Module Title: Security Fundamentals and Development (H7SFD)

Programme: BSHC3A

Assignment Type: Open book, Working in Groups

Deadline submission: **Wed 15/11/23 @11pm (W9)**

Weighting: The project will be marked out of 100. **This CA is worth 50% of the total marks for this module.**

Turnitin: All report submissions will be electronically screened for evidence of academic misconduct (i.e., plagiarism and collusion).

Learning Outcomes Assessed:

#	Learning Outcome Description
LO1	Identify a range of security threats and examine technologies, regulations, standards, and practices to protect individuals and organisations from cyber-attacks.
LO2	Identify threats and formulate responses to mitigate risk through the application of appropriate tools and technologies.
LO4	Demonstrate an in-depth knowledge of cryptographic mechanisms and the ability of applying these mechanisms to the achievement of security services.

CA1 BRIEF

You are a group of security software developers responsible for designing and developing software systems that are resilient against cyber threats and vulnerabilities. In this CA, your group will select a specific use case scenario for cryptography from Table 1. Your CA involves utilizing your knowledge in coding and encryption to build a robust cryptography software solution. You will also investigate a recent threat/high-profile cyber-attack and prepare a presentation. Each group is limited to 5 people.

Components of the CA

The CA consists of the following components:

1) **Slides** of group presentation about threats/high-profile cyber-attacks (in **Powerpoint/PDF**). The first slide must list the names and student IDs of the group members who contributed to the work. The **filename must include the GroupID**.
2) **Report** for the Cryptography Programming Group Project (in **PDF**). Make sure to acknowledge any original sources of your investigation as appropriate, including the use of AI. You need to **include the cover page** providing this is applicable. The **filename must include the GroupID.**
3) **Source code** for Cryptography Programming Group Project (GitHub link included in the report template).
4) **Demo video** for Cryptography Programming Group Project (YouTube link included in the report template).

Note: Only one member of the group will submit all the artifacts to Moodle.

Group Presentation (20 marks)

1) Check your group number from your Moodle page. Each student has chosen or been allocated a group.
2) Each group must select a topic related to threats/high-profile cybersecurity attacks from the excel sheet provided or propose a new one (needs approval from the lecturer) for their presentation.
3) The group will investigate the topic and prepare a set of slides, following the guidelines provided.
4) The group will present their topic and participate in Q&A during their corresponding lab slot.
5) Marks for group presentation will be awarded based on presenting the slides at your allocated slot, handling Q&As, and submitting the slides by the given deadline at the specified location. The quality of the content presented, presentation skills, and time management will also be considered.

Group Programming Project (80 marks)

Each group will implement an application applying concepts of cryptography. A list of potential project descriptions is available in Table 1. You can choose to start your project from scratch or extend an existing project that you have already worked on (if you do so, your report must include details of the original source and clearly indicate the novel parts or contributions to this particular project).
Please note the following guidelines for the code implementation:

- Use Java or Python as the programming language.
- Comment your code as appropriate (e.g., providing explanatory information about a function of the code).
- The application should compile & run, offer the main functionality chosen from Table 1, and offer a clear interface to enter the inputs and see the outputs.
- Deliverables for this part:

1. A report: Using the template provided on Moodle, explain the main functionality provided by the application, the algorithms and technical details utilized in the implementation, instructions to download, run and test your application, and illustrate the application's operating process with a flowchart. You must also indicate the contribution of each member of the group **(20 marks)**
2. Source Code: upload your code to Github and include the link in your Report. **(50 marks)**
3. A 5-minute video demonstrating how the application works and a quick walkthrough of the code. Include the link to the video in your report. **(10 marks)**

Table 1 Use Case Scenarios for Cryptography

No.	Use Case Scenario for Cryptography
1	**Secure Instant Messaging App**: Create an application that encrypts messages for secure communication between users.
2	**Secure Email Client**: Develop an email client that uses end-to-end encryption to protect email content.
3	**Secure Voice Calls**: Design a VoIP application that encrypts voice calls to prevent eavesdropping.
4	**Secure Video Conferencing:** Create a video conferencing platform with end-to-end encryption to safeguard video and audio data.
5	**Secure Online Voting System:** Build an online voting system that ensures the confidentiality and integrity of votes through cryptography.
6	**Secure Cloud Storage:** Develop a cloud storage service where files are encrypted before uploading, and only the owner can decrypt them.
7	**Secure Healthcare Records:** Create a system for secure storage and sharing of health records using cryptographic techniques.
8	**Secure Supply Chain Tracking:** Implement a system for supply chain tracking with cryptographic hashing to verify product authenticity.
9	**Secure Document Signing:** Implement a digital signature system (like a document signing platform) that uses digital signatures (using hash functions) to verify the authenticity and integrity of electronic documents or messages.
10	**Secure Digital Identity:** Create a system for secure management and verification of digital identities using cryptography.
11	**Secure E-commerce Transactions:** Build an e-commerce platform with end-to-end encryption for payment transactions.
12	**Secure Exchange of Images:** Create an application that encrypts images to share them in a secure way between 2 parties.

