*.avi), with any size (e.g. 1kB - small file, and also 500 MB – large file) must be implemented.

- The AES block cipher should be used to cipher the data.
- It is obligatory to use two modes of operation of the block ciphers (ECB, CBC), it will be selected by the user in the GUI.
- It is obligatory to implement status icons and a progress bar to present the current connection status and presenting the progress of sending the large files.
- For large files a method of data division must be implemented before sending them via the Ethernet interface.
- A UDP (*User Datagram Protocol*) or TCP (*Transmission Control Protocol*) communication protocol must be used to send the data between the applications.
- When the UDP protocol was used a data loss exception must be handled.
- A pseudorandom generator must be used to generate the session key.
- The session key must be encrypted by using the RSA public key of the receiving person and then send to the receiving person.
- The public and private keys must be stored separately (e.g. in a different directories). The RSA private keys must be encrypted by using the AES block cipher operating in the CBC mode. The encryption key (named as *local key*) is the hash (generated by using the SHA function) of the user-friendly password. In other words, user must type the password to access the application.
- It is allowed to use the available implementations of the AES, RSA, SHA algorithms.
- In the report the results of performed tests must be included (e.g. example transfers of different files, time of data transfer, usage scenarios).
- In the report the code of the application must be included (as a *.zip archive).
- The operation of the application must be presented in a form of a movie.

Notes:

- During realization of the project, it is obligatory to generate the following keys:
  - session key (used for data encryption),
  - private and public RSA keys of the users (used for secure transmission of the session keys),