УДК 681.3.06

ПОРІВНЯЛЬНИЙ АНАЛІЗ КРИПТОГРАФІЧНИХ БІБЛІОТЕК З ВІДКРИТИМ КОДОМ ТА РЕКОМЕНДАЦІЇ З ЇХ ВИКОРИСТАННЯ

І.Ф. АУЛОВ, Ю.І. ГОРБЕНКО

Запропоновано методику, що дозволяє провести порівняльний аналіз криптографічних бібліотек за сукупністю критеріїв та показників. Наводяться результати порівняльного аналізу найпоширеніших криптографічних бібліотек: Crypto++, MIRACLE, OpenSSL, OpenPGP, Botan, GNU Crypto, CryptLib, NTL за запропонованою методикою. На основі вимірів, проведених відповідно до методології, яка враховує ефективність і відносну частоту використання примітивних криптографічних операцій, а також показників швидкості основних криптографічних перетворень виконується порівняння криптографічних бібліотек.

Ключові слова: криптографічна бібліотека, показники ефективності, порівняльний аналіз

ВСТУП

Сьогодні стало вже зрозуміло, що в комп'ютерних системах та мережах потрібно забезпечувати захист інформації не тільки в державних, банківських та комерційних установах, але й надавати основні послуги з захисту інформації звичайним користувачам.

Для звичайного користувача головним критерієм вибору засобу захисту персональної інформації є доступність цього засобу. Під доступністю засобу захисту розуміються умови розповсюдження, відсутність обмежень на використання та його ціна.

В сучасному світі серед користувачів найбільше розповсюдження отримали програмні засоби захисту інформації. Це пов'язано з низкою факторів, до яких відносяться: ціна (яка з об'єктивних причин нижче за ціну на аналогічні апаратні пристрої), кроссплатформеність (здатність програмного забезпечення функціонувати на різних платформах), простіша інтеграція в систему захисту, модульність та розширюваність (можливість в залежності від потреб захисту включати додаткові модулі розширяючи цим функціонал існуючих). Розглянуті аргументи на користь використання програмних засобів захисту, говорять про актуальність роботи з дослідження критеріїв та показників для порівняння програмних засобів захисту – криптографічних бібліотек.

Кожний користувач висуває до програмного засобу захисту свій унікальний набір критеріїв, з яких потім формуються різні показники. Унікальність набору критеріїв полягає не тільки в їх різному наборі, але й в ранжуванні цих критеріїв за ступенем важливості.

Метою цієї роботи є узагальнення вимог, що висуваються користувачами до криптографічних бібліотек та вироблення на їх основі сукупності критеріїв та показників для проведення порівняння криптографічних бібліотек.

Для проведення порівняльного аналізу у нашому дослідженні, було обрано найбільш поширені бібліотеки з відкритим кодом:

– NTL [5], OpenSSL [4], OpenPGP [1], GNU Crypto [3], CryptLib(Sleepycat) [7];

– умовно безкоштовні (BSD): Crypto++ [2], Botan [8];

– комерційні (AGPL): MIRACLE [6].

В процесі аналізу, було проведено оцінку придатності використання вищезгаданого програмного забезпечення бібліотеки для реалізації різноманітних криптосистем, з використанням ефективності реалізації примітивних операцій в якості основного критерію оцінки.

Порівняльний аналіз ефективності програмного забезпечення розглядається не тільки з точки зору ефективності реалізації криптографічного примітиву, а й як комплекс з великим числом змінних таких як, операційна система, процесор, об'єм пам'яті, вибір компілятора і його параметри оптимізації.

Також порівняльний аналіз включає в себе ряд вторинних критеріїв, таких як підтримка різноманітних криптографічних перетворень: асиметричні та симетричні криптоперетворення, функції гешування, реалізація протоколів, документація, простота використання і портативність.

Це дослідження ставить перед собою мету забезпечити розробників програмного забезпечення знаннями, необхідними, для того щоб зробити більш правильний вибір стосовно використання доступних бібліотек в своїх продуктах на основі набору критеріїв та показників.

1. КРИТЕРІЇ ТА ПОКАЗНИКИ ОЦІНКИ

Попередній аналіз показав, що більшість користувачів криптографічних бібліотек виділяють дві основні групи критеріїв: основні (базові) та вторинні. Під основними розуміються окремі критерії чи групи критеріїв, які є основними (найбільш важливими) для досягнення основної мети: обрання тієї чи іншої альтернативи. При цьому таким критерієм не можна нехтувати або вважати його не суттєвим, бо відмова від критерію призведе до отримання помилкового результату.

