DEREE COLLEGE SYLLABUS FOR:

ITC 3431 CRYPTOGRAPHY AND NETWORK SECURITY

(Fall 2020)

3/0/3
UK LEVEL: 5
UK CREDITS: 15

PREREQUISITES:	ITC 2024 Computer Networks & Cybersecurity Fundamentals ITC 2088 Introduction to Programming MA 2010 Statistics I ***or*** MA 2021 Applied Statistics for Business ***or*** MA 2025 Applied Statistics for Science
COREQUISITES:	ITC 3006 Mathematics for Computing
CATALOG DESCRIPTION:	Basic symmetric encryption algorithms; DES, AES; Public key encryption; hash functions; digital signatures; confidentiality issues; authentication and identity management; SSL/TLS; IP security.
RATIONALE:	The course focuses on the techniques used for cryptography and cryptanalysis, the principles underpinning all modern network security techniques and their relation to existing protocols and real system implementations. Students are exposed to network security through practical applications using tools such as Wireshark.
LEARNING OUTCOMES:	As a result of taking this course, the student should be able to: 1. Analyze and apply symmetric encryption algorithms. 2. Analyze and apply public-key encryption algorithms, functions, and standards. 3. Interpret cryptographic security threats. 4. Discuss main network security requirements and applications.
METHOD OF TEACHING AND LEARNING:	In congruence with the teaching and learning strategy of the college, the following tools are used: • Classroom lectures, laboratory practical sessions using various simulations tools. • Office hours held by the instructor to provide further assistance to students. • Use of the Blackboard Learning platform, where instructors post lecture notes, assignment instructions, timely announcements, as well as additional resources.

ASSESSMENT:

Summative:

1st assessment: Group Project literature review, design, implementation (code, script or simulation)	**30%**
2nd assessment: Portfolio of student work and oral assessment	**10%**
Final assessment: Final Exam Short essay questions and case problems.	**60%**

Formative:

Take-home short problems, quizzes, project progress	**0%**

	The formative assessments aim to prepare students for the summative assessments. The 1st summative assessment tests the LOs 1 and 3. The 2nd summative assessment tests the LOs 1-4. The final summative assessment tests the LOs 1-4. *The final grade for this module will be determined by averaging all summative assessment grades, based on predetermined weights for each assessment. If students pass the* ***final summative assessment,*** *which tests all Learning Outcomes for this module, and the average grade for the module is 40 or above, students are not required to resit any failed assessments.*
INDICATIVE READING:	**REQUIRED READING:** 1. Stallings W., Cryptography and Network Security, Prentice Hall, 7th edition 2019. **RECOMMENDED READING:** 1. Paar C. & Pelzl J., (2010) *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer 2. Ferguson N. & Schneier B., (2003), *Practical Cryptography*, Wiley 3. Erickson J., (2008), *Hacking: The Art of Exploitation,* No Starch Press (latest international edition).
INDICATIVE MATERIAL: *(e.g. audiovisual, digital material, etc.)*	**REQUIRED MATERIAL:** N/A **RECOMMENDED MATERIAL:** N/A
COMMUNICATION REQUIREMENTS:	Daily access to the course's site on the College's Blackboard CMS. Communication using proper written and oral English. Use of word processing and/or presentation graphics software for documentation of deliverables and final project.
SOFTWARE REQUIREMENTS:	MS-Office C, Python Octave, Matlab, VMWare
WWW RESOURCES:	• Textbook student resources (http://williamstallings.com/Crypto/Crypto4e.html) • Christof Paar - Introduction to Cryptography courses in YouTube. • Cryptography demos (http://nsfsecurity.pr.erau.edu/crypto/index.html) • Security Cartoon (http://securitycartoon.com/) • IETF Security Area (http://trac.tools.ietf.org/area/sec/trac/wiki) • Internet Cryptography (http://www.mindspring.com/~dmcgrew/ic/internet-crypto.html)
INDICATIVE CONTENT:	1) Symmetric Ciphers a) Classical encryption techniques b) DES c) AES 2) Public-key encryption and hash functions a) Public-key cryptography and RSA

	b) Key management c) Message authentication and hash functions d) Hash and MAC algorithms e) Digital signatures and authentication protocols 3) Network security applications a) Authentication applications b) Electronic mail security c) Web Security Standards (SSL/TLS) d) IP Security