Технічні науки

УДК 004.896

Гроза Петро Миколайович

кандидат технічних наук,

старший науковий співробітник кафедри комп'ютерної інженерії

Полтавський національний університет імені Юрія Кондратюка

Гроза Пётр Николаевич

кандидат технических наук,

старший научный сотрудник кафедры компьютерной инженерии

Полтавский национальный университет имени Юрия Кондратюка

Hroza Petro

Candidate of Technical Ssciences,

Senior Researcher of the Department of Computer Engineering

Poltava National Yuri Kondratyuk University

Кімачук Тетяна Володимирівна

студентка

Полтавського національного університету імені Юрія Кондратюка

Кимачук Татьяна Владимировна

студентка

Полтавского национального университета имени Юрия Кондратюка

Kimachuk Tetiana

Student of the

Poltava National Yuri Kondratyuk University

ДОСЛІДЖЕННЯ АКТУАЛЬНИХ АЛГОРИТМІВ КОДУВАННЯ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ
ИССЛЕДОВАНИЕ АКТУАЛЬНЫХ АЛГОРИТМОВ КОДИРОВАНИЯ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

RESEARCH OF ACTUAL CODING OLGORITHMS FOR PROTECTION OF PERSONAL DATA

Анотація. *Досліджено основні криптопримітиви відносно механізмів захисту персональної інформації. Проведено аналіз механізмів захисту персональних даних з обов'язковим порівнянням основних з них. Зазначено основні відмінності між шифруванням блочним та потоковим, окреслено особливості хеш-функцій. Описано механізми реалізації хеш-функції SHA-256, визначено, що алгоритм SHA-256 є більш стабільним та забезпечує достатню ступінь захисту будь-якої важливої інформації.*

Ключові слова: *криптопримітив, захист, персональні дані, алгоритм, кодування, хеш-функція, шифрування, безпека.*

Аннотация. *Исследованы основные криптопримитиви относительно механизмов защиты персональной информации. Проведен анализ механизмов защиты персональных данных с обязательным сравнением основных из них. Указаны основные различия между блочным шифрованием и потоковым, обозначены особенности хэш-функций. Описаны механизмы реализации хэш-функции SHA-256, определено, что алгоритм SHA-256 является более стабильным и обеспечивает достаточную степень защиты любой важной информации.*

Ключевые слова: *криптопримитив, защита, персональные данные, алгоритм, кодирование, хэш-функция, шифрование, безопасность.*

Summary. *The basic, kryptoperidinium regarding the mechanisms of protection of personal information. The analysis of the mechanisms for the protection of personal data with obligatory comparison of them. The main difference between block ciphers and stream marked features of hash functions. Describes mechanisms used to implement the hash function SHA-256, it is*

determined that the SHA-256 algorithm is more stable and provides a sufficient degree of protection of any important information.

Key words: *cryptomemetic, protection of personal data, algorithm, encoding, hash function, encryption, security.*

Вступ та постановка проблеми. Криптографія, як прикладна дисципліна, існує вже дуже давно. Один з найпростіших шифрів, шифр алфавітної заміни, використовувався ще за часів Цезаря. Але справжній розквіт криптографії стався лише в останні декілька сторіч, коли до завдань шифрування був застосований математичний апарат. Для захисту інформації використовується, насамперед, шифрування. При шифруванні відбувається перетворення даних у вид, недоступний для читання без відповідної інформації (ключа шифрування). Завдання полягає в тому, щоб забезпечити конфіденційність, приховавши інформацію від осіб, яким вона призначена, навіть якщо вони мають доступ до зашифрованих даних. Проте зважаючи на масштабність сучасних наукових розробок у сфері криптографії визначення найбільш дієвого та ефективного алгоритму захисту є проблемою, яка потребує детального дослідження.

