прикладами їх застосування в банках, пропуск в приміщення тощо.

Список використаних джерел:

1. Сабынин В. Н. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации // *Информост – радиоэлектроники и телекоммуникации*, 2001. № 3 (16).

Ключові слова: Система управління контролю доступом, контроль, система безпеки, технічні засоби.

Ключевые слова: Сисетема контроля доступа, контроль, система безопастности, технические средства.

Key words: Access control system, control, safety system, technical means.

***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

Золотоверх Денис Олегович
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ ОЗНАК КРИПТОСТІЙКИХ ХЕШ-ФУНКЦІЙ

Хеш-функції надзвичайно корисні і з'являються майже у всіх програмах захисту інформації.

Хеш-функція – це математична функція, яка перетворює числове вхідне значення в інше стиснене числове значення. Вхід у хеш-функцію є довільної довжини, але вихід завжди має фіксовану довжину.

Значення, що повертаються хеш-функцією, називаються дайджестом повідомлення або просто хеш-значеннями.

Хеш функціям притаманні наступні ознаки:

Дайджест фіксованої довжини. Кожна хеш функція може приймати на вході повідомлення довільної довжини, та на виході видавати дайджест однієї, чітко визначеної довжини.

Дайджест може мати будь-яку довжину, якщо розглядати на прикладах найпопулярніших імплементацій хеш функцій (SHA-1, MD-5, SHA-2), то довжина блоку становить зазвичай 160, 256 та 512 біт. Але слід зазначити, що одна хеш функція може працювати у різних режимах, маючи різну довжину даджесту.

З попередньої властивості випливає те, що вихідні дані зазвичай містять меншу кількість інформації, а тому хеш функції також називають функціями стиснення.

Функція хешу покриває дані довільної довжини до фіксованої довжини. Цей процес часто називають хешуванням даних.

Як правило обчислення дайджесту є нескладною операцією з точки зору об'ємів обчислювальних ресурсів. Але обчислення вхідного повідомлення, навпаки є дуже складною задачею, що навпаки вимагає величезну кількість обчислювальних ресурсів.

Але для використання хеш функції як методу захисту інформації, до неї ставляться певні вимоги.

Дайджести хеш функції мають бути рівномірно розподілені, тобто хеш значення має генеруватися у вихідному діапазоні з однаковою рівномірністю, тобто діапазоном є усі значення дайджестів, наприклад для MD5 вихідним діапазоном є значення від 00000000000000000000 до ffffffffffffffff, якщо їх представити у 16-рядковому форматі. А кожний біт дайджесту повинен генеруватися з вірогідністю, що наближається до 50% [1].

Хеш функція повинна приймати дані будь-якого формату, зазвичай алгоритми хешування приймаються масив байтів, що забезпечує їх універсальність.

Хеш функція є детерміністичною, вхідне повідомлення завжди генерує один дайджест. Тобто алгоритми хешування не використовують генератори псевдовипадкових чисел, або певні вхідні дані, які неможливо отримати при повторному використанні алгоритму (наприклад часу доби, атмосферного тиску інше). Також не повинно мати значення адреси

пам'яті об'єкта. Припускається використання зерна генерації або вектору ініціалізації, але зазвичай такі механізми не використовуються.

Ефективність хеш функції є досить важливим аспектом, адже окрім криптографічних методів захисту інформації, вони використовуються для зберігання та пошуку даних. Так наприклад при зберіганні даних простіше зберігати ключ значення файлу, адже його обчислення займає визначений проміжок часу, та не зростає зі збільшенням розміру файлу.

Тому хеш-функції повинні обчислюватись досить швидко, на відміну від алгоритмів блокового симетричного шифрування, що є дуже схожими за будовою та принципом дії. Для цього при обчисленні використовується мінімальна кількість інструкцій. Зазвичай для забезпечення швидкості використовуються прості логічні та арифметичні оператори. Але використання операторів множення і особливо ділення використовуються рідко через їх складність реалізації на апаратному рівні [2].

Одним із визначальних атрибутів алгоритмів хешування є наявність колізій. Колізією є випадок, коли дайджест одного повідомлення є ідентичним до дайджесту іншого. Це пов'язано з тим, що при визначеній довжині дайджесту, існує невизначена кількість можливих повідомлень.

Вірогідність колізії, є незначущою, і у криптостійких алгоритмів хеш-функцій наближається до теоретичного мінімуму. Зазвичай при використанні наявність колізій або ігнорується, або вирішується (наприклад додавання солі при зберіганні хеш-таблиці паролів), але також існує можливість використання ін'єктивної хеш-функції [3].

Вірогідність колізії напряму залежить від довжини дайджесту хеш-функції, але великий розмір ключа напряму негативно впливає на швидкість обичлення.

Як вже було зазначено за принципом дії, алгоритми хешування за механізмом дії на алгоритми блокового симетричного шифрування.

Розмір кожного блоку даних змінюється залежно від алгоритму. Зазвичай розміри блоків становлять від 128 до 512 біт. Якщо повідомлення не «заповнює» блок, створюються відступи.

Над кожним блоком здійснюються визначені операції елементарної логіки та арифметики. Перший блок «перемішується» з вектором ініціалізації, що, зазвичай, чітко визначений алгоритмом. Другий блок «перемішується» з першим і т.д.

У криптографічних функціях необхідна наявність лавинного ефекту, його показником є наявність двох істотно різних дайджестів для повідомлень, які відрізняються одним бітом [4].

Отже, це математична функція яка перетворює числове вхідне значення в інше стиснене числове значення. Хеш функція має повертати дайджест сталої довжини, а довжина повідомлення не має значення. Вона повинна бути швидкою та односторонньою.

Криптографічно стійким вважається алгоритм хешування, якщо в ньому наявні такі ознаки, як рівномірність розподілення дайджестів, детерміністичність, наявність лавинного ефекту, а вірогідність колізії є теоретично мінімальною.

Список використаних джерел:

1. Брюс Шнайер, «Прикладна криптографія» 2е видання Тріумф, 2002

2. Брюс Шнайер. «Прикладна криптографія. Протоколи, алгоритми, вихідні тексти на мові Си» Тріумф, 2002

3. Єршов Ю. Л., Палютін Е. А. Математична логіка: Навчальний посібник. – 3-е, стереотип. изд. – СПб .: Лань, 2004. – 336 с.

4. Кастро та ін., 2005, «Суворий критерій критерію випадковості», Математика та комп'ютери в моделюванні, 2005

Ключові слова: Хеш-функція, колізія хеш-функції, дайджест, шифрування, симетричне шифрування.

Ключивые слова: Хеш-функция, коллизия хеш-функции, дайджест, шифрование, симмнтрическое шифравания.

Key words: Hash-function, hash-function collision, digest, cypher, symmetric cypher.

***Науковий керівник**: д. фіз. - мат. н., професор Василенко М. Д.*