Під вторинними розуміються критерії, які не суттєво будуть впливати на остаточний результат, та можуть бути відкинуті в процесі аналізу.

В залежності від конкретної задачі набір основних критеріїв може змінюватися, та доповнюватися з групи вторинних.

Для вибору базових критеріїв при проведенні порівняльного аналізу бібліотек конкретизуємо кінцеву мету цього аналізу, як отримання бібліотеки, яка найбільш ефективно реалізує криптографічні перетворення.

Виходячи з мети аналізу до основних критеріїв буде відноситися:

– базові математичні операції, що використовуються в криптографічних алгоритмах;

– криптографічні алгоритми, що реалізовано;

– необхідні ресурси системи: пам'ять, процесорний час.

До вторинних критеріїв нами було віднесено:

– універсальність, розширюваність та переносиміть на інші платформи;

– доступність бібліотек;

– підтримка криптографічних та Інтернет протоколів;

– можливість проведення тестування.

Запропоновані критерії будемо оцінювати за наступними показниками:

– швидкість виконання базових математичних та криптографічних операцій (вимірюється в оп/с);

– швидкість виконання криптографічних функцій: шифрування, розшифрування, генерації ключем, гешування і т.д.(вимірюється в Мбіт/с);

– розмір загальносистемних параметрів та ключів (вимірюється в бітах);

– розмір пам'яті (вимірюється в Мб);

– процесорний час (такти процесора);

– підтримка різних програмних та апаратних платформ та компіляторів;

– можливості з оптимізації бібліотеки за рахунок налаштувань компілятору під певну платформу;

– можливість розпаралелювання;

– можливість експорту, необхідність отримання ліцензії та використання в комерційних додатках;

– наявність реалізованих протоколів;

– наявність функцій тестування, самотестування.

2. ЗАГАЛЬНА ХАРАКТЕРИСТИКА БІБЛІОТЕК ТА ПЛАТФОРМИ ДЛЯ ТЕСТУВАННЯ

Загальна характеристика бібліотек наводиться в табл. 1. В якості мови програмування в бібліотеках використовується C та C++. Більшість з цих бібліотеки можуть бути описані як ті, що реалізують криптографічні алгоритми: симетричного шифрування, функцій гешування, направленого шифрування, підпису. Бібліотеки NTL та MIRACLE представляють собою бібліотеки, що реалізують математику багато розрядної точності.

Такі бібліотеки, як Crypto++, OpenSSL, OpenPGP, GNU Crypto, CryptLib(Sleepycat) реалізують не тільки криптографічні алгоритми, але і мережеві протоколи: Kerberos, S/MIME, PGP, SSL/TLS, SSH.

Для аналізу ефективності реалізації алгоритмів було використано дві робочі станції з наступними характеристиками: Pentium IV 2,0 ГГц з 512 Мб ОЗУ та C2D 2,2 ГГц з 1 Гб ОЗУ. На машині Pentium IV та C2D було встановлено Windows XP32 (Cygwin). Бібліотеки були скомпільовані з використанням GNU C / C + + компілятору.

В табл. 2 наведено основні математичні операції, що реалізовано в бібліотеках для асиметричної криптографії. В табл. 3 наведено основні криптографічні алгоритми, які використовуються сьогодні або мають перспективу в застосуванні.

3. МЕТОДИКА ПОРІВНЯННЯ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Для оцінки ефективності реалізації криптографічних алгоритмів для кожної бібліотеки, використаємо методику, яка наводиться в роботі [9].

Основні кроки методики порівняння:

1. Обирається множина бібліотек $LIB_0 ... LIB_{N-1}$.

2. Обирається множина алгоритмів за якими буде здійснюватися порівняння бібліотек $ALG_0 ... ALG_{M-1}$.

3. Обирається фіксований розмір вхідних параметрів для кожного алгоритму ALG_i .У випадку якщо алгоритм, який порівнюється приймає різні довжини параметрів, то потрібно обрати вектор довжин параметрів $PRM_0 ... PRM_{T-1}$.

