**Security of Computer Systems**

**Project Report**

Authors:

Jan Barczewski 188679

Radosław Gajewski 188687

Version: 1.0

**Versions**

|  |  |  |
| --- | --- | --- |
| Version | Date | Description of changes |
| 1.0 | 19.04.2024 | Creation of the document |
| 1.1 | … | … |

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

Całość projektu realizowana jest za pomocą języka python. Do wygenerowania kluczy RSA oraz szyfrowania została wykorzystana biblioteka *cryptography.* Aplikacja okienkowa została zrealizowana za pomocą biblioteki *tkinter*.

Na stan obecny powstała aplikacja konsolowa do generowania pary kluczy RSA. Klucz prywatny jest dodatkowo szyfrowany algorytmem AES za pomocą pinu wprowadzanego ręcznie przez użytkownika oraz zapisywany na odpowiednio nazwanym pendrive. Aplikacja prosi użytkownika o uprzednie odpowiednie nazwanie pendrive’a w celu poprawnego odnalezienia urządzenia.

Rozpoczęliśmy również pracę and drugą aplikacją, w wersji okienkowej. Aplikacja wykrywa już podłączonego pendrive’a z kluczem i za jego pomocą pozwala na podpisanie dokumentu po podaniu poprawnego hasła. Nie zostały jeszcze narzucone ograniczenia, jeśli chodzi o typ dokumentu.

* 1. ***Results***

Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie

*Fig. 1 – Block diagram.*

Działanie rozpoczynamy od wygenerowania pary kluczy RSA za pomocą aplikacji konsolowej. Aby skorzystać z aplikacji, należy wcześniej podłączyć pendrive nazwany „PRIVATE\_KEY”. Aplikacja poprosi użytkownika o wprowadzenie pinu do zaszyfrowania klucza prywatnego a następnie zapisze go na podłączonym urządzeniu.

Druga aplikacja umożliwia wykrycie podłączonego pendrive’a z wygenerowanym kluczem RSA. W celu podpisania dokumentu należy wybrać z eksploratora plików odpowiedni dokument oraz podać poprawne hasło. Po wykonaniu tych czynności aplikacja wygeneruje plik .xml zawierający:

* Informacje ogólne o dokumencie
* Informacje o podpisującym użytkowniku
* Hash dokumentu zaszyfrowany kluczem RSA
* Datę i godzinę podpisu

Poniższe zdjęcia przedstawiają rezultaty dotychczasowej pracy:

Obraz zawierający tekst, oprogramowanie, Czcionka, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Zdjęcie 1: działanie aplikacji generującej parę kluczy RSA

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Opis wygenerowany automatycznie

Zdjęcie 2: Druga aplikacja – nie wykryto pendrive’a

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, System operacyjny

Opis wygenerowany automatycznie

Zdjęcie 3: Druga aplikacja – Podano złe hasło

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Opis wygenerowany automatycznie

Zdjęcie 4: Wygenerowany plik .xml

* 1. ***Summary***

Aplikacja do generowania kluczy RSA została w pełni ukończona.

Druga aplikacja na chwilę obecną zawiera podstawową funkcjonalność podpisywania dokumentów, którą należy udoskonalić (między innymi o wprowadzenie ograniczeń do rozszerzeń plików). Należy również uzupełnić ją o brakujące funkcjonalności (sprawdzanie podpisu, szyfrowanie/deszyfrowanie pliku) oraz udoskonalić interfejs aplikacji.

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 18.02.2024).

[3] Book.