Лабораторна робота № 1.
Вибір та реалізація базових фреймворків та бібліотек

Виконали: *Бараніченко Андрій, Гаврилова Анастасія, Дрозд Софія, Зібаров Дмитро, Колесник Андрій*

Завдання:

Підгрупа 2А. Порівняння бібліотек OpenSSL, Crypto++, CryptoLib, PyCrypto для розробки гібридної криптосистеми під Windows платформу.

Порівняння бібліотек

Загальне порівняння

Бібліотека	**Опис функцій**	**Алгоритми**	**Вхідні дані**	**Вихідні дані**	**Коди повернення**	**Контрольний приклад**	Загальний опис

OpenSSL	Реалізація криптографічних примітивів, таких як шифрування, хешування, генерація ключів	AES, RSA, SHA-256	Вхідний текст, ключ	Зашифрований текст, хеш	0 - успіх, інші - помилки	Generate an RSA key:
						
						#include <openssl/rsa.h>
						EVP_PKEY_keygen_init(ctx);
						EVP_PKEY_keygen(ctx, &pkey);
						_____
						`openssl genrsa -out example.key [bits]`
							Висока продуктивність, підтримка багатьох алгоритмів, активна спільнота

Crypto++	Бібліотека для C++, що підтримує широкий спектр криптографічних алгоритмів	AES, RSA, SHA-256	Вхідний текст, ключ	Зашифрований текст, хеш	0 - успіх, інші - помилки (виключення)	#include <cryptlib.h> CryptoPP::RSA::PrivateKey privateKey; privateKey.GenerateRandomWithKeySize(rng, 2048);	Легка інтеграція з C++, велика кількість алгоритмів

CryptLib	Легка бібліотека для базових криптографічних операцій	AES, RSA, MD5	Вхідний текст, ключ	Зашифрований текст, хеш	0 - успіх, інші - помилки	CryptoLib::AES aes;
						aes.setKey(key);
						aes.encrypt(input, output);
							Простота використання, підходить для базових задач

PyCrypto	Бібліотека для Python, що забезпечує криптографічні функції	AES, RSA, SHA-256	Вхідний текст, ключ	Зашифрований текст, хеш	0 - успіх, інші - помилки	from Crypto.Cipher import AES cipher = AES.new(key, AES.MODE_ECB) ciphertext = cipher.encrypt(plaintext)	Легка інтеграція з Python, зручність використання

Порівняння по різних параметрам

- Public key algorithms

Implementation	**RSA**	**DSA**	**ECDSA**	**EdDSA**	**Ed448**	**DH**	**ECDH**	**ECIES**	**ElGamal**	**NTRU (IEEE P1363.1)**	**DSS**
cryptlib	Yes	Yes	Yes	No	No	Yes	Yes	No	Yes	No	Yes
Crypto++	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes
OpenSSL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No

PyCrypto	Yes	Yes	Yes	Yes	Yes	-	Yes	-	No	-	-

- Elliptic-curve cryptography (ECC) support

Implementation	NIST	SECG	ECC Brainpool	Curve25519	Curve448	GOST R 34.10	SM2
cryptlib	Yes	Yes	Yes	No	No	No	No
Crypto++	Yes	Yes	Yes	Yes	No	No	No
OpenSSL	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PyCrypto	Yes	No	No	Yes	Yes	No	No

- Public key cryptography standards

Implementation	PKCS #1	PKCS #5, PBKDF2	PKCS #8	PKCS #12	IEEE P1363	ASN.1
cryptlib	Yes	Yes	Yes	Yes	No	Yes
Crypto++	Yes	Yes	Yes	No	Yes	Yes
OpenSSL	Yes	Yes	Yes	Yes	No	Yes
PyCrypto	-	-	Yes	-	-	-

- Hash functions

Implementation	MD5	SHA-1	SHA-2	SHA-3	RIPEMD-160	Tiger	Whirlpool	BLAKE2	GOST R 34.11-94 (aka GOST 34.311-95)	GOST R 34.11-2012 (Stribog)	SM3
OpenSSL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Crypto++	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
cryptlib	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No
PyCrypto	Legacy	Yes	Yes	Yes	Legacy	No	No	Yes	No	No	No

- Block ciphers

Implementation	AES	3DES	Camellia	Blowfish	Twofish	IDEA	CAST5	ARIA	GOST 28147-89 / GOST R 34.12-2015 (Magma & Kuznyechik)	SM4
cryptlib	Yes	Yes	No	Yes	No	Yes	Yes	No	No	No
Crypto++	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Partial	Yes
OpenSSL	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
PyCrypto	Yes	Legacy	No	Legacy	No	No	No	No	No	No

- Stream ciphers

Implementation	RC4	HC-256	Rabbit	Salsa20	ChaCha	SEAL	Panama	WAKE	Grain	VMPC	ISAAC
cryptlib	Yes	No	No	No	No	No	No	No	No	No	No
Crypto++	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
OpenSSL	Yes	No	No	No	Yes	No	No	No	No	No	No
PyCrypto	Deprecated	No	No	Yes	Yes	No	No	No	No	No	No

З порівняння цих таблиць, найкращими виглядають бібліотеки OpenSSL та Crypto++, оскільки надають найбільше доступних алгоритмів та шифрів.

