НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра математичних методів захисту інформації

ЛАБОРАТОРНА РОБОТА №1

на тему: "Вибір та реалізація базових фреймворків та бібліотек"

Виконали: студенти 5 курсу, групи ФІ-12мп
Бублик Єгор, Волинський Євгеній та Слуцький Андрій

Київ — 2021

1. Мета роботи

Вибір базових бібліотек/сервісів для подальшої реалізації криптосистеми.

2. Завдання на лабораторну роботу

Вибір бібліотеки реалізації основних криптографічних примітивів з точки зору їх ефективності за часом та пам'яттю для різних програмних платформ, а саме — порівняння бібліотек OpenSSL, crypto++, CryptoLib, PyCrypto для розробки гібрідної криптосистеми під Windows платформу.

3. OpenSSL

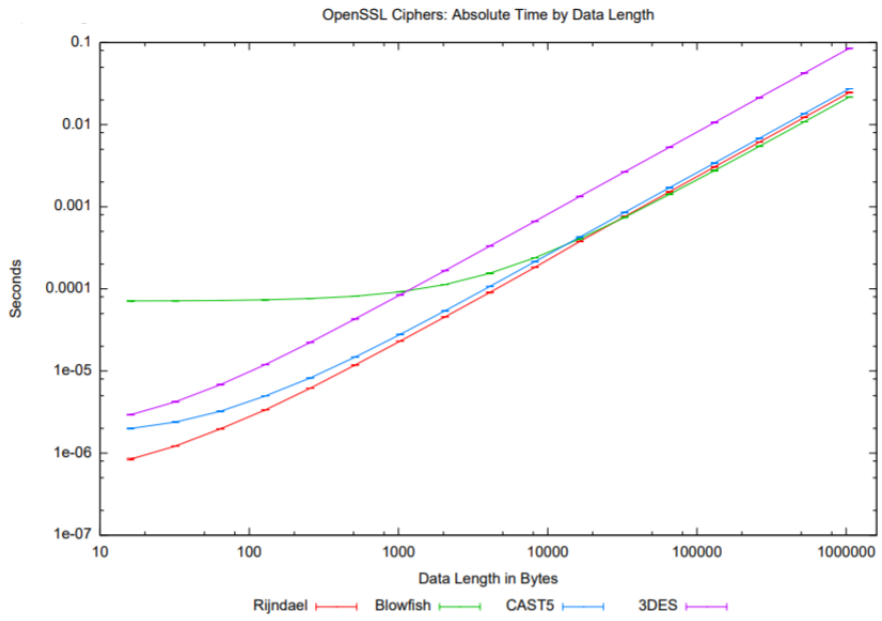

Рис. 1. Результати тестів OpenSSL

4. crypto++

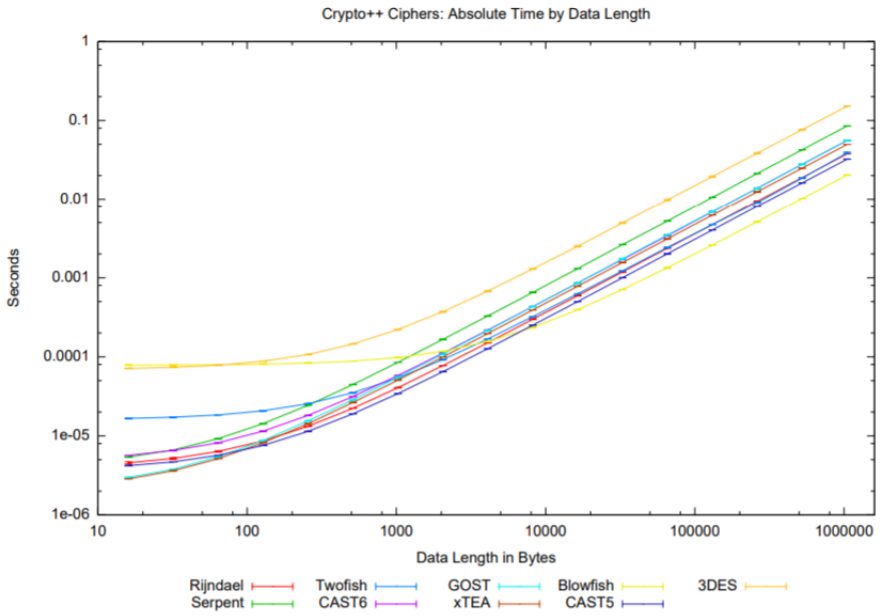

Рис. 2. Результати тестів crypto++

5. PyCrypto

Оскільки тестування бібліотеки PyCrypto не було проведено в наявному порівняльному аналізі, ми виконали його самостійно для мінімальної, заданої OpenSSL, множини алгоритмів, які також представлені у PyCrypto. Для тестування було використане хмарне середовище Google Colaboratory. Результати тестування представлені на рисунку 3.

