Bezpieczeństwo Systemów Komputerowych

Adam Jakubowski 193352, Hubert Wajda 193511

Spis treści

1. Opis projektu

Głównym celem projektu było opracowanie aplikacji umożliwiającej emulację kwalifikowanego podpisu elektronicznego zgodnego ze standardem PAdES (PDF Advanced Electronic Signature). Na potrzeby projektu stworzyliśmy dwie aplikacje:

- **Aplikacji pomocniczej** – generującej parę kluczy RSA oraz szyfruje klucz prywatny algorytmem AES, przy użyciu kodu PIN pobranego od użytkownika.
- **Aplikacji do podpisywania dokumentów** – realizującej podpisywanie dokumentów PDF oraz weryfikację poprawności podpisu z wykorzystaniem klucza publicznego.

2. Wykorzystane technologie

- **Python** z bibliotekami:
  - `hashlib`, `Crypto`, `cryptography` – do operacji kryptograficznych (generowanie kluczy RSA, szyfrowanie AES).
  - `tkinter` – do stworzenia interfejsu graficznego aplikacji pomocniczej.
- **Electron.js** z bibliotekami:
  - `crypto-js`, `crypto` – do obsługi podpisu cyfrowego, deszyfrowania klucza prywatnego oraz komunikacji z urządzeniami USB.
  - `drivelist` – do automatycznego wykrywania pendrive'a z kluczem.

3. Literatura

- https://nodejs.org/api/crypto.html
- https://www.electronjs.org/docs/latest
- https://dev.to/aaronktberry/generating-encrypted-key-pairs-in-python-69b
- https://ritwik-69146.medium.com/encrypt-and-decrypt-your-data-using-aes-and-rsa-algorithm-e6a19bc1f29c