Мета роботи. Дослідження основних криптопримітивів відносно механізмів захисту персональної інформації. Аналіз механізмів захисту персональних даних з обов'язковим порівнянням основних з них. Визначення основних відмінностей між шифруванням блочним та потоковим, аналіз хеш-функцій.

Аналіз останніх досліджень і публікацій. На сьогодні, питанням дослідження актуальних алгоритмів кодування для захисту персональної інформації займалося чимало, як зарубіжних так і вітчизняних вчених, до їх числа варто віднести: С. М. Алдошин, А. А. Савельєва [1], Н. Смарт [2], І.В. Лисенко [3] та А.Г. Проценко [4].

Низка авторів [6] розглядають особливості алгоритму RC5. Досліджено швидкість програмної реалізації та характеристик дифузії та конфузії алгоритму RC5. Показано, що дифузійні характеристики алгоритму RC5-32/12/16 практично відповідають сильному лавинному критерію і мають статистично однорідний розподіл [5].

Ряду сучасних методів і засобів захисту інформації в різних інформаційно-вимірювальних системах від різних видів несанкціонованого доступу, включаючи електромагнітні витоки, технічні, радіоелектронні канали, опис програмних реалізацій на основі програмних закладок, для реалізації витоку інформації з використанням комп'ютерних вірусів і ряду інших технічних методів присвячено робота А.Б. Ісаєва [7].

Однак питання дослідження основних криптопримітивів відносно механізмів захисту персональної інформації залишається дослідженим не повною мірою та потребує ретельного доопрацювання.

Виклад основного матеріалу. На сьогодні, у світі програмної інженерії, по суті є п'ять основних механізмів, що використовуються для захисту персональної інформації. До них варто віднести: симетричне шифрування, несиметричне шифрування, цифровий підпис, без ключові хеш-функції, ключові хеш-функції. Кожен із зазначених механізмів має певні особливості застосування та працює на основі крипто примітивів, розподіл яких наведено у таблиці 1.

Таблиця 1

Киптопримітиви відносно механізмів захисту персональної інформації

№	Механізм захисту	Криптопримітив
1	Симетричне шифрування	AES, DES, 3DES, IDEA, RC2, RC4, RC5, RC6, XOR, Blowfish, Twofish
2	Несиметричне шифрування	RSA, ElGamal, ECIES
3	Цифровий підпис	RSA, DSA, ECDSA,
4	Безключові хеш-функції	MD2, MD4, MD5, SHA-1, SHA-224, SHA256,

		SHA-384, SHA-512, SHA-3
5	Ключові хеш-функції	HMAC, SHA-1, SHA256, MD5

Основне призначення будь-якого шифру – забезпечення можливості передачі повідомлення по незахищеним каналам (не обов'язково мережевим) із захистом від прочитання цього повідомлення сторонніми особами. Шифри також бувають блоковими і потоковими. Блочний шифр працює з повідомленнями фіксованого розміру (наприклад, 64 біти), а поточний – шифрує весь потік даних (наприклад, побайтно). Відомі блокові шифри – DES, IDEA, Blowfish, потокові – RC4.

Блочність шифру не означає неможливість шифрування повідомлень, що перевищують по довжині розмір блоку. Основне призначення криптографічних хешів – контроль достовірності даних шляхом обчислення від них деякої функції $H(.)$, дає результат фіксованої (і зазвичай невеликої довжини). Функція $H(.)$ повинна задовольняти наступним вимогам: Для будь-яких повідомлень $m, h = H(m)$ повинна бути легко обчислювальною. Задача знаходження такого u (відмінного від m), щоб $H(u) = h$, повинна бути важкою при невідомому m. Задача знаходження такого u, що $H(u) = H(m)$ є важкою при відомому m.

