- local key for securing the RSA keys during storage on the hard disk.

- The proposed communication protocol (using the UDP/TCP-IP) must allow the transmission of the encrypted session key (using the RSA algorithm) besides the transmission of the encrypted data.
- It must be remembered that also the parameters of the cipher (algorithm type, key size, block size, cipher mode, initial vector) must be send (in a secure way) to the 2nd user to allow the correct reception of the encrypted data.

3. Project submission

Control date submission:

- Partial report (recommended in the template)
- Code in a *.zip archive.
- Video of partially working application.

Final date submission:

- Final report (recommended in the template)
- Code in a *.zip archive.
- Video presenting the application functionality, according to the "*Evaluation Card*".

The project report must contain a description of the applications' GUI interface, description of communication protocol, description of the secure key distribution method and results of performed tests (e.g. example transfers of different files - with different sizes, time of data transfer, usage scenarios). Additionally, a video file presenting the operation of the application must be provided.

Only one submission date is planned. In a case of obtaining insufficient number of points to obtain a positive mark from the project classes, a 2nd date for submission the project is proposed, but in that case totally 60 % of points can be obtained.