Module 5: Cryptography

Stage	1
Semester	2
Module Title	Cryptography
Module Number	5
Module Status	Mandatory
Module ECTS Credits	10
Module NFQ level	9
Pre-Requisite Module Titles	None
Co-Requisite Module Titles	None
Capstone Module?	No
List of Module Teaching Personnel	Dr. Faheem Bukhatwa

Contact Hours				**Non-contact Hours**			**Total Effort (hours)**
60				**140**			**200**
Lecture	**Practical**	**Tutorial**	**Seminar**	**Assignment**	**Placement**	**Independent Work**	
36		24		40		100	

Allocation of Marks (Within the Module)					
	Continuous Assessment	**Project**	**Practical**	**Final Examination**	**Total**
Percentage Contribution	**50**			**50**	**100**

Intended Module Learning Outcomes

On successful completion of this module the learner will be able to:

1. Discuss the fundamentals of communication security
2. Analyse and document the skills and tools necessary to develop secure communication systems
3. Apply a number of important cryptographic schemes
4. Conduct appropriate research about future trends in the area
5. Design and develop a conventional encryption based system
6. Design and develop a Public-key encryption based system

Module Objectives

This module aims to provide the learner with a mastery of the core aspects of computer communication security. This module gives the learner a mastery of security models, policies and mechanisms, encryption and decryption, confidentiality, integrity, authentication, cryptography and secure communication, digital signatures, certificates and coding. The learner will gain in depth knowledge of the classical techniques as well as state of the art approaches of cryptography.

Module Curriculum

- **Introduction**
  History of classical encryption and security

- **Conventional Encryption Systems**
  Modern secret key encryption, Key distribution for symmetric ciphers.

- **Public key Encryption Systems**
  Public key system key generation, Public key encryption and decryption, Random number generation, Key distribution for symmetric ciphers.

- **Integrity and Authentication verses Confidentiality**
  Hash functions; message authentication codes; digital signatures

- **Encryption and the Internet**
  Public key infrastructure (PKI); e-mail security; IPsec; Secure socket layer (SSL); secure electronic transactions (SET); firewalls.

- **Message authentication codes and Hash functions**
  Implementation, comparisons and design.

- **Developments in Modern Encryption**
  Digital watermarking; identification schemes; mobile communications and security; factoring; steganography; biometrics; distributed denial of service attacks; secret sharing; probabilistic encryption

- **Digital signatures**
  Hashing, Message authentication and digital signatures.

Reading Lists and other learning materials

Recommended Reading

Stallings W, 2010, *Cryptography and Network Security – Principles and Practice, 5th Edition*, Prentice Hall

Secondary Reading

Additional reading as recommended by lecturer, appropriate to topic area of security.

Module Learning Environment

Lectures and tutorials are carried out in class rooms / lecture halls or labs in the College.

Library

All learners have access to an extensive range of physical and electronic (remotely accessible) library resources. The library monitors and updates its resources on an on-going basis, in line with the College's Library Acquisition Policy. Lecturers update reading lists for this course on an annual basis as is the norm with all courses run by Griffith College.

Module Teaching and Learning Strategy

Learners are taught using a combination of lectures and tutorials. Case studies are used to demonstrate issues of relevance and guest lecturers bring current professional experience into the classroom.

Module Assessment Strategy

Assessing the learners includes continuous assessment carrying 50% and a final exam carrying 50% of the overall mark of the course.

Learners are continually assessed on a combination of the following work, completed during the course of the module:

Element No.	Weighting	Type	Description	Learning Outcomes Assessed
1.	10%	Tutorials	This will involve a series of tutorials. These aim at enhancing the understanding of concepts and ideas.	1,3,5, 6
2.	15%	Assignment	This will involve a programming work or producing a written technical paper format report.	2, 4
3.	25%	Test	This will happen during the second half of the semester. This will cover most of the topics involved during the course.	3,5, 6
4.	50%	Examination	End of module examination	1,2,3, 5, 6