese Remainder Theorem • Discrete Logarithm Problem and Diffie-Hellman Problem	4	2
3. Classical Ciphers • Symmetric Cipher Model • Substitution Ciphers • Transposition Ciphers • The Security of Classical Ciphers	2	1
4. Symmetric Encryption • The Feistel Networks • The Data Encryption Standard (DES) • The Security of DES • Triple DES • The Advanced Encryption Standard (AES) • Block Cipher Modes of Operation - ECB, • CBC, CFB, OFB, CTR • Stream Ciphers and RC4	5	3
5.Message Authentication and Hash Functions • Authentication Requirements and Functions • Message Authentication Codes (MAC) • Hash Functions • Security of Hash Functions and MAC • Specific MACs - HMAC, CBC-MAC, CMAC • Specific Hash Functions – SHA-1	3	1

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

15. Tutorials

- Finite Fields and Computational Number Theory
- Classical Ciphers
- Symmetric Encryption
- Message Authentication and Hash Functions
- Asymmetric (Public-Key) Encryption
- Digital Signature
- Key Establishment and Key Management

16.

Total Student Learning Time (SLT)	Face to Face (Hour)	Total Guided and Independent Learning
Lecture	28	28
Tutorials	14	14
Laboratory/Practical		
Presentation		
Assignment	-	10
Mid Term Test	1	5
Final Exam	2	20
Quizzes	2 times	2
Sub Total	45	79
Total SLT	124/40 = 3.1 => 3	

17.	Credit Value	3
18.	Reading Materials :	
	Textbook	Reference Materials

	1. Wenbo Mao, “Modern Cryptography: Theory and Practice”, Wiley 2003. ISBN 0-130066943- 2. William Stallings, “Cryptography and Network Security - Principles and Practices”, 4th Edition, Prentice Hall 2006. ISBN 0-13-111502-2.	1. D. Stinson, “Cryptography: Theory and Practice”, CRC Press Inc., 2nd Edition, 2002. ISBN 1-58488-206-9. 2. Bruce Schneier, “Applied Cryptography, 2nd Edition - Protocols, Algorithms and Source Code in C, John Wiley & Sons. ISBN:0-471-12845-7 3. Alfred J. Menezes, Paul C. van Oorshot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001. http://www.cacr.math.uwaterloo.ca/hac 4. WadeTrappe, Lawrence Washington, “Introduction to Cryptography with Coding Theory”, Second Edition, Prentice Hall. ISBN : 0-13-186239-1. 5. M. G. Luby, “Pseudorandomness and Cryptographic Applications”, Princeton University Press, 1996. 6. R. E. Smith, “Internet Cryptography”, Addison-Wesley, 1997.
19.	Appendix (to be compiled when submitting the complete syllabus for the programme) : 1. Mission and Vision of the University and Faculty 2. Mapping of Programme Objectives to Vision and Mission of Faculty and University 3. Mapping of Programme Outcome to Programme Objectives 4. Programme Objective and Outcomes (Measurement and Descriptions)	