Більшість популярних хеш-функцій генерують хеш довжиною 128 біт і більше. Прикладами найбільш поширених хеш-функцій є MD5 і SHA. Значення хеш-функцій часто використовуються в системах електронного цифрового підпису для генерації дайджесту повідомлення, який потім і підписується тим чи іншим алгоритмом [8]. Також хеш-функції застосовуються в системах аутентифікації для перевірки паролів – відкритий пароль користувача не повинен зберігатися в системі, замість нього зберігається його хеш, який потім порівнюється з хешем від пароля, що вводиться користувачем при вході в систему.

Електронний цифровий підпис (ЕЦП), дозволяє встановити якусь позначку, що вказує на приналежність електронного повідомлення конкретному автору. Алгоритми цифрового підпису тісно пов'язані з асиметричними шифрами. Наприклад, алгоритм цифрового підпису RSA – це практично шифр RSA, але шифрується не саме повідомлення, а його дайджест, і шифрування проводиться не на відкритому ключі, а на закритому. У цьому випадку будь-який одержувач, що має відкритий ключ автора, може розшифрувати дайджест і перевірити його правильність.

В даний час практично жоден додаток криптографії не обходиться без використання хешування.

Хеш-функція – це функція, призначена для «стиснення» довільного повідомлення чи набору даних, записаних, зазвичай, в двійковому вигляді, в певну бітову комбінацію фіксованої довжини - згортку. Хеш-функції застосовуються для: проведення статистичних експериментів, тестування логічних пристроїв, побудови алгоритмів швидкого пошуку, а також при перевірці цілісності записів в базах даних. Рівномірність розподілу їх значень при випадковому виборі значень аргументу – основна вимога до них.

Криптографічною хеш-функцією називається всяка хеш-функція, яка є криптостійкою, тобто задовольняє ряду вимог специфічних для криптографічних додатків. У криптографії хеш-функції застосовуються для вирішення наступних завдань:

– побудові систем контролю цілісності даних при їх передачі або зберіганні,

– автентифікації джерела даних.

Хеш-функцією називається будь-яка функція $h: X -> Y$, яка легко обчислюється і така, що для будь-якого повідомлення M значення $h(M) = H$ (згортка) має фіксовану бітову довжину. X – множина всіх повідомлень, Y – множина двійкових векторів фіксованої довжини.

До ключових функцій хешування пред'являються наступні вимоги: неможливість фабрикації (високу складність підбору повідомлення з правильним значенням згортки) і модифікації (високу складність підбору для заданого повідомлення з відомим значенням згортки іншого повідомлення, з правильним значенням згортки).

До безключових функцій пред'являють такі вимоги: односпрямованість, стійкість до колізій та до знаходження другого прообразу.

Під односпрямованістю розуміють високу складність знаходження повідомлення по заданому значенню згортки. Слід зауважити, що на даний момент немає використовуваних хеш-функцій з доведеною односпрямованістю.

Алгоритм CRC16/32 – контрольна сума (не криптографічне перетворення).

Сімейство алгоритмів MD розроблено Роном Райвестом, одним з розробників алгоритму RSA. Алгоритм MD5 є послідовником MD4 з поліпшеним побітовим хешуванням, додатковим раундом і поліпшеним "лавиноподібним ефектом" (avalanche effect). Головним недоліком алгоритму MD5 є його недостатня стійкість до пошуку колізій.

Алгоритми лінійки SHA на сьогодні є найбільш поширеними. Сьогодні проводиться активний перехід від SHA-1 до стандартів версії SHA-2. SHA-2 – загальна назва алгоритмів SHA224, SHA256, SHA384 і SHA512. SHA224 і SHA384 є по суті аналогами SHA256 і SHA512 відповідно, тільки після розрахунку згортки частина інформації в ній відкидається.

Алгоритм SHA також походить від MD4 і відрізняється від останнього розширеною трансформацією, додатковим раундом і поліпшеним "лавиноподібним ефектом". У порівнянні з MD5 алгоритм SHA з більш довшим дайджестом є більш стійким до атак.

