Module Title:	Secure Systems
Module Code:	01H
Level:	6
Credits:	15
Pre-Requisites:	None

Module Description:
IT security is one of the key concerns of organisations today. Protection of company data, either on networked systems within the company or while in transit over the internet, has become a priority.

The aim of this module is to provide a practical guide to network security issues. It looks at the threats faced by organisations. Cryptography and authentication issues are covered. Problems concerned with securing the perimeter, securing the network, securing applications and securing data are all investigated. Ethical issues concerning data protection and hacking will be explored. Strategies for disaster recovery are examined.

Indicative Content:

- Security objectives and policies
- Principles of encryption, hashing, digital signatures, digital certificates, Public-Key encryption algorithms
- Web Security, such as Secure Socket Layer and Secure Electronic Transaction
- Viruses and worms
- Securing web applications and FTP, securing e-mail systems, securing databases
- Data security and access control mechanisms. Securing data using encryption and signing
- Penetration testing
- Disaster Planning
- Cross-Site Scripting, SQL injection, Google Hacking
- Firewall, Intrusion Detection Systems, Intrusion Protection Systems

Learning and Teaching Methods:
The module will be presented through lectures) that provide the opportunity for research and group work. Moodle will be used to facilitate learning.

Specific Learning Resources:

Access to PCs, on a private network, on which Intrusion Detection Software and probe software can be loaded

Bibliography

Highly Recommended

McClur, S., Scambray, J. and Kurtz, G. (2012) *Hacking Exposed 7: Network Security*

Secrets and Solutions. USA: McGraw-Hill

Pfleeger, C and Pfleeger, S.L. (2006) *Security in Computing, (4th edition).* New Jersey: Prentice Hall

Recommended

Stallings, W. (2010) *Cryptography and Network Security: International Version: Principles and Practice*, Pearson

Background Reading

Dhillon, G. (2006) *Principles of Information Systems Security: Text and Cases.* Hoboken: John Wiley and sons

National Institute of Standards and Technology (NIST) Information Technology Library http://www.csrc.nist.gov

Sans Institute (2009) *The Top Cyber Security Risks.* [online] Available at: <http://libweb.anglia.ac.uk/referencing/harvard.htm>

Stinson, D. (2006) *Cryptography: Theory and Practice, (3rd Edition) (Discrete Mathematics and Its Applications)*. USA: CRC Press

The ISO 27000 Directory http://www.2700.org

Whitman, M and Mattford H. (2010) *Management of Information Security. (3rd edition)*. Boston: Course Technology

Module Learning Outcomes

Subject Specific Learning Outcomes

On successful completion of this module you will be able to:

LO 1	Analyse recent security threats and available mechanisms to protect organisations
LO 2	Evaluate the algorithms used in cryptography, and be able to perform implementations of selected algorithms in this area
LO 3	Select and justify choices of the appropriate security measures to put in place for a given network and/or operating system

LO 4	Examine and appraise IT security policies, and evaluate data security in the light of ethical and legal frameworks

Assessment Title or element	**Weighting (%)**
Assignment: analyse security threats and propose security measures and policies to address these threats (2000 words) [late semester]	50%
Exam (1hr 30min) [end semester]	50%

Information correct at point of publication.