4. Для кожної бібліотеки та кожного обраного алгоритму експериментально обчислюється

Таблиця 1

Загальна характеристика криптографічних бібліотек

№	Бібліотека	Тип бібліотеки	Ліцензія	Версія
1	NTL	Реалізує математику підвищеної точності	GNU GPL	5.3.1
2	MIRACLE	Реалізує математику підвищеної точності	AGPL	4.82
3	Botan	Криптографічна	BSD	1.10.1
4	Crypto++	Криптографічна	BSD	5.61
5	OpenSSL	Криптографічна, реалізує протокол SSL	GNU	0.9.7c
6	OpenPGP	Криптографічна, реалізую схему захищеної електронної пошти PGP	GNU	0.9
7	GNU Crypto	Криптографічна, реалізує протокол Kerberos	GNU	2.0.1
8	CryptLib	Криптографічна, протоколи Kerberos, S/MIME, PGP, SSL/TLS, SSH	GNU	3.4.1

Таблиця 2

Аналіз математичних операцій, що реалізовано в криптографічних бібліотеках

№	Бібліотека	Метод множення великих чисел	Метод зведення в ступінь за модулем	Метод знаходження GCD та xGCD	Каратцуби скалярного множення ЕК
1	NTL	Каратцуби	Зліва на право(≥2 -512), - Sliding window (≥512)	Узагальнений бінарний	-
2	MIRACLE	Звичайний/ Каратцуби	Sliding window (≥2)	Lehmer	wNAF-based interleaving
3	Botan	Каратцуби	Блочний метод (≥2	Узагальнений бінарний	Зліва на право
4	Crypto++	Каратцуби	З ліва на право(≥2 -32), блочний(≥32)	Евкліда	Simultaneous Sliding Window
5	OpenSSL	Звичайний/ Каратцуби	Sliding window (≥2)	Бінарний	wNAF-based interleaving
6	OpenPGP	Звичайний	Sliding window (≥2)	Бінарний	-
7	GNU Crypto	Каратцуби	З ліва на право(≥2 -32), блочний(≥32)	Узагальнений бінарний/ Lehmer	wNAF-based interleaving
8	CryptLib	Каратцуби	Sliding window (≥2)	Lehmer	wNAF-based interleaving

Таблиця 3

Криптографічні алгоритми, що реалізовано в криптографічних бібліотеках

№	Бібліотека	Симетрична криптографія			Асиметрична криптографія	Функції гешування
		Блокові шифри	Потокові шифри	Коди аутентифікації		
1	NTL	-	-		-	-
2	MIRACLE	Rijndael AES	-	-	**Підпис:** RSA, DSA, ECDSA, ECGDSA, ECKCDSA **НШ:** RSA	SHA-1, SHA-2
3	Botan	Rijndael AES, Serpent, Twofish, TDES, GOST 28147	ARC4, Salsa20/ XSalsa20, Turing	HMAC, CMAC (aka OMAC1), CBC-MAC, ANSI X9.19, DES-MAC	**Підпис:** RSA, DSA, ECDSA, GOST 34.10-2001, Nyberg-Rueppel, **НШ:** RSA, ElGamal **ВК:** Diffie-Hellman, ECDH	SHA-1, SHA-2, Skein-512, Keccak, Whirlpool, Tiger, GOST 34.11
4	Crypto++	Rijndael AES, Twofish, Serpent, TDES	Panama, Sosemanuk, Salsa20, XSalsa20	VMAC, HMAC, GMAC (GCM), CMAC, CBC-MAC, DMAC	**Підпис:** ECDSA, RSA, DSA, ECNR, **НШ:** RSA, ElGamal, Nyberg-Rueppel, **ВК:** DH, DH2, ECDH	SHA-1, SHA-2, Tiger, WHIRLPOOL, RIPEMD-256, RIPEMD-320
5	OpenSSL	Rijndael AES, GOST 28147 TDES	-	GOST 28147-89 MAC, HMAC	**Підпис:** ECDSA, RSA, DSA **НШ:** RSA, ElGamal, **ВК:** DH, ECDH	SHA1
6	OpenPGP	Rijndael AES, Twofish, TDES	-	-	**Підпис:** RSA, DSA **НШ:** RSA, ElGamal	SHA-1, SHA-2
7	GNU Crypto	Rijndael AES, Twofish, Serpent, TDES	-	HMAC, UMAC	**Підпис:** RSA, DSS **НШ:** RSA, ElGamal **ВК:** DH	SHA-1, SHA-2
8	CryptLib	Rijndael AES, Twofish, Serpent, TDES	-	HMAC	**Підпис:** ECDSA, RSA, DSA **НШ:** RSA, ElGamal, **ВК:** DH, ECDH	SHA-1, SHA-2

вектор $LIB_k^{ALG_i(PRM_t)}$, i={0...M-1}, k={0...N-1}, t={0...T-1} значень часу виконання довжиною L.

5. Для кожної бібліотеки LIB_k та кожного алгоритму $ALG_i(PRM_t)$ з вектором параметрів PRM_t обирається мінімальне значення $MIN(LIB_k^{ALG_i(PRM_t)})$ з вектору $LIB_k^{ALG_i(PRM_t)}$.

