Лабораторна робота №1

Підгрупа 2А

Порівняння криптографічних бібліотек OpenSSL, PyCryptoDome, RSA(pure python) для розробки криптографічної системи під ОС Windows.

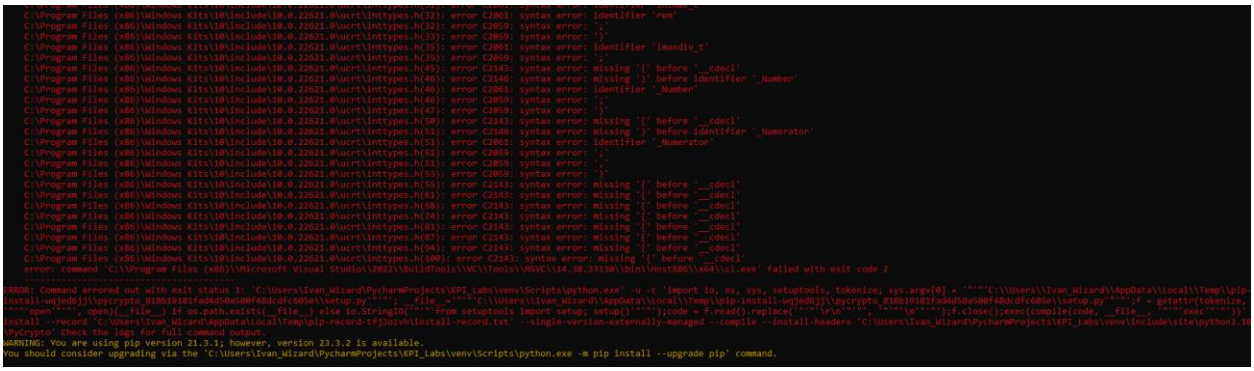
У цьому дослідженні, я хотів би порівняти бібліотеки PyCrypto та OpenSSL з точки зору ефективностю за часом для ос Windows. Доцільно взяти криптопримітив, що присутній в обох бібліотеках.

Нехай це буде просто стандартна RSA.

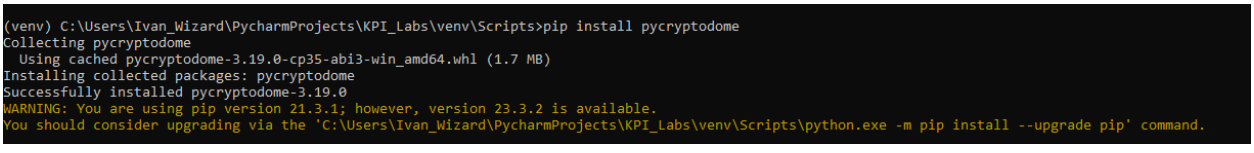
PyCrypto:

Безпосередньо з PyCrypto, відразу почались проблеми, зокрема з залежностями від C++, тоді як більш сучана надбудова – pycryptodome, інсталювалася без проблем:

PyCrypto:



Pycryptodome:



Деякі модулі бібліотеки реалізовані в C для підвищення продуктивності;

інші написані на Python для зручності модифікації. Як правило, низькорівневі функції, такі як шифри та геш-функції, пишуться на мові C, тоді як менш критичні функції були написані на Python. В даний час криптографічні реалізації є прийнятно швидкими, але не надзвичайно хорошими.

OpenSSL:

На даний час OpenSSL складається з чотирьох частин:

1. Libcrypto — це основна бібліотека для реалізації численних криптографічних примітивів та автентифікації. Крім того, вона надає набір допоміжних сервісів для реалізації таких протоколів, як CMS та OCSP;

2. Engine — функціонал libcrypto може бути розширений за допомогою API Engine. Зазвичай engines – це динамічно завантажувані модулі, які зареєстровані у libcrypto і використовують доступні інтерфейси для забезпечення реалізації криптографічного алгоритму. Зазвичай це альтернативні реалізації алгоритмів, які вже надаються libcrypto і використовуються (наприклад, для забезпечення апаратного прискорення алгоритму), але вони можуть включати алгоритми, не реалізовані в стандартному OpenSSL. Деякі engines надаються як частина дистрибутиву OpenSSL, а деякі — зовнішнім сторонам (наприклад ГОСТ);

3. Libssl — це бібліотека залежить від libcrypto та реалізує протоколи TLS та DTLS;

4. Applications (додатки) — це набір інструментів командного рядка, які використовують базові компоненти libssl та libcrypto для забезпечення набору криптографічних та інших функцій, таких як:

(а) Генерація та перевірка ключів та параметрів;

(б) Створення та перевірка сертифікатів;

(в) Інструменти тестування SSL / TLS;

(г) Інспекція ASN.1.

Порівняння часу генерації ключів:

Бібліотека	Час генерації ключів
OpenSSL	3.09848846785678383
PyCryptoDome	78.57848894947484889

Висновки:

Звичайно в середньому бібліотека OpenSSL буде швидшою за pycryptodome, проте на стороні останньої швидкість та зручність використання. Тож для навчальних проектів, можливо доцільніше обирати Pycryptodome.