Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА

з

Методи реалізації криптографічних механізмів

Виконав:

студент 6 курсу ФТІ

групи ФБ-21мн

Мельник Дмитро

Скидан Данилов

київ-2023

Результати роботи

rsa
Genarate 1 keys
result_time 2.2768821716308594
cipher 1000 massage
result_time 0.16150784492492676
decipher 1000 massage
result_time 6.992327451705933

crypto_plus
Genarate 1000 keys
result_time 0.01812744140625
cipher 1000 massage
result_time 0.004106044769287109
decipher 1000 massage
result_time 0.014217615127563477

openssl
Genarate 1000 keys
result_time 60.995665311813354
cipher 1000 massage
result_time 46.947168827056885
decipher 1000 massage
result_time 49.1867196559906

По результатам бібліотека crypto_plus є найбільш продуктивною по часу. Тобто витрачається менше часу розшифрування а шифрування.
Сама бібліотека pycryptodome є оберткою над бібліотекою c++.

також у даній роботі була використана бібліотека pyOpenSSL що не є дуже добрим варіантом. Краще використати `cryptography`.
https://github.com/pyca/cryptography