УДК 621.391.7

А. О. Зварич

АНАЛІЗ МОЖЛИВОСТІ ВИКОРИСТАННЯ ЦИКЛІЧНОГО НАДЛИШКОВОГО КОДУ В КРИПТОГРАФІЧНИХ ШИФРАХ ДЛЯ ПІДВИЩЕННЯ ЇХ КРИПТОСТІЙКОСТІ

Вінницький національний технічний університет

Анотація

В роботі розглянуто та детально проаналізовано можливість використання математичного апарату циклічного надлишкового коду в криптографічних шифрах для підвищення їх криптостійкості. Описано основні властивості контрольних сум та використання їх для захисту даних.

Ключові слова: циклічний надлишковий код, криптографія, криптостійкість, контрольна сума.

Abstract

The possibility of using the mathematical apparatus of the cyclic redundancy code in cryptographic ciphers in order to increase their cryptographic stability is considered and thoroughly analyzed. The basic properties of checksums and their use for data protection are described.

Keywords: cyclic redundancy code, cryptography, cryptoscope, checksum.

Вступ

Криптографія призначена для передачі захищених даних через незахищену мережу в зашифрованому варіанті, щоб лише один із користувачів, якому призначена ця інформація, міг проаналізувати його. Зв'язок через повідомлення, електронні листи або різні інші режими вимагає високої безпеки. Отже, на сьогоднішній день є дуже важливо вжити заходи для захисту ключових елементів та забезпечення конфіденційності інформації.

Метою роботи є аналіз можливості використання циклічного надлишкового коду в криптографічних шифрах для підвищення їх криптостійкості.

Результати дослідження

Контрольна сума – деяке значення, розраховане по набору даних шляхом застосування певного алгоритму і використовується для перевірки цілісності даних при їх передачі або зберіганні. Також контрольні суми можуть використовуватися для швидкого порівняння двох наборів даних на нееквівалентність: з великою ймовірністю різні набори даних матимуть нерівні контрольні суми. Це може бути використано, наприклад, для виявлення комп'ютерних вірусів. Незважаючи на свою назву, контрольна сума не обов'язково обчислюється шляхом підсумовування.

З точки зору математики контрольна сума є результатом хеш-функції, використовуваної для обчислення контрольного коду - невеликої кількості біт всередині великого блоку даних, наприклад, мережевого пакету або блоку комп'ютерного файлу, що застосовується для виявлення помилок при передачі або зберіганні інформації. Значення контрольної суми додається в кінець блоку даних безпосередньо перед початком передачі або запису даних на будь-який носій інформації. Згодом воно перевіряється для підтвердження цілісності даних.

Популярність використання контрольних сум для перевірки цілісності даних зумовлена тим, що подібна перевірка легко реалізовується в двійковому цифровому обладнанні, легко аналізується і добре підходить для виявлення загальних помилок, викликаних наявністю шуму в каналах передачі даних.

Класифікувати алгоритми розрахунку контрольної суми можна таким чином:

1. Циклічний надлишковий код (зокрема, CRC8, CRC16, CRC32) застосовується для перевірки цілісності передачі даних. Така контрольна сума проста в реалізації і забезпечує низьку ймовірність виникнення колізій.
2. MD5 і інші криптографічні хеш-функції використовуються, наприклад, для підтвердження цілісності та автентичності переданих даних. Одна з найпопулярніших криптографічних функцій MD5 вже майже не використовується для визначення контрольних сум, так як виявилося, що для неї можна

швидко створювати два різних файли, що мають різну довжину в байтах, але однакові величини контрольних сум, підрахованих за допомогою алгоритму MD5.

Циклічний надлишковий код (CRC) - алгоритм знаходження контрольної суми, призначений для перевірки цілісності даних. CRC є практичним застосуванням завадостійкого кодування, заснованим на певних математичних властивостях циклічного коду.

У загальному вигляді контрольна сума являє собою деяке значення, обчислене за певною схемою на основі кодованого повідомлення. Перевірочна інформація при систематичному кодуванні приписується до переданих даних. На приймаючій стороні абонент знає алгоритм обчислення контрольної суми: відповідно, програма має можливість перевірити коректність прийнятих даних.

При передачі пакетів з мережевого каналу можуть виникнути спотворення вихідної інформації внаслідок різних зовнішніх впливів: електричних наводок, погані погодні умови і багатьох інших. Сутність методики в тому, що при хороших характеристиках контрольної суми в переважній кількості випадків помилка в повідомленні призведе до зміни його контрольної суми. Якщо вихідна і обчислена суми не рівні між собою, приймається рішення про недостовірність прийнятих даних, і можна запросити повторну передачу пакета.

Циклічні надлишкові коди є частиною стандартів, найпопулярніший і рекомендований IEEE поліном для CRC-32 використовується в Ethernet, FDDI, крім того цей многочлен є генератором коду Хеммінга.

Оцінюючи швидкодію алгоритму CRC-32, можна зробити висновки, що він є значно швидшим за криптографічні хеш-функції. Так, наприклад, для файлу розміром 1 Мб, час знаходження контрольної суми алгоритмом CRC-32 є 0.009 секунди, тоді коли алгоритму SHA-1 необхідно 0.022. Розмір контрольної суми алгоритма CRC-32 є в 5 разів меншим.

Таким чином, використовуючи циклічні надлишкові коди для перевірки вхідного шифротексту чи ключів, значно підвищується криптостійкість самого алгоритму шифрування інформації.

Висновки

У даній роботі було детально проаналізовано математичний апарат циклічного надлишкового коду. Описані його основні властивості та переваги. Обґрунтовано можливість його використання для підвищення стійкості криптографічних шифрів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гулак Г. М. Основи криптографічного захисту інформації / Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук – Вінниця, 2011 – 199 с.

2. Азаров О. Д.. Комп'ютерна криптографія / Азаров О. Д., Хорошко В. О., Шєлєст М. Є., Мухачьов В. А., Яремчук Ю. Є. - НАУ, 2003 – 14 с.

3. Ю. Є. Яремчук. Сучасний захист інформації / Ю.Є. Яремчук, А. П. Бондарчук, С. Я. Довбня, Ю. І. Хлапонін – Вінниця, 2013.

4. Cryptography [Electronic Resource]. – Mode of access : URL : https://en.wikipedia.org/wiki/Cryptography - Назва з екрану.

5. Strong cryptography [Electronic Resource]. – Mode of access : URL : https://en.wikipedia.org/wiki/Strong_cryptography - Назва з екрану.

Зварич Андрій Олександрович — магістр, Вінницький національний технічний університет, Вінниця, e-mail: andrii1996z@gmail.com.

Науковий керівник: ***Яремчук Юрій Євгенович*** — доктор технічних наук, професор, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця.

Zvarych Andrii Olexandrovych — master degree, Vinnitsa National Technical University, Vinnitsa, e-mail: andrii1996z@gmail.com.

Supervisor: ***Yaremchuk Yuriy E***. — Ph. D., professor, management and security of information Systems department; Vinnitsa.