I am planning to design and implement subpart of Secure Emailing System (SES). In SES: generating key-pairs and uploading public-keys to server, secure distribution of the users’ public-keys and encrypted/signed message interchanging between parties are included. I want to complete secure message interchanging between parties (End Entities) in this course. I am presuming that all the public keys are distributed to everyone related and the private keys to owner of which only. So, my responsibility related to this course is just to provide security nothing else. I mean encrypting/decrypting and signing the message by security. Providing the compatible Graphical User Interface (GUI) for sending, receiving, editing, encrypting, decrypting and signing will also be under responsibility.

The architecture of SES is given below. The system has 3 main points that are software to be implemented. Management Entity (ME), End Entities (EE) and the Connection Protocols (CP) between them. ME is a server side that keeps the public keys of all EE’s which are registered to Management System (MS) before. EE is a user of SES and he/she will contact with ME to set his/her public key to ME and also to get target recipient’s public key from the ME. The CP is in one name of several ME-EE connection protocols. Some of the CP’s are Initialization and Public Key Settlement Protocol (InitKeySet), Public Key Obtainment Protocol (KeyObt) and Public Key Removal Protocol (KeyRem) etc...