6. Використовуючи $MIN(LIB_k^{ALG_i(PRM_t)})$ для кожного алгоритму $ALG_i(PRM_t)$ формується вектор мінімальних значень для бібліотек розміром N: $MIN_j(LIB_k^{ALG_i(PRM_t)})$, j={0, N-1}.

7. З цього вектору обирається мінімальне значення $MIN(MIN_j(LIB_k^{ALG_i(PRM_t)}))$, та за ним нормується весь вектор значень.

8. Далі виконується обчислення загального значення для кожного алгоритм кожної бібліотеки $RANK(LIB_k^{ALG_i})$ для всіх значень параметрів PRM_t:

$$RANK(LIB_k^{ALG_i}) = \sqrt[T-1]{\prod_{t=0}^{T-1} \frac{MIN_j(LIB_k^{ALG_i(PRM_t)})}{MIN(MIN_j(LIB_k^{ALG_i(PRM_t)}))}}$$

9. Загальний результат для бібліотеки LIB_k, обчислюється як:

$$RANK(LIB_k) = \sqrt[M]{\prod_{i=0}^{M-1} LIB_k^{ALG_i}}.$$

Порівняння бібліотек за значенням $RANK(LIB_k)$ дозволяє отримати найбільш ефективну бібліотеку за набором алгоритмів ALG_i, та розмірів вхідних параметрів PRM_t, чим менше це значення тим більш ефективною вважається бібліотека.

4. РЕЗУЛЬТАТИ ПОРІВНЯЛЬНОГО АНАЛІЗУ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Для порівняння ефективності реалізації криптографічних алгоритмів за методикою, наведеною в пункті 3, в бібліотеках було обрану наступну множину функцій:

– операцій множення великих чисел (MUL);

– зведення до ступеня за модулем (POWMOD);

– знаходження зворотнього елементу за модулем двох чисел (xGCD);

– ECMUL – множення точки ЕК на скаляр над полем F2m.

Для кожного алгоритму було виконано 100 тестів. В результаті були отримані відповідні значення RANK (табл. 4) для кожної з бібліотек та функцій відповідно.

Для порівняння ефективності реалізації крипто алгоритмів за показником швидкості було обрано:

– для симетричних шифрів AES-192(Rijnael) та TDES;

– для підпису RSA (2048), та ECDSA (F2m=283);

– код-аутентифікації повідомлення HMAC (SHA-1) блок даних 256 байт;

– функцію гешування SHA-1, блок даних 256.

Отримані результати наведені в табл. 4. В табл. 5 наведені реальні значення швидкості розглянутих криптографічних алгоритмів.

Таблиця 4

Результати оцінки ефективності реалізації криптографічних алгоритмів

№	Бібліотека	*RANK(ALG$_i$)*				AES-192	TDES	RSA (2048)		ECDSA (F2m=283)		HMAC SHA-1	SHA-1 ($l_{бл}$=256)	RANK
		MUL	POWMOD	xGCD	ECMUL			*sign*	*verf*	*sign*	*verf*			
1	NTL	1,01	1,18	1,0	-	-	-	-	-	-	-	-	-	1,06
2	MIRACLE	3,58	2,62	3,15	1	1,00	-	2,29	1,72	2,02	2,76	-	1,12	1,40
3	Botan	3,41	5,21	1,09	1,42	2,16	1,98	1,00	1,00	1,60	1,95	1,15	1,13	1,67
4	Crypto++	4,49	5,04	16,82	4,35	2,68	1,90	1,12	1,15	1,00	1,00	1,05	1,07	2,19
5	OpenSSL	2,80	2,43	12,49	1,15	4,49	3,39	1,68	1,51	1,85	2,53	1,00	1,00	2,26
6	OpenPGP	2,87	2,31	3,11	1,41	1,12	1,37	2,35	1,73	1,54	2,00	-	1,06	1,79
7	GNU Crypto	1,0	1,0	1,01	1,24	1,38	1,00	2,71	1,80	1,75	2,13	1,06	1,08	1,35
8	CryptLib	5,25	4,17	8,59	1,7	1,03	1,47	1,09	1,08	1,07	2,05	1,02	1,06	1,82

