

Module 6: Communications Security

Stage	1						
Semester	2						
Module Title	Communication Security						
Module Number	6						
Module Status	Mandatory						
Module ECTS Credits	10						
Module NFQ level	9						
Pre-Requisite Module Titles	None						
Co-Requisite Module Titles	Telecommunications and Network Services						
Capstone Module?	No						
List of Module Teaching Personnel	Dr. Faheem Bukhatwa						
Contact Hours				Non-contact Hours			Total Effort (hours)
36				164			200
Lecture	Practical	Tutorial	Seminar	Assignment	Placement	Independent Work	
36		24		40		100	200
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. explain the fundamentals of communication security
2. demonstrate an understanding of the skills and tools necessary to develop secure communication systems
3. employ a number of important cryptographic schemes
4. obtain knowledge 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 course aims to provide the learner with a mastery of the core aspects of computer communication security. This course of study gives them a mastery of security models, policies and mechanisms, confidentiality, integrity, authentication, cryptography and secure communication, digital signatures, certificates and the practical aspects of secure programming.

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

Reading Lists and other learning materials

Recommended Reading

Cryptography and Network Security – Principles and Practice	Stallings, W	Prentice-Hall	2010
Firewalls and Internet Security	Cheswick, W. R. Bellovin, S. M.	Addison Wesley	2003

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.

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 given on weekly basis. These aim at enhancing the understanding of concepts and ideas.	1,2,3,4,6
2.	15%	Assignment	This will involve a programming work or producing a written technical paper format report.	1,2,4,5
3.	25%	Test	This will happen during the second half of the semester. This will cover most of the topics involved during the course.	1,2,3
4.	50%	Examination	End of module examination	1,2,3,5,6