УДК 004.8

О. В. Лесик
В. І. Месюра

АНАЛІЗ МЕТОДІВ ШИФРУВАННЯ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

Метою даної роботі є розгляд та оцінка сучасних методів аналізу та шифрування інформації в області "мобільне шифрування та дешифрування інформації" виявлення проблематики, розробка інформаційної технології.

Ключові слова: шифрування, дешифрування, криптографія.

Abstract

The purpose of this work is to review and evaluate modern methods of analysis and encryption of information in the field of "mobile encryption and decryption of information" problem identification, development of information technology.

Keywords: encryption, decryption, cryptography.

Вступ

З розвитком інформаційного суспільства стрімко зростають інформаційні потоки, а з ними зростає і важливість шифрування інформації, яка, як і дані, потребує захисту. Завдяки шифруванню забезпечується її цілісність і гарантується «недоторканість», коли доступ до певної інформації може мати тільки конкретний адресат, у якого є ключ для її дешифрування. А оскільки мережею Інтернет передається велика кількість конфіденційної інформації, то її потрібно вберегти від несанкціонованого доступу. В цьому і полягає основна ціль шифрування і мета даної роботи.

Криптографія - наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації [1]. Вона розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри та теорії ймовірностей [2].

Тривалий час під криптографією розумілось лише шифрування - процес перетворення звичайної інформації (відкритого тексту) в незрозуміле «сміття».

Дешифрування - зворотний процес відтворення інформації з зашифрованого тексту. Шифром називається пара алгоритмів шифрування/дешифрування.

Результати досліджень

Сучасні дослідження симетричних алгоритмів шифрування зосереджені, в основному, навколо блочних та потокових алгоритмів шифрування та їхнього застосування. Блочний шифр подібний до поліалфавітного шифру Альберті: блочні шифри отримують фрагмент відкритого тексту та ключ, і видають на виході шифротекст такого самого розміру. Оскільки повідомлення зазвичай довші за один блок, потрібен деякий метод склеювання послідовних блоків. Було розроблено декілька методів, що відрізняються в різних аспектах. Вони є режимами дії блочних шифрів та мають обережно обиратись під час застосування блочного шифру в криптосистемі.

Потокові шифри, на відміну від блочних, створюють ключ довільної довжини, що накладається на відкритий текст побітово або політерно, в дечому подібно до одноразової дошки. В потокових шифрах, потік шифротексту обчислюється на основі внутрішнього стану алгоритму, який змінюється протягом його дії. Зміна стану керується ключем, та, в деяких алгоритмах, ще і потоком відкритого тексту. Одним з прикладів добре відомого, та широко розповсюдженого потокового шифру є RC4 [3].

Інформація, що може бути прочитана, осмислена і зрозуміла без яких-небудь спеціальних заходів, називається відкритим текстом (plaintext, clear text). Метод перетворення відкритого тексту таким чином, щоб сховати його суть, називається зашифруванням (encryption або enciphering). Шифрування

відкритого тексту приводить до його перетворення в незрозумілу абракадабру, іменовану шифротекстом (cipЬегїехї). Шифрування дозволяє сховати інформацію від тих, для кого вона не призначається, попри те, що вони можуть бачити сам шифротекст [1]. Протилежний процес перетворення шифротексту в його вихідний вид називається розшифруванням (decryption або deciphering).

Для встановлення криптографічного зв'язку за допомогою симетричного алгоритму, відправникові й одержувачеві потрібно попередньо погодити ключ і тримати його в таємниці. Якщо вони знаходяться в географічно віддалених місцях, то повинні вдатися до допомоги довіреного посередника, наприклад, надійного кур'єра, щоб уникнути компрометації ключа в ході транспортування. Зловмисник, що перехопив ключ на шляху, зможе пізніше читати, змінювати і підробляти будь-яку інформацію, зашифровану або завірену цим ключем. Глобальна проблема симетричних шифрів (DES і AES) полягає в складності керування ключами.

В основному, симетричні алгоритми шифрування вимагають менше обчислень, ніж асиметричні. На практиці, це означає, що якісні асиметричні алгоритми в сотні або в тисячі разів повільніші за якісні симетричні алгоритми. Недоліком симетричних алгоритмів є необхідність мати секретний ключ з обох боків передачі інформації. Так як ключі є предметом можливого перехоплення, їх необхідно часто змінювати та передавати по безпечних каналах передачі інформації під час розповсюдження.

Висновок

В даній роботі були виявлені переваги і недоліки використання кожного з алгоритмів шифрування. Проведений аналіз дослідженої інформації привів до висновку, що для вирішення задачі шифрування/дешифрування інформації найкраще підходить використання алгоритму симетричного шифрування.

Симетричне шифрування має низку переваг. Перше - швидкість криптографічних операцій. Воно особливо корисне для шифрування даних, що залишаються у нас. Однак, симетричне шифрування, використане саме по собі як засіб захисту коштовних даних, що пересилаються, може виявитися досить витратним просто через складність передачі таємного ключа.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с.

2. Дошина А. Д., Михайлова А. Е., Карлова В. В. Криптография. Основные методы и проблемы. Современные тенденции криптографии [Текст] //Современные тенденции технических наук: материалы IV междунар. науч. конф. (г. Казань, октябрь2015 г.). – Казань: Бук, 2015.

3. Мао Венбо. Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice. – М.: Вильямс, 2005. – 768 с. – 2 000 экз. – ISBN 5-8459-0847-7, ISBN 0-13-066943-1

Лесик Олександр Валентинович *— студент групи 1КН-18МС, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, E-mail: sasha.lesik.98@gmail.com;*

Месюра Володимир Іванович — канд. техн. наук, професор кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця, e-mail: mesyura@vntu.edu.ua.

Lesyk Oleksander V. - student of the Computer Science Department, Faculty of Information Technology and Computer Engineering, Vinnitsa National Technical University, Vinnitsa, E-mail:sasha.lesik.98@gmail.com;

Mesyura Volodymyr I. — Cand. Sc. (Eng.), Professor of Computer Science Department, Vinnitsa National Technical University, Vinnytsia, e-mail: mesyura@vntu.edu.ua.