Таблиця 5

Швидкість розглянутих криптографічних алгоритмів

№	Бібліотека	AES-192(Rijnael)	TDES	RSA(2048)		ECDSA (F2m=283)		HMAC	SHA-1
				sign	verf	sign	verf		
		KB/s	KB/s	op/s	op/s	op/s	op/s	MB/s	MB/s
1	NTL	-	-	-	-	-	-	-	-
2	MIRACLE	10,125	-	78	2412	303	105	-	160
3	Botan	21,917	6,979	34	1404	240	74	161	162
4	Crypto++	27,111	6,702	38	1612	150	38	147	153
5	OpenSSL	45,461	11,94	57	2120	278	96	140	143
6	OpenPGP	11,311	4,845	80	2430	231	76	-	151
7	GNU Crypto	13,925	3,525	92	2531	263	81	149	155
8	CryptLib	10,398	5,195	37	1512	161	78	143	151

ВИСНОВКИ

За результатами порівняльного аналізу ефективності криптографічних бібліотек можна зробити наступні висновки:

– бібліотеки NTL та GNU Crypto показали кращі показники за операціями з великими цілими числами;

– кращим вибором для розробників програмного забезпечення, що використовує арифметику великих цілих чисел, з точки зору швидкості перетворень буде бібліотека GNU Crypto;

– якщо орієнтуватися на кількість зусиль розробника, які необхідно прикласти при розробці криптографічного алгоритму, а також на переносимість на інші платформи, то слід звернути увагу на бібліотеки MIRACLE та OpenSSL;

– в процесі вибору криптографічної бібліотеки розробник важливим фактором є апаратна та програмна платформа на якій буде використовуватися бібліотека, тому слід приділяти увагу налаштуванням компілятора та бібліотеки для кожної платформи;

– при використанні значення RANK для вибору криптографічної бібліотеки слід також звертати увагу на конкретні показники швидкості для криптографічних перетворень, які будуть використовуватися, бо на значення RANK впливають сукупність усіх показників.

Література

[1] OpenPGP: The Open Source toolkit for PGP http://openpgp.nominet.org.uk/

[2] Crypto++ Library 5.1: a Free C++ Class Library of Cryptographic schemes http://www.eskimo.com/weidai/cryptlib.html

[3] The GNU Crypto Library http://www.swox.com/gmp/

[4] OpenSSL: The Open Source toolkit for SSL/TLS http://www.openssl.org/

[5] NTL: A Library for doing Number Theory http://www.shoup.net/ntl/

[6] Shamus Software Ltd MIRACL http://indigo.ie/mscott/

[7] CryptLib: Security toolkit http://www.cs.auckland.ac.nz/~pgut001/cryptlib/

[8] Botan: Security toolkit http://botan.randombit.net/download.html

[9] Ashraf Abusharekh, Kris Kaj, Comparative Analysis of Software Libraries for Public Key Cryptography. — CRC-Press, 2007 – 18 p.

Надійшла до редколегії 28.03.2012

Аулов Іван Федорович, магістрант кафедри БІТ ХНУРЕ. Область наукових інтересів: дослідження принципів побудови, розгортання і аналізу стійкості асиметричних криптографічних систем.

Горбенко Юрій Іванович, фото та відомості про автора див. на с. 187.

УДК 681.3.06

Сравнительный анализ криптографических библиотек с открытым кодом и рекомендации по их использованию / И.Ф. Аулов, Ю.И. Горбенко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2012. – Том 11. № 2. – С. 220–224.

Предложено методику, которая позволяет провести сравнительный анализ криптографических библиотек за совокупностью критерием и показателей. Приводятся результаты сравнительного анализа наиболее распространенных криптографических библиотек: Crypto++, MIRACLE, OpenSSL, OpenPGP, Botan, GNU Crypto, CryptLib, NTL по предложенной методике. На основе измерений, проведенных соответственно методологии, которая учитывает эффективность и относительную частоту использования примитивных криптографических операций, а также показателей скорости основных криптографических преобразований выполняется сравнение криптографических библиотек.

Ключевые слова: криптографическая библиотека, показатель эффективности, сравнительный анализ.

Табл. 05. Библиогр.: 09 назв.

UDC 681.3.06

Comparative analysis of open source cryptographic libraries and recommendations for their use / I.F. Aulov, Yu.I. Gorbenko // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 220–224.

The paper proposes a technique which allows to make a comparative analysis of cryptographic libraries for the collection of criteria and indicators. Results of the comparative analysis of the most common cryptographic libraries: Crypto + +, MIRACLE, OpenSSL, OpenPGP, Botan, GNU Crypto, CryptLib, NTL on the proposed methodology are presented. The comparative analysis is implemented on the basis of the measurements taken, according to a methodology that takes into account the effectiveness and relative frequency of using primitive cryptographic operations and key indicators of the speed of the main cryptographic transformations.

Keywords: cryptographic library, performance indicator, comparative analysis.

Tab. 05. Ref.: 09 items.