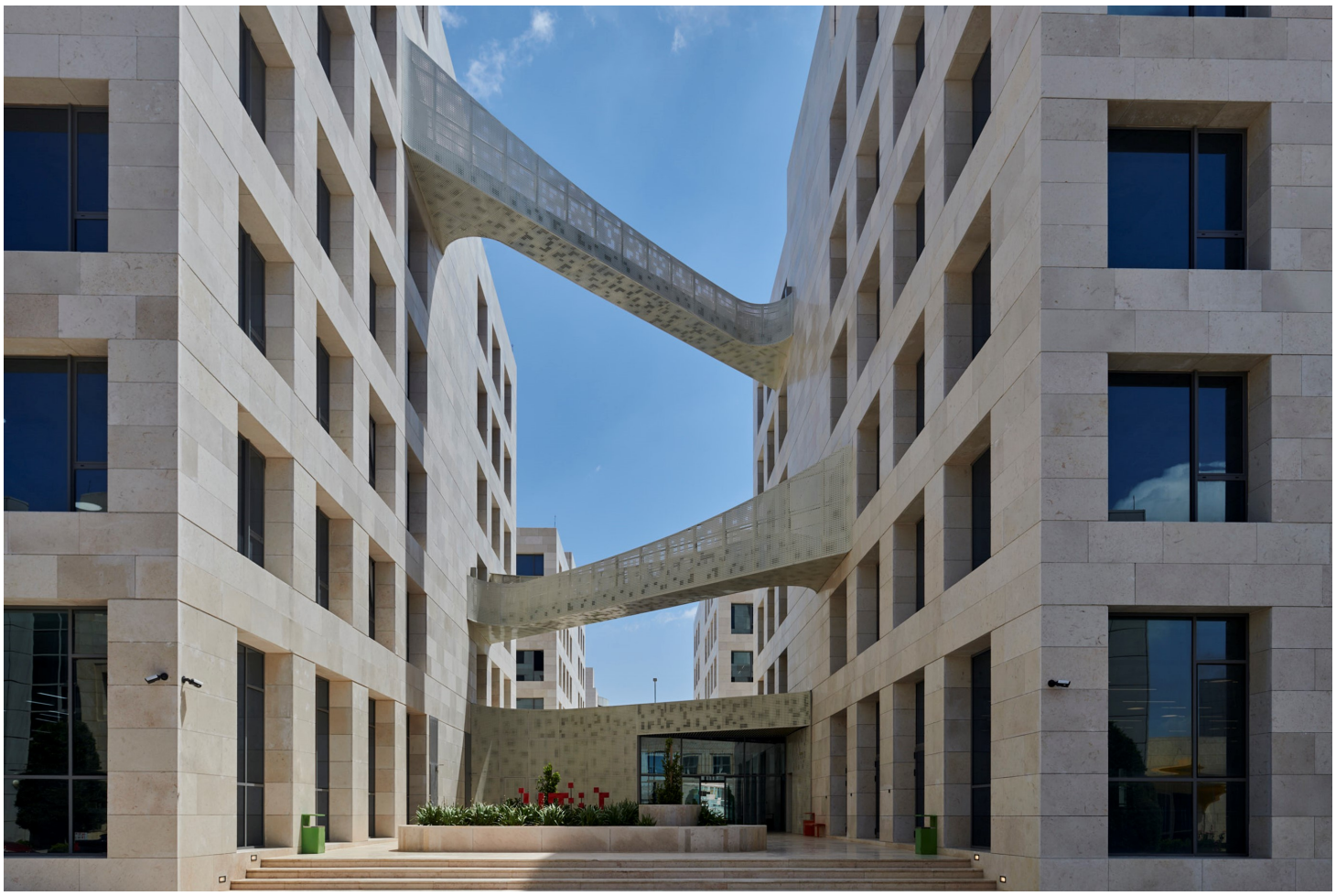
جامعة الحسين التقنية
Al Hussein Technical University

ASSIGNMENT BRIEF

HTU Course No: 10203340	**HTU Course Name:** Cryptography
BTEC Unit Code:	**BTEC UNIT Name:**

Version: 3



Student Name/ID Number/Section	
HTU Course Number and Title	10203340 Cryptography
BTEC Unit Code and Title	
Academic Year	2023-2024 Spring
Assignment Author	Eyad Taqieddin
Course Tutor	Eyad Taqieddin - Raed Bani-Hani
Assignment Title	Applied Cryptography
Assignment Ref No	1
Issue Date	18/04/2024
Formative Assessment dates	From 02/05/2024 to 30/05/2024
Submission Date	14/06/2024
IV Name & Date	Fawaz Khasawneh 17/04/2024

Submission Format

Each student is expected to individually submit his/her work including:

- An individual written report in Word format covering the required details in the (Assignment Brief and Guidance) section.
- A signed Student Assessment Submission and Declaration form (Must be given in a separate file).
- Evidence of the implemented work (softcopy). Students should submit their original source code.
- An oral discussion about the report and the implemented work. Instructions, date, and time for the discussion will be provided later. A witness statement or observation record is considered as evidence for this part.
- An in-class written exam. Instructions, date, and time for the exam will be provided later.

PS: Files should be uploaded separately rather than in a zipped file.

Report guidelines:

The report should be written in a concise, formal business style using single spacing and font size 12 with use of headings, paragraphs and subsections as appropriate (Cover page, table of contents, and an introduction to provide an overview of your report.). The expected word limit is about 3000 words, although you will not be penalised for exceeding the total word limit. The report must be supported with research and referenced using the Harvard referencing system.

