Information Technology Department
College of Computing and Information Sciences

Course Delivery Plan

جامعة التقنية والعلوم التطبيقية
University of Technology and Applied Sciences

	Section	Day(s)	Time	Location	Tutorial Hours
Schedule of Course Lectures	1	Sun/Tue	10-12	D105	2
	2				
	3				

Course Name: Introduction to Cryptography	**Credit hours: 3**		**Academic Year:** 2022-2023	**Course Level: 2nd year Diploma**
Course Code: CSSY2201	**Contact Hours:**	**Theory (hr/week): 3** **Practical (hr/week): 3**	**Semester:** ☐ **Fall** ☒ **Spring** ☐ **Summer**	**Passing Grade:** C
Course Pre-requisite(s)/ Co-requisite(s): **CSSY1208- Introduction to Information Security**	**Course Type:** ***(Tick all that applies)*** ☐ University Requirement ☐ University Elective ☐ Department Requirement ☐ Department Elective ☐ College Requirement ☒ Specialization Requirement ☐ Specialization Elective			

Faculty Details

Name	
Room No.	
Office Hours	
Contact for Academic Inquiries	

Course Description
This course provides basic and practical concepts on cryptography and cryptanalysis. The course covers a detailed description of the building blocks of symmetric ciphers, hash/HMAC algorithms, asymmetric ciphers, key management process with a practical implementation using Python 3.8. VS code or PyCharm are recommended IDEs for Python programming. Jupyter Notebook is used for interactive Python programing

Course Objectives	Course Learning Outcomes
This course will enable the students to: 1. Have an Extensive, detailed and critical understanding of basic concepts behind most used cryptographic primitives. 2. Develop a familiarity in modern cryptographic algorithms and enrich the knowledge to the students of existing deployed standards. 3. Equip students with practical implementation of symmetric and asymmetric cryptographic Algorithms	By the end of the course, the students will be able to: 1. Understand basic background behind most cryptographic standards 2. Implement cryptographic algorithms defined in cryptographic standards 3. Describe the purpose of cryptography and list ways it is used in data communications 4. Describe the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plaintext into ciphertext. 5. Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilitie 6. Analyse the dangers of inventing one’s own cryptographic methods 7. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation

4. Implement most of the algorithms using Python and Openssl.	

Graduate Attributes	1. Communication skills	2. Teamwork and leadership	3. Discipline knowledge and skills	4. Creativity and innovation
	5. Entrepreneurial skills	6. Lifelong learning	7. Technical and Digital competency	8. Critical thinking, analysis, and problem solving

Weekly Distribution of the lessons

Topics to be covered	**Contact Hours**		**Time plan (Week no.)**	**Coverage of Learning Outcomes**	**Coverage of Graduate Attributes**	**Methods for coverage of Outcomes**	**Assessment Method(s) /Activate(s)**
	Theory	**Practical**					
1. Introduction to cryptology **1.1.** Overview of Secret communications using cryptography **1.2.** Symmetric Cryptography **1.3.** Cryptanalysis **1.4.** Data Encoding	**2**	**2**	**1**	**1, 3, 4**	**1, 3, 6, 7**	Class Demonstration Hands on Exercise Discussion	**Lab1A:** Create a reverse encryption algorithm **Lab1B:** Authentication of a user using a password
2. Classical Cryptography **2.1.** Caesar Cipher **2.2.** Brute forcing Caesar **2.3.** Vigenere **2.4.** Playfair **2.5.** Rail Fence **2.6.** OTP	**4**	**4**	**2,3**	**1, 3, 4**	**1, 3, 6, 7**	Class Demonstration Hands on Exercise Discussion	**Lab2A:** Implement Caesar **Lab2B:** Implement brute force attack on Caesar

