УДК 004.896

Т.В. Кімачук, студент гр. 401-ТК,
П.М. Гроза, к.т.н., с.н.с.
Полтавський національний технічний
університет імені Юрія Кондратюка

ДОСЛІДЖЕННЯ АКТУАЛЬНИХ АЛГОРИТМІВ КОДУВАННЯ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

В доповіді представлений аналіз алгоритму криптографічного хешування для захисту персональних даних лінійки SHA.

За для досягнення поставленої мети у роботі було виконано низку завдань:

– досліджено основні методи і засоби захисту інформації;

– проаналізовано сучасний стан розробки програмних засобів захисту персональних даних;

– розкрито особливості застосування крипто примітивів та криптографічних алгоритмів.

Хеш-функції – це функції, призначені для «стиснення» довільного повідомлення або набору даних, записаних, як правило, в двійковому алфавіті, в певну бітову комбінацію фіксованої довжини, яка називається згорткою. Хеш-функції мають різноманітні застосування при проведенні статистичних експериментів, при тестуванні логічних пристроїв, при побудові алгоритмів швидкого пошуку і перевірки цілісності записів в базах даних. Основною вимогою до хеш-функцій є рівномірність розподілу їх значень при випадковому виборі значень аргументу.

Криптографічною хеш-функцією називається будь-яка 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,

– аутентифікації джерела даних.

До ключових функцій хешування пред'являються наступні вимоги:

– неможливість фабрикації,

– неможливість модифікації.

Алгоритми лінійки SHA, на сьогодні є найбільш поширені. Йде активний перехід від SHA-1 до стандартів версії SHA-2. SHA-2 – збірна 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. Використовувати їх слід лише для забезпечення сумісності з устаткуванням старих моделей.

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»). В основі хеш-функції лежить 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 в 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.

В результаті аналізу було встановлено, що на сьогодні SHA-256 – це найбільш 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. Більш того, він законодавчо дозволений для захисту державних даних в США, що доводить його актуальність і значимість.

Отримані результати можуть бути використані у межах організацій для впровадження засобів інформаційної безпеки.

Література

1. Авдошин С.М. Криптотехнологии Microsoft / 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,005 – 528с.

3. Исаев А.Б. Современные технические методы и средства защиты информации: Учебное пособи – М.: РУНД. 2008 – 253с.

4. Гринь Я.В. Аналіз алгоритмів симетричного шифрування даних з точки зору можливості їх поліморфної реалізації . Я.В. Гринь // Національний технічний університет України «Київський політехнічний інститут»: Журнал науковий огляд, 2016 - №5 (26)