Module Title:	Computer Systems Security 2025
Module Code:	B9IS103
Module Lecturer:	Paul Laird
Assessment Title:	Secure Communications/Collaboration System Design and Deployment Analysis of Secure System Deployment
Assessment Number (if relevant):	1
Assessment Type:	Practical (lab-based)
Restrictions on Time/Length:	N/A
Individual/Group:	Group
Assessment Weighting:	50%
Planned Feedback/Results Release Date:	Within four weeks of submission
Mode of Submission:	On-line **ONLY Moodle**

The assignment is a group assignment.

Requirements: You are required to submit an application and accompanying report, which may be written in Python or any other suitable programming language. Please comment code and use appropriate variable names. Please make use of a publicly hosted git repository (e.g. GitHub)

Submission: Zip the Solution and Project folder and upload using the CA_ONE link on Moodle. Include links to your code repository and deployment location in the online text section.

IMPORTANT NOTE: Only one submission is allowed so please ensure that you have everything that is required in the zip before uploading to Moodle.

The following table illustrates the percentage allocation for each individual part of the assignment.

Total Marks (100)

Problem	**Detail**	**Breakdown of Marks**
Design and Implementation	Design specification plus Python or other Code	40 marks
Presentation	Presentation of your solution	30 marks
Vulnerability Report	Analysis of potential vectors of attack on another system	30 marks

The task:
Design and deploy to the cloud an encrypted communications/collaboration application, which must, at a minimum, allow for messages to be encrypted between two parties who have not met to exchange keys.
You can use a self-hosted server as a relay, or you can integrate into a social medium or email fro communications.

Some form of authentication of the identity of the participants should be used, in line with the form of identity selected. Examples include, but are not limited to:

- PKI/DNS based identity, with keying information posted on https sites with valid certificates
- Social media based identity, with x (twitter) / facebook / other channels / profiles being used to certify identity
- Communications channel based identity, e.g. email and/or SMS
- Idiosyncratic identity verification (could include authenticated media transmission during setup phase, or novel ideas)
- Combinations of the above

You must outline the requirements of the system, including functional and nonfunctional requirements, and specifically detail the security requirements.

The system must not rely upon any secret algorithm or security through obscurity, although you may use (only as an additional layer) steganography for plausible deniability. Your system must be documented in sufficient detail so as to allow another developer to efficiently augment your work.

Every system has weaknesses, and can at very least be attacked on the basis of the assumptions upon which it relies. You will be assigned another group's project to analyse, and must describe how you would propose to attack the system if you were attempting to intercept relevant communications, and also describe any other potential vectors of attack or weakness.

Resources

Software or tools required/ useful: Azure, GitHub.dev, GitHub spaces
Templates, files, data tables provided by the lecturer: Moodle and GitHub resources

Generative Artificial Intelligence Assessment Scale

Can generative AI be utilised in this assignment?

1	2	3	4	5
NO AI	**AI-ASSISTED IDEA GENERATION AND STRUCTURING**	**AI-ASSISTED EDITING**	**AI TASK COMPLETION, HUMAN EVALUATION**	**FULL AI**
The assessment is completed entirely without AI assistance. This level ensures that students rely solely on their knowledge, understanding, and skills. **AI must not be used at any point during the assessment.**	AI can be used in the assessment for brainstorming, creating structures, and generating ideas for improving work. **No AI content is allowed in the final submission.**	AI can be used to make improvements to the clarity or quality of student created work to improve the final output, but no new content can be created using AI. **AI can be used, but your original work with no AI content must be provided in an appendix.**	AI is used to complete certain elements of the task, with students providing discussion or commentary on the AI-generated content. This level requires critical engagement with AI generated content and evaluating its output. **You will use AI to complete specified tasks in your assessment. Any AI created content must be cited.**	AI should be used as a 'co-pilot' in order to meet the requirements of the assessment, allowing for a collaborative approach with AI and enhancing creativity. **You may use AI throughout your assessment to support your own work and do not have to specify which content is AI generated**
			The use of AI-generated content is treated in the same manner as the use of any other external resource such as libraries, packages or frameworks. It must be clearly identified and attributed, and credit will be limited to the student's own work, to the exclusion of such resources, except for how students integrate and deploy all of these resources. Questions will be asked during the presentation.	