3. DES and modes of operations **3.1.** DES Structure **3.2.** 3DES structure **3.3.** Modes of operations ECB, CBC, CFB, OFB, CTR	**4**	**4**	**4,5**	**1, 2, 3, 4, 6,7**	**1, 3, 6, 7**	Class Demonstration Hands on Exercise Discussion	**Lab3A:** Use "Pycryptodome" module to Implement DES to encrypt/decrypt a message using ECB, CBC **Lab3B:** Use 3DES to encrypt/decrypt a file stored in your disk. **Activity 3C** : Apply ECB, CBC, CFB, OFB on a simple 2-bit or 4-bit substitution cipher. (wiki)
4. AES Standard **4.1.** General Design of AES **4.2.** Addroundkey **4.3.** SubBytes and InvSubBytes **4.4.** Shiftrows and InvShiftRows **4.5.** Mixcolumns and InvMixColumns	**2**	**2**	**6**	**1, 2, 3, 4, 6,7**	**1, 3, 6, 7**	Class Demonstration Hands on Exercise Discussion	**Lab4A:** Implement AES using the "Pycryptodome" module with different modes of block encryption. **Lab4B:** Implement AES using the "cryptography.fernet" module
			7	**Midterm**			

5. **Asymmetric Cryptography & RSA** **5.1.** Motivations for public key cryptography **5.2.** Principles of Asymmetric Cryptography **5.3.** Public key cryptography : Confidentiality **5.4.** Public key cryptography : Authentication **5.5.** Public key cryptography : Confidentiality + Authentication **5.6.** Applications for public key cryptography **5.7.** The RSA Algorithm : Encryp/Decryp and Key Generation **5.8.** RSA working examples **5.9.** Security of RSA	**4**	**4**	**8,9**	**1, 4, 5, 6,7**	**1, 3, 6, 7**	Class Demonstration Hands on Exercise Discussion	**Lab5A:** Openssl : RSA key generation using openssl, extract RSA pem keys, encryption/decryption **Lab5B:** Python : use “rsa” module to encrypt/decrypt. **Lab5C + Activity5C:** Python: generate keys, encrypt/decrypt with no helper module. Verify the python coding result with your own calculations using a calculator. **Course Project Progress**

6. Hash Function and Keyed Hash **6.1.** Defining hash functions **6.2.** Verifying data integrity with hashing **6.3.** Verifying data authentication with keyed hashing **6.4.** The HMAC primitive **6.5.** Using the hmac module for cryptographic hashing of documents in transit **6.6.** Pseudo Random Number Generators	**4**	**4**	**10, 11**	**1, 2, 6,7**	**1, 2, 3, 6, 7**	Class Demonstration Hands on Exercise Discussion	**Lab6A:** Use of Hashlib module to implement SHA256, MD5 to hash a message. Use digest(), hexdigest(), update() and base64 **Lab6B:** Simulate a hmac communication between two users (use a json file to store the message+digest) **Lab6C:** Random number generation using the modules random, randint, uniform, sample, shuffle, os.urandom and secrets
7. Digital Signatures and Certificates **7.1.** Digital Signature Generation and Verification scheme **7.2.** RSA Digital Signature Approach **7.3.** NIST DSA digital signature **7.4.** Public Key distribution approaches **7.5.** X.509 Format certificates **7.6.** PKI	**2**	**2**	**12**	**3, 5, 6,7**	**1, 3, 6, 7**	Class Demonstration Hands on Exercise Discussion	**Lab8A:** Openssl : - decode a digital certificate with openssl. the certificate can be loaded from a secure web site using python or openssl **Lab8B:** use “rsa” module to sign/verify a message.
8. Key Management of Symmetric Encryption **8.1.** Diffie-Hellman Key Exchange **8.2.** KDC	**2**	**2**	**13**	**5, 6,7**	**1, 3, 6, 7**	Class Demonstration Hands on Exercise Discussion	**Lab9A:** Use Diffie-Hellman to share a secret key and use it in a symmetric encryption/decryption algorithm **Lab9B:** implement a simple PKI and use it.

