**Security of Computer Systems**

**Project Report**

Authors:

Piotr, Kolasiński, 193275

Hubert, Szymczak, 193316

Version: 1.0

**Versions**

|  |  |  |
| --- | --- | --- |
| Version | Date | Description of changes |
| 1.0 | 09.04.2025 | Report for a control term |
| 1.1 | … | … |

1. **Project – control term**
   1. ***Description***

The auxiliary application developed for the control term of the project enables secure generation of RSA key pairs. The application is implemented in Python with a graphical interface built using tkinter.  
The user is prompted to enter a PIN code, which is used to derive a 256-bit AES key via SHA-256 hashing. The private RSA key is then encrypted using the AES-CBC mode and saved to a selected location. The public key is saved separately in PEM format for later use in signature verification.  
The application follows the requirement of generating RSA keys with a length of 4096 bits using a secure pseudorandom generator.

* 1. ***Results***

The application consists of three main components:

* main.py – the entry point of the program
* gui.py – handles GUI creation, PIN input, and calling the key generation
* key\_generator.py – contains logic for generating, serializing, encrypting, and saving RSA keys

Upon clicking the “Generate & Save Keys” button:

* a new RSA key pair is generated,
* the private key is serialized and encrypted using AES-256 (CBC),
* the user selects where to save the encrypted private key and the public key.
  1. ***Summary***

Task 1, the auxiliary application was implemented.

* 1. ***Github repository:***

[***https://github.com/Trebuh01/secure-pdf-signer/tree/main***](https://github.com/Trebuh01/secure-pdf-signer/tree/main)

1. **Project – Final term**
   1. ***Description***

Content

* 1. ***Code Description***

Content

|  |
| --- |
| /\*!  \* A list of events:  \* <ul>  \* <li> mouse events  \* <ol>  \* <li>mouse move event  \* <li>mouse click event<br>  \* More info about the click event.  \* <li>mouse double click event  \* </ol>  \* <li> keyboard events  \* <ol>  \* <li>key down event  \* <li>key up event  \* </ol>  \* </ul>  \* More text here.  \*/ |

*List. 1 – Code listing [2].*

Final Content.

* 1. ***Description***

Content

* 1. ***Results***

Content

* 1. ***Summary***

Content

1. **Literature**

[1] Article.

[2] Online Doxygen documentation, https://www.doxygen.nl/manual/lists.html, (accessed on 01.02.2025).

[3] Book.