A formatted version of the brief.

Beans

The project involves developing a cryptography-based software solution. These use cases may cover various applications of cryptography, such as secure messaging, secure file storage, and digital signatures. Groups are required to implement cryptographic mechanisms (e.g., encryption, decryption, hashing) and demonstrate the functionality of their application.

The deliverables for this component include: A detailed project report outlining the purpose, design, and technical implementation of the software. The report must also include a description of the cryptographic algorithms used and each group member’s contribution. A GitHub link to the project’s source code. A 5-minute demo video showing the functionality of the application and a walkthrough of the code. This programming project is worth 80 marks.

Submissions required for CA:

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.

Source code for Cryptography Programming Group Project (GitHub link included in the report template).

Demo video for Cryptography Programming Group Project (YouTube link included in the report template).

Please note the following guidelines for the code implementation:

You can use any programming language of your choosing, preferably Java or Python.

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.

Each member of the group should be responsible for at least one use case or a distinct feature of the application and its security. This ensures that each member contributes meaningfully to the overall project (The chosen use case should be significant enough that the member’s contribution is clear and measurable).

Deliverables for this part:

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)

Source Code: upload your code to Github and include the link in your Report. (50 marks)

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)

File Integrity Verification: Develop a tool to calculate and verify the hash values of files, ensuring their integrity during transfer or storage.

What is the architecture of a project such as this?