9. Image Cryptography and Steganography **9.1.** Image representation **9.2.** Image Cryptography **9.3.** Data hiding and Steganography	**2**	**2**	**14**	**3, 6,7**	**1, 2, 3, 4, 6, 7, 8**	Class Demonstration Hands on Exercise Discussion	**Lab7A:** Use "Fernet" to implement image encryption **Lab7B:** use "cryptosteganography" to hide a text file into an image. **Lab7C:** use “cryptosteganography" to hide an mp3 file into an image.
Course Review and Project Presentation					**1, 2, 3, 4, 5 6, 7, 8**		**Project Presentation**

Sources	
Text Book	- Text1: Full Stack Python Security : Cryptography, TLS, and attack resistance. Dennis Byrne. Manning Publications Co. ISBN: 9781617298820. 2021 - Text2: Implementing Cryptography Using Python. Shannon W. Bray. John Wiley & Sons, Inc. 2020. ISBN: 978-1-119-61220-9. 2020
Book References	Cryptography and Network Security: Principles and Practice, EBook, Global Edition. William Stallings. 8th edition. ISBN 978-0-13-670722-6. 2023
Web References\ e-library(s)	
Software Requirement	- Ubuntu machine : besides python based labs, there is an intensive use of command-line Linux shell for OpenSSL - Python 3.8 through Anaconda distribution. This is to install the right version of python that is needed for the describe labs and to properly fetch additional modules with appropriate versions. Jupyter Notebook and VS code can be installed through Anaconda Navigator. Alternatively the same packages can be installed and imported through the use of replit.com.
Hardware Requirement	PC with a minimum of 2.6 GHz CPU and 16 GB of RAM memory and 64-bit operating system, x64 based processor.

Assessment Plan

No.	Assessment Activity	Weight %	Learning Outcomes Mapping
1	Practical Exam I	5	1,2,3,4
2	Quiz	10	1,4
3	Midterm	20	1,3,4,6
4	Project	15	1,2,3,4,5,6
5	Practical Exam II	10	1,2,3,4
6	Final	40	1,3,4,5,6
Total		100	

Prepared & Agreed by:

S. No.	Faculty Name	Branch	Signature
1.	**Dr Rhouma Hamed**	**UTAS-CAS Salalah**	
2.	**Mr Geogen George**	**UTAS-IBRI**	
3.	**Dr Narayanasamy Rajendran**		

4.	**Dr. Bharaguram Thayyil**	**UTAS Shinas**	
5.	**Dr Steven Vinil Kumar**	**UTAS - Salalah**	
6.	**Dr. Said Al Riyami**	**UTAS - Muscat**	
7.	**Dr. Raphael Joseph Akkara**		
8.	**Mr. Burhanuddin Mohammad**	**UTAS - Al Musanna**	**BM**
Date of Submission:	**12 February**		

Approved by:			
Designation	Name	Date	Signature

IT Department Academic Calendar

Year: 2022/2023, Spring Semester

Week No.	SUN	MON	TUE	WED	THU	1st	2nd	Remarks
						Class	Class	
1	12-Feb	13-Feb	14-Feb	15-Feb	16-Feb	Orientation		**12-Feb**: Start of Teaching

2	19-Feb	20-Feb	21-Feb	22-Feb	23-Feb			**19-Feb**: Israa wal Mi’raj
3	26-Feb	27-Feb	28-Feb	1- Mar	2- Mar			**Quiz**
4	5- Mar	6- Mar	7- Mar	8- Mar	9- Mar			
5	12- Mar	13- Mar	14- Mar	15- Mar	16- Mar			
6	19- Mar	20- Mar	21- Mar	22- Mar	23- Mar			**23-Mar:** Expected Start of Ramadan
7	**26-Mar**	27- Mar	28- Mar	29- Mar	30- Mar			**26-Mar:** Start of Mid Exams
8	2-Apr	3-Apr	4-Apr	5-Apr	**6-Apr**			**6-Apr**: Last Day of Course Withdrawal
9	9-Apr	10-Apr	11-Apr	12-Apr	13-Apr			**Practical Exam 1**
10	16-Apr	17-Apr	18-Apr	19-Apr	20-Apr			**20 Apr-24 Apr:** Expected Eid Al-Fitr Holiday
11	23-Apr	24-Apr	25-Apr	26-Apr	27-Apr			
12	30-Apr	1-May	2-May	3-May	4-May			**Practical Exam 2**
13	7-May	8-May	9-May	10-May	11-May			
14	14-May	15-May	16-May	17-May	18-May			
15	21-May	22-May	23-May	24-May	25-May			**25-May:** Last Day of Teaching & Announcement of Total Internal Marks
16	**28-May**	29-May	30-May	31-May	1-Jun			**28-May**: Start of Final Exams
17	4-Jun	5-Jun	6-Jun	7-Jun	8-Jun			

