УДК 518.681

Благодир М.Л.
Перевозніков С.І.

КРИПТОГРАФІЧНИЙ ЗАХИСТ ЦИФРОВОЇ ІНФОРМАЦІЇ

Вінницький Національний Технічний Університет

Анотація

В роботі проаналізовано особливості використання різних методів криптографічного захисту цифрової інформації. Описано основні переваги та недоліки розглянутих методів. Доведено доцільність модифікації RSA-стандарту для підвищення криптостійкості кодування.

Ключові слова

Криптографічний захист, Криптостійкість, Кодування, Захист інформації.

Abstract

In the work analyzes the peculiarities of using different methods of cryptographic protection of digital information. The main advantages and disadvantages of the considered methods are described. The expediency of modification of the RSA-standard for increasing the cryptographic stability of the coding has been proved.

Keywords

Cryptographic protection, Cryptographic stability, Encoding, Information security.

Розвиток комп'ютерної техніки і її широке впровадження в різні сфери людської діяльності викликав зростання числа протизаконних дій, об'єктом або знаряддям здійснення яких є електронно-обчислювальні машини. Шляхом різного роду маніпуляцій, тобто внесення змін до інформації на різних етапах її обробки, в програмне забезпечення, оволодіння інформацією нерідко вдається отримувати значні суми грошей, ухилятися від оподаткування, займатися промисловим шпигунством, знищувати програми конкурентів і т.д. [1].

Системний підхід до захисту інформації вимагає, щоб засоби і дії, використовувані для забезпечення інформаційної безпеки – організаційні, фізичні і програмно-технічні – розглядалися як єдиний комплекс взаємозв'язаних, вза’ємодоповнюючих і взаємодіючих заходів. Один з основних принципів системного підходу до безпеки інформації - принцип "розумної достатності", суть якого: стовідсоткового захисту не існує ні за яких обставин, тому прагнути варто не до теоретично максимально досяжного рівня захисту, а до мінімально необхідного в даних конкретних умовах і при даному рівні можливої загрози.

Поява нових потужних комп'ютерів, технологій мережевих і нейронних обчислень зробило можливою дискредитацію криптографічних систем що ще недавно вважалися практично не розкриваними. В даній роботі проаналізовано RSA-алгоритм, який не порушує головний принцип криптосистем - секретність шифрів заснована на секретності ключа.

Основні напрями використання криптографічних методів - передача конфіденційній інформації по каналах зв'язку (наприклад, електронна пошта), встановлення достовірності передаваних повідомлень, збереження інформації (документів, баз даних) на носіях в зашифрованому вигляді.

Цілочисельна факторизація (IFP): RSA.

Цілочисельна факторизація (IFP): знаходить p і q, враховуючи складене число n, яке є добутком двох великих простих чисел p і q [2].

Виявлення великих простих чисел - відносно просте завдання, а проблема розкладання на множники, добутки двох таких чисел є надто важкою.
Дискретний логарифм (процесор передачі даних).
Якщо p - просте число, то Zp позначає набір цілих чисел 0, 1, 2..., p - 1, де складання і амплітудне спотворення - виконуються з модулем. Відомо, що існує ненульовий елемент O Zp такий, що кожен ненульовий елемент в Zp може бути написаний як потужність a, такий елемент називається генератором Zp.
Еліптична крива дискретного логарифму (ECDLP) полягає в наступному: враховуючи еліптичну криву E визначену по Fq, точка POE (Fq) порядку n, і точки QOE (Fq), визначаються цілим числом 0, l, 2..., n - 1, так що Добротність = lP, за умови, що таке ціле число існує.
Криптографічний захист двійкової інформації здійснюється шляхом перетворення вихідного (відкритого) тексту в зашифроване повідомлення по відомому алгоритму за допомогою секретних ключових послідовностей [3].
Згідно технічного завдання максимальна довжина пароля може складати 16 байт = 128 біт, що дає можливу кількість паролів 2128, що значно перевершує усі відомі методи.
Ключова послідовність відповідно являє собою процедурно формований 128 розрядний код на підставі 16-ти байтового пароля (відомого обмеженому колу осіб) і сукупності значень числа місяця і дня тижня. Вихідна інформація для формування ключової послідовності заноситься в змінне ПЗУ.
В результаті проведеного аналізу існуючих методів шифрування інформації визначені їхні недоліки, розглянуті шляхи їх усунення шляхом модифікації відомого RSA-стандарту та розробки удосконаленого методу захисту пароля від підбора та розголошення.
Вдала модифікація RSA-стандарту дозволила для шифрування і дешифрування використовувати той самий алгоритм, що значно спрощує його реалізацію.
Використаний алгоритм RSA має ряд переваг:
- алгоритм RSA є асиметричним, тобто він грунтується на розповсюдженні відкритих ключів в мережі. Це дозволяє декільком користувачам обмінюватися інформацією, що посилається по незахищених каналах зв'язку;
- користувач сам може змінювати відкритий і закритий ключ. Це дозволяє добиватися користувачеві потрібної йому криптостійкості.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Криптографія. [Електронний ресурс]. Режим доступу: http://uk.wikipedia.org/wiki/ Криптографія. (дата звернення 20.03.2018). — Назва з екрану.
2. 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. Дошина А. Д., Михайлова А. Е., Карлова В. В.
3. Криптография. Основные методы и проблемы. Современные тенденции криптографии [Текст] // Современные тенденции технических наук: материалы IV междунар. науч. конф. (г. Казань, октябрь 2015г.). – Казань: Бук, 2015.

Благодир Марина Леонідівна – студентка групи 2КН-14б, ФІТКІ, Вінницький національний технічний університет, м. Вінниця, Хмельницьке шосе 95, e-mail: blagodyr.m@gmail.com
Перевозніков Сергій Іванович - д.т.н., професор кафедри комп'ютерних наук, ФІТКІ, Вінницький національний технічний університет, м. Вінниця, Хмельницьке шосе 95, e-mail:perevoznikov@ukr.net

Maryna L. Blagodyr – student group 2KH-14, FISCE, Vinnitsa National Technical University, Vinnitsa, Khmelnitsky highway 95, e-mail: blagodyr.m@gmail.com
Serhiy I. Perevoznikov - Doctor of Engineering, professor of the department of Computer Science, FISCE, Vinnytsia National Technical University, Vinnytsia, Khmelnitsky highway 95, e-mail:perevoznikov@ukr.net