Отримані результати схожі на результати інших криптографічних бібліотек (за винятком Rjindael), але все ж таки PyCrypto показує гірший час ніж OpenSSL та crypto++, так як значення 0.01 сек. досягається за довжини, меншої за 10^5 байтів, на відміну від OpenSSL та crypto++.

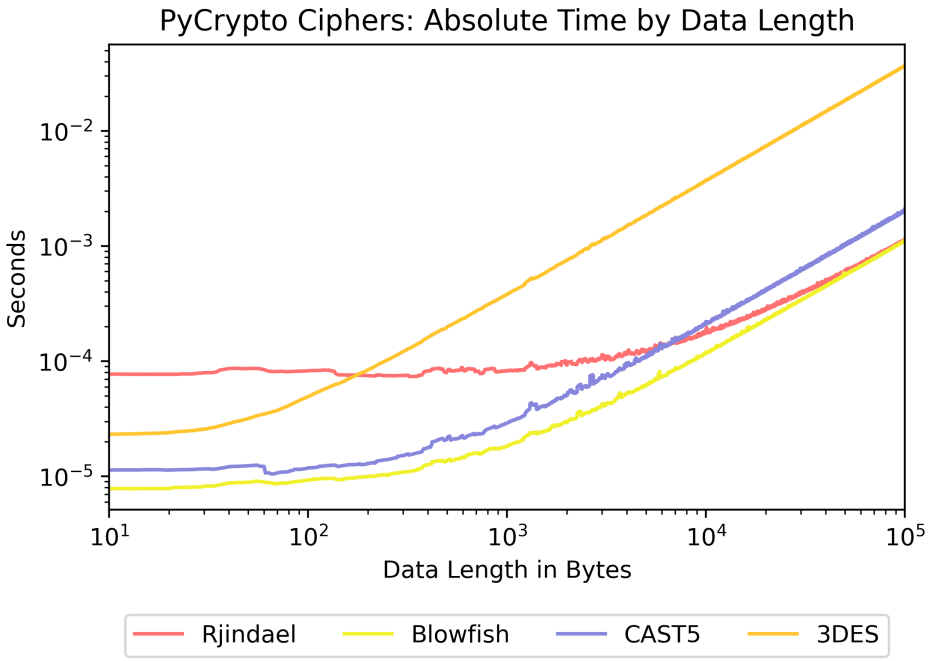

Рис. 3. Результати власних тестів PyCrypto

Зауважимо, що графіки отриманих залежностей не гладкі через нестабільне навантаження хмарного процесору, що також могло вплинути на швидкодію.

6. Висновки

Під час виконання лабораторної роботи, ми ознайомились із бібліотеками, що реалізують основні криптографічні примітиви.

Бібліотека PyCrypto виявилася повільнішою, оскільки Python є високорівневою мовою програмування, але ми не вважаємо це критичним, адже незважаючи на швидкість, по рівню комфорта та доступних можливостей, Python-у немає рівних. Саме тому, для подальшої роботи ми обрали PyCrypto.

Під час виконання роботи ми набули навичок з проведення аналізу та порівняння різних фреймворків та бібліотек.