1. The goal of project classes and the rules

The main goal of the project is to realize a software tool for sending files and messages in unsecure environment. Before the transmission process, the session key must be generated and securely transmitted to the other user.

The project is marked regarding the rules:

- Correct realization of the project before the deadline – 14 points.
- Technical report – 20 points.
- Presentation the project/concept (in a form of report) of the application and partially working application (in a given control term) – 5 points.

2. Project tasks

The main task of the project is to design and program an application to cipher text messages (e.g. like a text box) and data files and then send them by using the unsecure Ethernet network. In general, the application must take a form of a *network secure communicational tool*. The application must allow sending and receiving the ciphered data and messages on both sides of communication. It means that user **A** have the application, and so does the user **B**. Before the transmission user **A** and **B** must exchange their public keys (RSA algorithm for key generation, other algorithm for secure exchange of the keys). The pair of RSA keys will be used for a secure session key exchange – session key is used to cipher the text/data.

It can be assumed that user **A** generates session key for data encryption and securely send it to the user **B** by ciphering it by using the RSA public key. User **B** uses his private key to decrypt the session key and further encrypt/decrypt the transferred data.

During project realization the application must be executed as “two independent instances”. The communication between them (simulation of user A and B) must be realized by using the network sockets. In the Fig. 2.1 a sample block diagram of the data flow between the applications was presented.

Requirements:

- The GUI interface must allow to type and send a text message to the other user. Besides the text also an ability of sending any tipical files (e.g. *.txt, *.png, *.pdf,