13	**Historical Encryption Schemes:** Create an application that encrypts and decrypts text messages with historical encryption algorithms such as Caesar Cipher, Vigenère Cipher, Rail Fence cipher, etc.
14	**Password Manager:** Create an application that stores users' passwords safely that supports authentication by securely hashing and verifying user passwords to protect user accounts.
15	**File Integrity Verification:** Develop a tool to calculate and verify the hash values of files, ensuring their integrity during transfer or storage
16	**Data Deduplication:** Build a system that uses hashing to identify and eliminate duplicate data, thus optimizing storage resources.
17	**Anti-Virus Scanning:** Build an antivirus program that uses hash values to detect known malware by comparing file hashes with a database of known malicious hashes.
18	**Secure Data Backup:** Design a secure data backup service that encrypts data before storing it in the cloud.
19	**Content-Based File Retrieval:** Design a content-based file retrieval system that uses hashes to index and locate files based on their content
20	**Caching and Data Lookup:** Implement a caching system for a web application that uses hash-based data structures (e.g., hash tables) to optimize data retrieval and storage.

Assessment Criteria and Grading Rubric

Group Presentation

0-39 (Fail)	The presentation lacks structure and coherence. Visual aids (slides, visuals) are either missing or poorly designed. The presentation is difficult to follow or understand. Poor communication skills, such as speaking too fast or too softly. The investigation is incomplete or lacks depth. There is a significant lack of relevant information.
40-49 (Marginal)	The presentation has some structure but lacks clarity. Visual aids are present but may not effectively enhance the presentation. The presentation is somewhat difficult to follow or understand. Communication skills could be improved. The investigation is somewhat complete but lacks depth. Relevant information is missing or insufficient.
50-59 (Adequate)	The presentation is organized but may need improvement in terms of flow. Visual aids are included and reasonably supportive of the content. The presentation is generally clear and understandable. Communication skills are decent but could be more engaging. The investigation is reasonably complete and somewhat in-depth. Most relevant information is included.
60-69 (Good)	The presentation is well-structured and coherent. Visual aids effectively support the content and enhance understanding. The presentation is clear, engaging, and easy to follow. Communication skills are good and engage the audience. The investigation is thorough and detailed. All relevant information is included.
70+ (Excellent)	The presentation is exceptionally well-structured. Visual aids are outstanding, enhancing content comprehension and engagement. The presentation is exceptionally clear, engaging, and highly informative. Exceptional communication skills, such as a strong presence and audience engagement. The investigation is exceptionally thorough, comprehensive, and highly detailed. All relevant information is not only included but also exceptionally well-researched.

Group Programming Project

0-39 (Fail)	The source code is incomplete, non-functional, or severely flawed. Cryptographic algorithms are incorrectly implemented or not used. Code is poorly organized and lacks documentation. The report is missing essential sections. Technical details are missing or incorrect. The flowchart is missing or not related to the application. The report contains multiple grammatical or spelling errors.

	The demo video is missing or provides no meaningful information. The video lacks clarity and coherence. Key aspects of the application are not demonstrated.
40-49 (Marginal)	The source code is somewhat functional but contains errors or omissions. Cryptographic algorithms are partially implemented with some issues. Code organization and documentation need improvement. The report includes most essential sections but lacks detail. Technical details are somewhat accurate but incomplete. The flowchart is present but lacks clarity or detail. Some grammatical or spelling errors are present in the report. The demo video provides some information but lacks clarity. Key aspects of the application are demonstrated but with gaps or issues.
50-59 (Adequate)	The source code is functional but may contain some minor errors. Cryptographic algorithms are correctly implemented but could be more efficient. Code organization and documentation are reasonable. The report covers all essential sections with adequate detail. Technical details are accurate but may lack depth. The flowchart is clear but could provide more detail. Minor grammatical or spelling errors are present in the report. The demo video provides a reasonable demonstration of key aspects of the application. Clarity and coherence are improved, but there may be some gaps or minor issues.
60-69 (Good)	The source code is functional and well-structured. Cryptographic algorithms are correctly implemented. Code organization and documentation are well-done. The report is comprehensive and well-detailed in all sections. Technical details are accurate and sufficiently explained. The flowchart is clear and illustrative. Minor grammatical or spelling errors are present in the report. The demo video provides a clear and coherent demonstration of all key aspects. Clarity, coherence, and coverage are good, with minimal gaps or issues.
70+ (Excellent)	The source code is exceptional in functionality and structure. Cryptographic algorithms are expertly implemented. Code organization and documentation are exemplary. The report is outstanding, covering all aspects in-depth and with clarity. Technical details are excellently explained. The flowchart is excellent in clarity and detail. The report is free from grammatical or spelling errors. The demo video is exceptional in clarity, coherence, and coverage. It provides an outstanding demonstration of all key aspects. There are no gaps or issues in the video.