Хеш-функція SHA-256 є односпрямованої функцією алгоритму SHA-2 (Secure Hash Algorithm Version 2). SHA-256 являє собою криптографічну хеш-функцію, яка є розробкою Агентства національної безпеки США. Основним завданням будь-якої хеш-функції є перетворення (або хешування) довільного набору даних значення фіксованої довжини («дайджесту» або «відбитка»). За основу в ній використана структура Тьмяніла-Дамгарда, згідно якої вихідне значення після доповнення розбивається на блоки, а кожен блок в свою чергу на 16 слів. Кожен блок повідомлення пропускається алгоритмом через цикл з 80 або 64 інтераціями, або раундами. На кожному раунді задається функція перетворення слів, які входять до складу блоку. Два слова з повідомлення перетворюються цією функцією. Отримані результати сумуються, а в результаті виходить значення хеш-функції. Для обробки наступного блоку використовуються результати обробки попереднього блоку. Незалежно один від одного блоки обробляти не можна.

Алгоритм SHA-256 на даний час реалізований у всіх присутніх на ринку спеціалізованих ASIC-майнерах, в той час як ASIC-обладнання для інших алгоритмів майнінгу ще тільки розробляється. Крім Bitcoin, майнінг за допомогою алгоритму SHA-256, застосовується у багатьох інших цифрових валютах-клонах. Приміром, його використовують альткойни Peercoin і Namecoin. Також останнім часом спостерігається популяризація нових SHA-256 монет: Ocoin, Tekcoin, Zetacoin та ін.

Висновки. Провівши дослідження варто відзначити, що на сьогодні SHA-256 – це стабільний, універсальний, простий у використанні і такий, що забезпечує достатню ступінь захисту будь-якої важливої інформації алгоритм. SHA-256 займає більше 40% всього ринку криптографічних хеш-алгоритмів і не втрачає своїх позицій протягом останніх років. Більше того, він законодавчо дозволений для захисту державних даних в США, що доводить його актуальність і значимість.

Література

1. Авдошин, С.М. Криптотехнологии Microsoft [Текст] / С.М. Авдошин, А.А. Савельева // Приложение к журналу «Информационные технологии» – 2008. – №9. – С. 23–30.
2. Смарт, Н. Криптография: пер. с англ. / Н. Смарт – М.: Техносфера, 2005. – 528 с.
3. Лысенко, И.В. Исследование быстродействия алгоритмов шифрования на базе технологии .Net Framework [Текст] / И.В Лысенко, А. Г. Проценко // Системи обробки інформації / ХУПС. – Х., 2011. – Вип. 4(94). – С. 176-181.
4. Проценко, А.Г. Исследование быстродействия алгоритмов обеспечения целостности на базе технологии .Net Framework [Текст] / А.Г.Проценко // Системи обробки інформації: ХУПС. – Х.в, 2011. – Вип. 8(52). – С. 228-232.
5. Гринь Я.В. Аналіз алгоритмів симетричного шифрування даних з точки зору можливості їх поліморфної реалізації [Текст] / Я.В. Гринь // Національний технічний університет України «Київський політехнічний інститут»: Журнал науковий огляд, 2016. – № 5 (26). – С. 1-11.
6. Дослідження основних характеристик алгоритму симетричного шифрування RC5 для побудови модуля захисту розподіленої системи теплового проектування [Текст] / В. Яковина, О. Одуха, М. Сенів, О. Білас // Вісник Національного університету "Львівська політехніка". Комп'ютерні науки та інформаційні технології. – 2008. – № 616. – С. 143-150.
7. Исаев А.Б. Современные технические методы и средства защиты информации: Учеб. пособие. – М.: РУДН, 2008. – 253 с.

8. Efg2.com, Cryptography and Multiple-Precision Arithmetic [Электронный ресурс] / Efg2.com – Режим доступа: http://www.efg2.com/Lab/Library/Delphi / MathFunctions/Cryptography.htm.