18	11-Jun	12-Jun	13-Jun	14-Jun	**15-Jun**			**15-Jun**: End of Final Exams

GRADING SCHEME

Intakes before September 2022

New Intakes from September 2022 onwards

Grade Points	Range as Percentages	Grade	
4.00	95 100 –	A (أ)	إمتياز Excellent
3.7	90 94 –	A-(-أ)	
3.3	85 89 –	B+ (+ب)	جيد جدا Very good
3.0	80 84 –	B (ب)	
2.7	75 79 –	B-(- ب)	
2.3	70 74 –	C+ (+ ج)	جيد Good
2.0	65 69–	C (ج)	
1.7	60 64 –	C- (- ج)	
1.3	55 59 –	D+ (+ د)	مقبول Fair
1.0	54-50	D (د)	
0.0	أقل من50	F (هـ)	راسب Unsatisfactory
0.0		FW (هـ غ)	راسب بسبب الغياب Fail due to absence

Point	Grade	Range
4.0	A	100-90
3.7	A-	89-85
3.3	B+	84-80
3.0	B	79-76
2.7	B-	75-73
2.3	C+	72-70
2.0	C	69-67

1.7	C-	66-60
1.0	D	59-55
0.0	F	54-00

- *Refer to Academic bylaw*

STUDENT ATTENDANCE POLICY (*For Intakes before September 2022*)

Source: PL 70401 STUDENT ATTENDANCE POLICY
https://survey.hct.edu.om/pms/staff/activities/staffpolicy/50

