

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 ефективності 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 сучасна надбудова – pycryptodome, інстальовалася без проблем:

PyCrypto:

```
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(32): error C2061: syntax error: identifier 'run'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(32): error C2060: syntax error:
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(33): error C2060: syntax error:
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(35): error C2061: syntax error: identifier 'immed_t'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(35): error C2060: syntax error:
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(45): error C2143: syntax error: missing '[' before 'cdecl'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(46): error C2146: syntax error: missing ')' before identifier 'Number'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(46): error C2061: syntax error: identifier 'Number'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(46): error C2060: syntax error:
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(47): error C2060: syntax error:
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(50): error C2143: syntax error: missing '[' before 'cdecl'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(51): error C2146: syntax error: missing ')' before identifier 'Numerator'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(51): error C2061: syntax error: identifier 'Numerator'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(51): error C2060: syntax error:
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(53): error C2060: syntax error:
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(53): error C2143: syntax error: missing '[' before 'cdecl'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(61): error C2143: syntax error: missing '[' before 'cdecl'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(61): error C2143: syntax error: missing '[' before 'cdecl'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(68): error C2143: syntax error: missing '[' before 'cdecl'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(74): error C2143: syntax error: missing '[' before 'cdecl'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(81): error C2143: syntax error: missing '[' before 'cdecl'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(87): error C2143: syntax error: missing '[' before 'cdecl'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(94): error C2143: syntax error: missing '[' before 'cdecl'
C:\Program Files (x86)\Windows Kits\10\Include\10.0.22021.0\WinRT\IntTypes.h(100): error C2143: syntax error: missing '[' before 'cdecl'
error: command 'C:\Program Files (x86)\Microsoft Visual Studio\2022\BuildTools\VC\Tools\MSVC\14.30.32510\bin\Hostx86\x64\cl.exe' failed with exit code 2

ERROR: Command errored out with exit status 1: 'C:\Users\Ivan_Wizard\PycharmProjects\KPI_Labs\venv\Scripts\python.exe' -u -c 'import io, os, sys, setuptools, tokenize; sys.argv[0] = '"'"'C:\Users\Ivan_Wizard\AppData\Local\Temp\pip-install-uyj6d2j\pycrypto_818b1817e4ad6b0e0f40c6060\setup.py'"'; __file__ = '"'"'C:\Users\Ivan_Wizard\AppData\Local\Temp\pip-install-uyj6d2j\pycrypto_818b1817e4ad6b0e0f40c6060\setup.py'"'; if __name__ == '__main__': main()' file 'C:\Users\Ivan_Wizard\AppData\Local\Temp\pip-record-ffj0z0h\install-record.txt' -i --single-version-externally-managed --compile --install-header 'C:\Users\Ivan_Wizard\PycharmProjects\KPI_Labs\venv\include\python3.10\python3.10.pc'
WARNING: You are using pip version 21.3.1; however, version 23.1.2 is available.
You should consider upgrading via the 'C:\Users\Ivan_Wizard\PycharmProjects\KPI_Labs\venv\Scripts\python.exe -m pip install --upgrade pip' command.
```

PyCryptodome:

```
(venv) C:\Users\Ivan_Wizard\PycharmProjects\KPI_Labs\venv\Scripts>pip install pycryptodome
Collecting pycryptodome
  Using cached pycryptodome-3.19.0-cp35-abi3-win_amd64.whl (1.7 MB)
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.19.0
WARNING: You are using pip version 21.3.1; however, version 23.1.2 is available.
You should consider upgrading via the 'C:\Users\Ivan_Wizard\PycharmProjects\KPI_Labs\venv\Scripts\python.exe -m pip install --upgrade pip' command.
```

Деякі модулі бібліотеки реалізовані в С 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 проєктів, можливо доцільніше обирати Pycryptodome.