**DEREE COLLEGE SYLLABUS FOR:**

**ITC 4322 NETWORK SECURITY AND CRYPTOGRAPHY** **3/0/3**

(Updated Spring 2016) **UK LEVEL 6**
**UK CREDITS: 15**

**PREREQUISITES:**

MA 1108 College Algebra

ITC 3106 Mathematics for Computing

ITC 3121 Computer Networks, Modelling and Analysis

**CATALOG DESCRIPTION:**

Security trends and solutions; encryption techniques and standards; symmetric and public key encryption; hash functions; confidentiality issues; authentication and identity management; system security issues.

**RATIONALE:**

The course is intended for students following the Network Technologies emphasis of the IT major. It focuses on the techniques of cryptography and network security. Students are further exposed to network security through practical applications.

**LEARNING OUTCOMES:**

As a result of taking this course, the student should be able to:

1. Analyze security threats, attacks and needs.
2. Explain encryption standards and techniques.
3. Analyze security algorithms and functions.
4. Evaluate authentication protocols and requirements.

**METHOD OF TEACHING AND LEARNING:**

In congruence with the learning and teaching strategy of the College, the following tools/activities are used:

- Lectures, class discussions, and review of real-world cases based on specific theoretical concepts. Laboratory practical sessions.
- Instructor office hours
- Use of the Blackboard Learning platform, where instructors post lecture notes, assignment instructions, timely announcements, as well as additional resources.

**ASSESSMENT:**

**Summative:**

| | |
|---|---|
| Project: literature review/data collection/ methodology/implementation (code, script or simulation) | **50%** |
| Final Examination (2-hour comprehensive): combination of short essay questions and case problems. | **50%** |

**Formative:**

| | |
|---|---|
| In-class, 1-hour, "diagnostic" test: short answers to essay questions | **0** |
| Coursework: case problems | **0** |

The formative assessments aim to shape teaching along the semester and prepare students for the summative assessments.

The project tests learning outcomes 2, 3.

The final examination tests learning outcomes 1,2,3,4

**INDICATIVE READING:**

**REQUIRED READING:**

Stallings W., (2013), *Cryptography and Network Security*, Prentice Hall

| | |
|---|---|
| | **RECOMMENDED READING:**<br>Erickson J., (2008), *Hacking: The Art of Exploitation,* No Starch Press (latest international edition).<br>Ferguson N. & Schneier B., (2003), *Practical Cryptography*, Wiley<br>Paar C. & Pelzl J., (2010) *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer<br>Tanenbaum A., (2010), *Computer Networks*, Prentice Hall Inc. |
| **INDICATIVE MATERIAL:** *(e.g. audiovisual, digital material, etc.)* | **REQUIRED MATERIAL:** N/A<br>**RECOMMENDED MATERIAL:** N/A |
| **COMMUNICATION REQUIREMENTS:** | Daily access to the course's site on the College's Blackboard CMS. Effective presentation skills using proper written and oral English. Communicate and coordinate during team activities. |
| **SOFTWARE REQUIREMENTS:** | Microsoft Windows 20xx Advanced Server, latest<br>Microsoft Windows 7+ Professional, latest<br>Microsoft TechNet Library<br>Kali Linux (or Ubuntu) |
| **WWW RESOURCES:** | Textbook student resources (http://williamstallings.com/Crypto/Crypto4e.html)<br>Cryptography demos (http://nsfsecurity.pr.erau.edu/crypto/index.html)<br>Security Cartoon (http://securitycartoon.com/)<br>IETF Security Area (http://trac.tools.ietf.org/area/sec/trac/wiki)<br>Internet Cryptography<br>(http://www.mindspring.com/~dmcgrew/ic/internet-crypto.html) |
| **INDICATIVE CONTENT:** | 1. Security trends, attacks, services, and mechanisms<br>2. Symmetric Ciphers<br>  1. Classical encryption techniques<br>  2. Block ciphers and the data encryption standards<br>  3. Finite fields<br>  4. Advanced encryption standards<br>  5. Confidentiality using symmetric encryption<br>3. Public-key encryption and hash functions<br>  1. Overview of number theory<br>  2. Public-key cryptography and RSA<br>  3. Key management<br>  4. Message authentication and hash functions<br>  5. Hash and MAC algorithms<br>  6. Digital signatures and authentication protocols<br>4. Network security applications<br>  1. Authentication applications<br>  2. Electronic mail security<br>  3. IP Security<br>  4. Web Security<br>5. System security<br>  1. Intruders<br>  2. Malicious software<br>  3. Firewalls |