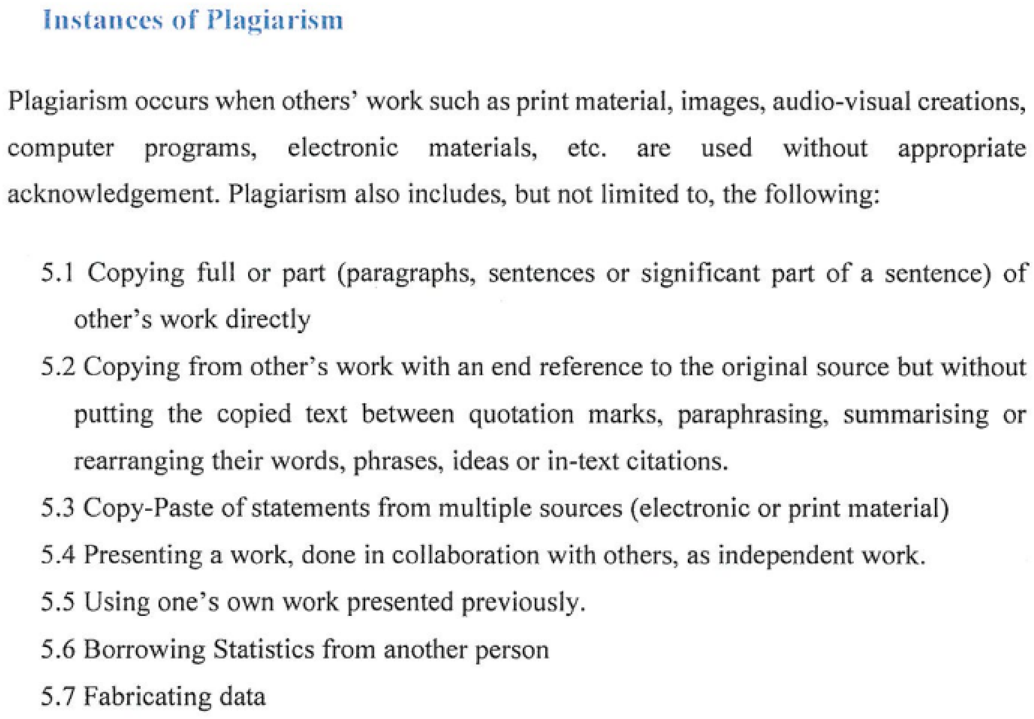
1. Student attendance in all classes is mandatory, and more than 30% of absence in classes shall lead to debarment of the students from writing the final examination of the course(s) the student missed the classes.
2. Students will be marked absent for a class after ten minutes of its commencement.
3. Student should be present in class before the commencement of the class. Students coming to class within 10 minutes from the start of the class shall be marked as 'late', and three late classes shall amount to one class of absence.
4. Students shall be issued a notice of first, second and debarment for 10%, 20% and 30% absence of total class hours in the semester respectively.
5. Students will be considered 'no-Show' if they are found absent from classes for more than 10 consecutive working days. Students who are reported no-show shall be suspended until they present themselves with a reason deemed acceptable, and consequently, their allowances shall be stopped. Students are not permitted to go to class without getting their status reactivated by the registration department.
6. Students who are absent due to medical reasons must provide 'sick leave certificate' attested by a government health center if obtained from a private hospital or clinic when they come back after their absence.
7. Medical certificates are considered as valid excuse for absence in classes or assessments. Students absent for assessments like quizzes, mid-semester and final examinations with a valid excuse are allowed to write the make-up assessment - continuous or final.
8. Student requests for leave of long absence on medical grounds, or allowing them to sit for the final examination will be subject to the approval of the College Council. Students should produce 'medical fitness certificate' when they return after the long leave for continuing the studies.

- *Refer to Academic bylaw*

ACADEMIC INTEGRITY AND HONESTY POLICY (*For Intakes before September 2022*)

Source: ACADEMIC INTEGRITY AND HONESTY POLICY V2.2
https://survey.hct.edu.om/pms/img/policypdf/ACADEMIC_INTEGRITY_AND_HONESTY_POLICY.PDF

Allowed Turnitin Similarity Index: 25%



Instances of Plagiarism

Plagiarism occurs when others' work such as print material, images, audio-visual creations, computer programs, electronic materials, etc. are used without appropriate acknowledgement. Plagiarism also includes, but not limited to, the following:

5.1 Copying full or part (paragraphs, sentences or significant part of a sentence) of other's work directly

5.2 Copying from other's work with an end reference to the original source but without putting the copied text between quotation marks, paraphrasing, summarising or rearranging their words, phrases, ideas or in-text citations.

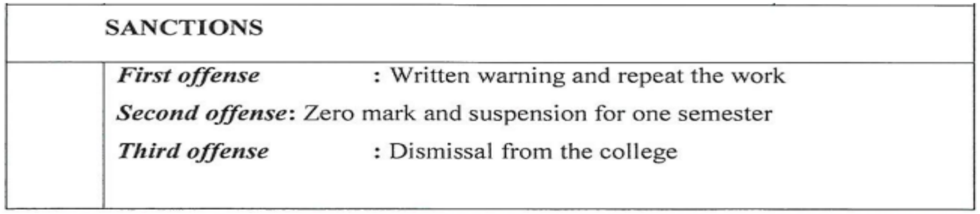
5.3 Copy-Paste of statements from multiple sources (electronic or print material)

5.4 Presenting a work, done in collaboration with others, as independent work.

5.5 Using one's own work presented previously.

5.6 Borrowing Statistics from another person

5.7 Fabricating data



SANCTIONS

First offense : Written warning and repeat the work

Second offense: Zero mark and suspension for one semester

Third offense : Dismissal from the college

Refer to Academic bylaw