

Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
НН Фізико-технічний інститут
Дисципліна: “Методи реалізації криптографічних механізмів”

ЛАБОРАТОРНА РОБОТА №4

Виконали:
Студенти групи ФБ-21мн

ЩЕРБАКОВ О.К.
КАЗМІДІ І.Д.

Завдання

1. Розробка реалізацій ІТ-систем (Реалізація Web-сервісу електронного цифрового підпису).

Web-застосунок

PFX: Файл не выбран. PFX password:

File to sign: Файл не выбран.

Signature: Файл не выбран.

File to check: Файл не выбран.

Веб-сторінка підпису для накладання підпису приймає PFX-контейнер з ключами користувача, пароль до контейнеру та файл, що треба підписати. У відповідь користувачу у браузері завантажується відокремлений підпис у вигляді файлу формату .p7s. Для перевірки підпису необхідно обрати файл та підпис у форматі p7s. У випадку неправильно паролю до pfx-контейнера, неспівпадіння підпису або інших помилок - видається відповідне повідомлення.

Check result:

Signing failed

Wrong password to pfx

Check result:

Check failed

ChilkatLib: VerifvP7S: T

Застосунок працює на веб-сервері Django. Криптографічні функції забезпечуються бібліотекою CkPython (Chilkat).

Висновки

Генератор ПВЧ модуля PyCryptoDome має достатній рівень захищеності для використання у криптографічних системах ОС Linux. У критичних криптографічних системах (наприклад у державних установах) рекомендується користуватися апаратними джерелами ентропії для генераторів ПВЧ.