МІНІСТЕРСТВО ОСВІТИ, НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Методи реалізації криптографічних механізмів

Лабораторна робота:

" Вибір та реалізація базових фреймворків та бібліотек"

(Підгрупа 2В)

Підготували:
студенти 5 курсу
групи ФІ-22 (мн)
Толмачов Є.Ю.
Ковальчук О.М.
Коломієць А. Ю.

Київ – 2023

Лабораторна робота №1

Тема: Вибір та реалізація базових фреймворків та бібліотек.

Мета роботи: Вибір базових бібліотек/сервісів для подальшої реалізації криптосистеми.

Завдання на лабораторну роботу

Підгрупа 2B. Порівняння бібліотек OpenSSL, crypto++, CryptoLib, PyCrypto для розробки гібрідної криптосистеми під Linux платформу.

Хід роботи

OpenSSL

OpenSSL – відкрита бібліотека для криптографії що має реалізацію TLS/SSL протоколів. Написана на C. Має базову реалізацію багатьох криптографічних стандартів (ключів, гешувань, сертифікатів, тощо) та має додаткові утиліти. Активно використовується через реалізацію мережевих протоколів. Працює на більшості UNIX-подібних систем, на Microsoft Windows та на деяких сумісних з ними систем.

Існують обгортки для багатьох інших мов програмування. Так, наприклад, в цій лабораторній буде використовуватися PyOpenSSL. PyOpenSSL відома простотою встановлення. Попри це, якщо немає необхідності в використанні TLS протоколів чи підтримки вже існуючої програми, замість неї рекомендують використати cryptography (що також використовує C бібліотеку OpenSSL).

PyCryptodome

PyCrypto/PyCryptodome – відкрита бібліотека на мові Python із реалізаціями низькорівневих криптографічних примітивів. PyCryptodome – зворотно сумісна з застарілою PyCrypto бібліотека, та є її більш актуальною альтернативою. На відміну від PyOpenSSL, що є обгорткою над бібліотекою для C, більшість алгоритмів реалізовано чисто мовою Python, і лише в деяких випадках, таких, як для частини гешування та роботи з блоковими шифрами код є розширенням над C.

Головною перевагою є простота встановлення та використання. Бібліотека має менший функціонал в порівнянні з альтернативами і фокусується на реалізації основних криптопримітивів та доступом до більшості актуальних геш функцій. Підходить для швидкої побудови/реалізації криптографічних алгоритмів.

Cryptography

pyca/cryptography – альтернатива, ціль котрої – стати стандартом для криптографії для мови Python. Також використовує C бібліотеку OpenSSL, але ставить ціллю виправити всі основні недоліки (нестачу високорівневого API, меншу підтримку, схильність окремих функцій до помилок, відсутність реалізації деяких алгоритмів, тощо). Її рекомендують використовувати в загальному випадку.

Порівняння

Результати тестів швидкості генерування ключів та гешування наведені в lab1.ipynb. З них можна сказати що PyCryptodome працює найдовше при генеруванні ключів. Гешування теоретично має бути в усіх однакове, проте, в PyOpenSSL воно швидше. Можливо через можливість викликання функції гешування із швидшим створенням об'єкту, інших причин не бачу, оскільки cryptography має мати подібну до PyOpenSSL реалізацію.

Висновок

При необхідності просто швидко збудувати криптографічний алгоритм та перевірити його працездатність – найкращим вибором буде саме ***PyCryptodome*** через простоту роботи з ним. Але бібліотека не надто швидка та не має API вищого рівня, тому в інших випадках для Python бажано використовувати ***cryptography*** (якщо немає необхідності підтримувати вже написану на PyOpenSSL програму).