Note: Soft copies submissions should be done through the university's eLearning system (https://elearning.htu.edu.jo) by the deadline assigned above.

Unit Learning Outcomes

LO1 Examine the symmetric encryption ciphers and algorithms.

LO2 Assess public key encryption protocols and digital signatures.

LO3 Analyse the security issues related to symmetric and asymmetric ciphers.

LO4 Demonstrate the use of cryptographic tools.

Assignment Brief and Guidance

As an employee at Crypto-Crack, you are responsible of handling cases that involve encrypted, digitally signed, or hashed files. For some cases, you have access to the encryption keys, while in others you need to do some cryptanalytic work (mainly brute force).

Part 1: Cryptanalysis of a double-encryption cipher:

Your company is investigating a case where a person of interest is exchanging encrypted data with another party. You were able to identify that he/she is using the Simple-DES (sDES) cipher. Also, traffic traces indicate that the files being exchanged are encrypted using double encryption (2-sDES). Based on the samples from the encrypted files, your job is to find the encryption keys. You need to use the Meet-in-the-Middle technique.

(Note: The traces are given in a file called traces.txt). A description of sDES will be provided through e-learning and you are responsible of writing its corresponding code.

Deliverable: Part 1 of the report must cover the following details:

1) The detailed step-by-step procedure to find the keys.
2) The values of the keys K_1 and K_2.
3) Your code/scripts (in text format).
4) Screenshots of the result of running the codes.

Part 2: Encryption using ECB and CBC modes:

Your company was chosen to build a simple encryption tool for image encryption. Your team leader has suggested to use either ECB or CBC modes. Given your expertise in cryptography, he asked you to run a test case, in which you will encrypt the original image using ECB mode and then repeat the same by encrypting the original image using CBC. Based on the output images, you need to justify the decision for which mode is better suited for the task. *(Note: The test image is given in a file called test_image.jpg).* Feel free to use to use whatever symmetric cipher you find suitable.

Deliverable: Part 2 of the report must cover the following details:

1) The detailed step-by-step you followed in your test.
2) An explanation of why you found a specific mode more suitable.
3) Include both output images with proper captions.
4) Your code/scripts (in text format)

Part 3: Message Exchange System:

Crypto-Crack is also responsible of building a Message Exchange System. The system should support the following functionalities:

1) Key exchange capability based on public/private keys.
2) A symmetric encryption function (you're free to choose the cipher, but it must be justified).
3) A digital signature for both integrity and authentication.

Deliverable: Part 3 of the report must cover the following details:

1) A solid case to support the CIA pillars being achieved in the system.
2) A detailed diagram showing how:
    a. The keys are exchanged between the sender and receiver.
    b. The message(s) are signed.
    c. The message(s) are encrypted.
    d. The operations are done at the receiver side.
3) Your code/scripts (in text format).
4) A critical evaluation of the Message Exchange System along with suggestions for enhancement.

You will be given a test file to show the proper operation of your code (during the oral discussion).

Part 4: Research

Your manager has asked you to investigate the following points:

1) Evaluate the improvement introduced by AES compared to DES and 3DES encryption standards.
2) The use of symmetric vs asymmetric cryptography. Give advantages and disadvantages and explain whether any of them is superior to the other.
3) Research security flaws in symmetric ciphers used in Transport Layer Security.

Deliverable: Part 4 of the report must cover the three points above.

Part 5: In-class Exam

The in-class written exam will cover all the material taught during the course, with particular emphasis on the following topics:

1. Examine mathematic algorithms and their use in cryptography.
2. Explain the operation of stream ciphers and block ciphers.
3. Compare the operational differences between stream cipher and block cipher.
4. Examine common public key cryptographic methods and their uses.
5. Explain public key exchange and digital signatures.
6. Analyse the difference between digital signatures and hash values.
7. Explain the common attacks on an asymmetric key encryption scheme.

Learning Outcomes and Assessment Criteria			
Learning Outcome	**Pass**	**Merit**	**Distinction**
LO1 Examine the symmetric encryption ciphers and algorithms.	**P1** Examine mathematical algorithms and their use in cryptography. **P2** Explain the operation of stream ciphers and block ciphers.	**M1** Compare the operational differences between stream ciphers and block ciphers. **M2** Compare between encryption modes.	**D1** Evaluate the improvement introduced by AES compared to DES and 3DES encryption standards.
LO2 Assess public key encryption protocols and digital signatures.	**P3** Examine common public key cryptographic methods and their uses. **P4** Explain public key exchange and digital signatures.	**M3** Analyse the difference between digital signatures and hash values.	**D2** Evaluate the difference between symmetric and asymmetric ciphers from a practical point of view.
LO3 Analyse the security issues related to symmetric and asymmetric ciphers.	**P5** Discuss the common attacks on a symmetric key encryption scheme. **P6** Explain the common attacks on an asymmetric key encryption scheme.	**M4** Research security flaws in symmetric ciphers used in Transport Layer Security.	
LO4 Demonstrate the use of cryptographic tools.	**P7** Produce code that implements mathematical ciphers and algorithms to encrypt and decrypt data. **P8** Illustrate the use of encryption modes with media files.	**M5** Implement a system for secure message exchange guaranteeing privacy, integrity, and authentication.	**D3** Critically evaluate the message exchange system and provide suggestion for future enhancements.