«Crypto++ надає більше криптографічних примітивів низького рівня. Crypto++ не надає нічого пов'язаного з TLS і DTLS. Crypto++ схожий на низькорівневий криптографічний *швейцарський армійський ніж*.

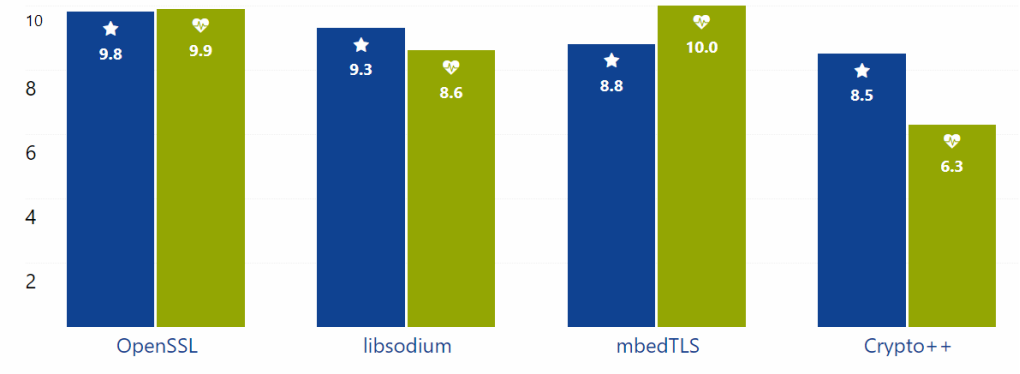
OpenSSL надає деякі низькорівневі криптографічні примітиви, підтримку апаратних модулів і робочі реалізації TLS і DTLS. Оскільки він підтримує апаратне забезпечення, він забезпечує інтерфейс PKCS 11. Оскільки він підтримує TLS і DTLS, він має розширену підтримку сокетів і аналізатор X509.»

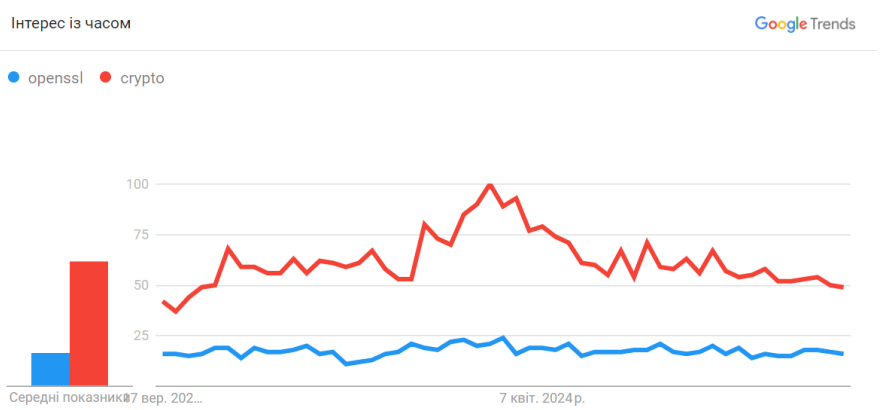
В той же час, CryptoLib - проста у використанні бібліотека, яка підходить для базових криптографічних задач. PyCrypto - для розробників на Python, має менше різних механізмів та можливостей.

Тенденцій OpenSSL та Crypto++

OpenSSL		Crypto++
	Repository	
25,477	★ Stars	4,796
1,012	Watchers	195
10,062	Forks	1,487
101 days	Release Cycle	-
over 4 years ago	Latest Version	-
2 days ago	Last Commit	about 2 months ago
	More	
L2	Code Quality	L1
C	</> Language	C++
Apache License 2.0	© License	GNU General Public License v3.0 or later
Cryptography	Tags	Cryptography

Бібліотека OpenSSL є значно популярнішою та краще оціненою порівняно з Crypto++. Це призводить до наявності більшої кількості документації, а також до активного обговорення та вирішення різних проблем на форумах і інших платформах користувачів OpenSSL. Проте інтерес до Crypto++ більший і зростає.





Висновок.

Для розробки гібридної криптосистеми під Windows, найкращим вибором буде **OpenSSL**, завдяки високій продуктивності, широкому спектру доступних алгоритмів та популярності серед користувачів.