GDAŃSK UNIVERSITY OF TECHNOLOGY

FACULTY OF ELECTRONICS, TELECOMMUNICATIONS AND INFORMATICS

# Bezpieczeństwo Systemów Komputerowych – Projekt
# Security of Computer Systems – Project

## Encrypted Data Transmission With a Session Key Transfer in Unsecure Environment

Version 2.0, Gdańsk, 2023

## 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,

*.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),

    - 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.