НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ТА АНАЛІЗУ ДАНИХ

Лабораторна робота №1

З дисципліни «Методи реалізації криптографічних механізмів»

Студента групи ФІ-21мн
Прохоренко О.С.

Викладач:
Селюх П.В.

Київ-2023

ХІД РОБОТИ

1. Завдання

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

2. Результати

Аналогічні бібліотеки для python:

- OpenSSL – **pyOpenSSL** (але рекомендують від нього відмовлятись і переходити до **cryptography**);
- Crypto++ – **PyCrypto** (але він давно не підтримується та має дірки в безпеці, рекомендують використовувати **cryptography** або **PyCryptodome**);
- CryptoLib – не знайшов жодного нормального рішення;
- Додатково знайшов **Python-RSA** (імплементація на чистому python)**;**

Для порівняння швидкодії використовувалися наступні тести:

- Генерація 100 пар ключів RSA 2048 біт
- Шифрування 128 байт даних 100 разів
- Розшифрування 128 байт даних 100 разів

RSA (Rivest–Shamir–Adleman) є одним із найвідоміших алгоритмів асиметричного шифрування та використовується для безпечного обміну інформацією. Ось основні аспекти RSA:

- Асиметричне шифрування: Відрізняється від симетричного шифрування тим, що використовує два ключі — публічний для шифрування та приватний для дешифрування. Це дозволяє користувачам шифрувати повідомлення публічним ключем, яке можна розшифрувати лише відповідним приватним ключем.
- Генерація ключів: Ключі генеруються на основі великих простих чисел та їхніх математичних властивостей. Процес включає вибір двох великих простих чисел, обчислення їхнього добутку (модуля), та вибір публічного та приватного експонентів.
- Безпека: Основою безпеки RSA є труднощі факторизації великого числа, що є добутком двох великих простих чисел. Величина ключа (зазвичай 2048 або 4096 біт) має велике значення для безпеки алгоритму.
- Застосування: RSA використовується для шифрування даних, цифрових підписів, та інших застосувань, де потрібен безпечний обмін ключами або даними.
- Виклики та обмеження: Оскільки безпека RSA залежить від складності факторизації великих чисел, збільшення обчислювальної потужності та розвиток квантових комп'ютерів може в майбутньому поставити під загрозу його безпеку. Також, RSA є відносно повільнішим у порівнянні з симетричними алгоритмами шифрування.

2.1. **Cryptography**

```
Keys generating
Time to generate 100 keys: 5.353 sec
Average time to generate 1 key: 0.054 sec

Encryption
Time to encrypt 100 messages: 0.006 sec
Average time to encrypt 1 message: 0.00006 sec

Decryption
Time to decrypt 100 messages: 0.143 sec
Average time to decrypt 1 message: 0.001 sec

All messages were decrypted correctly
```

Висновок: Найшвидша бібліотека з найменшим часом генерації ключів та шифрування/дешифрування.

2.2. **PyCryptodome**

```
Keys generating
Time to generate 100 keys: 53.009 sec
Average time to generate 1 key: 0.530 sec

Encryption
Time to encrypt 100 messages: 0.096 sec
Average time to encrypt 1 message: 0.00096 sec

Decryption
Time to decrypt 100 messages: 3.690 sec
Average time to decrypt 1 message: 0.037 sec

All messages were decrypted correctly
```

Висновок: Помітно повільніше за Cryptography, особливо у генерації ключів та дешифруванні.

2.3. Python-RSA (RSA)

```
Keys generating
Time to generate 100 keys: 371.609 sec
Average time to generate 1 key: 3.716 sec

Encryption
Time to encrypt 100 messages: 0.018 sec
Average time to encrypt 1 message: 0.00018 sec

Decryption
Time to decrypt 100 messages: 0.910 sec
Average time to decrypt 1 message: 0.009 sec

All messages were decrypted correctly
```

Висновок: Найповільніша бібліотека, особливо у генерації ключів.

3. Висновок

Cryptography (аналог OpenSSL) є найкращим вибором для розробки гібридної криптосистеми. Ця бібліотека забезпечує найкращий баланс швидкості генерації ключів та ефективності шифрування/дешифрування. Вона значно швидша за інші бібліотеки, що робить її ідеальною для сценаріїв, де потрібна висока продуктивність та мінімальний час обробки.