УДК 004.4'277.2.056.55

А. О. Азарова
Р. О. Крохмаль

ВИКОРИСТАННЯ КРИПТОАЛГОРИТМУ ШИФРУВАННЯ DESX ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Вінницький національний технічний університет

Анотація

Розглянуто базові поняття криптографічного шифрування. Авторами запропоновано використання алгоритму шифрування DES як блочного шифру з симетричним ключем DES, що уможливлює підвищення складності атаки грубої сили та захисту інформації від несанкціонованого доступу.

Ключові слова: шифрування, алгоритму шифрування DES, симетричний ключ, захист інформації, несанкціонований доступ.

Abstract

Basic concepts of cryptographic encryption are considered. The authors propose to use the DES encryption algorithm as a block cipher with a symmetric DES key, which allows to increase the complexity of the brute force attack and protect information from unauthorized access.

Keywords: encryption, DES encryption algorithm, symmetric key, information security, unauthorized access.

Вступ

У криптографії процес шифрування є процесом кодування інформації. Він перетворює вихідне інформаційне повідомлення – відкритий текст – на альтернативну його форму – зашифрований текст. Згідно процедури шифрування лише уповноважені сторони мають можливість розшифрувати зашифрований текст, перетворити його на відкритий текст і отримати доступ до вихідної інформації. Сама процедура шифрування не дозволяє потенційному перехоплювачу отримати зрозумілий вміст інформації, що зашифрована.

Слід відзначити, що для вирішення проблем криптографічного захисту інформації доволі ефективним засобом є саме шифрування. Перші методи шифрування застосовувалися для вирішення проблем захисту військових повідомлень. Це уможливило розвиток таких підходів, що стали сьогодні широко застосовуваними в усіх галузях людської діяльності, зокрема, концепції відкритого та симетричного ключа у схемах шифрування.

У контексті криптографії шифрування служить механізмом забезпечення конфіденційності. Оскільки дані можуть бути видимими в Інтернеті, конфіденційна інформація, така як паролі та особисте спілкування, може бути піддана потенційним перехоплювачам. Процес шифрування та дешифрування повідомлень пов’язаний із застосуванням ключів у криптографічних системах: симетричний ключ і відкритий ключ (також відомий як асиметричний ключ).

У схемах із симетричними ключами ключі шифрування та дешифрування однакові. Сторони, що спілкуються, повинні мати однаковий ключ, щоб забезпечити безпечне спілкування. Німецька машина Enigma щодня використовувала новий симетричний ключ для кодування та декодування повідомлень.

Шифрування з відкритим ключем було вперше описане в секретному документі в 1973 р. У схемах шифрування з відкритим ключем ключ шифрування публікується для використання та шифрування повідомлень будь-ким. Однак, лише сторона, яка отримує, має доступ до ключа дешифрування, який дозволяє читати повідомлення.

Раніше всі схеми шифрування були із симетричним ключем (також званим закритим ключем). Знаковою в теорії шифрування стала робота Діффі та Хеллмана, метод яких став відомим як обмін ключами Діффі-Хеллмана.

Шифрування вже давно використовується військовими та урядами для полегшення таємного спілкування. Зараз воно широко використовується для захисту інформації в багатьох видах цивільних систем. Шифрування можна використовувати для захисту даних, що знаходяться в стані спокою,

наприклад інформації, що зберігається на комп'ютерах і пристроях зберігання даних (наприклад, USB-флеш-накопичувачі). Системи керування цифровими правами, які запобігають несанкціонованому використанню або відтворенню матеріалів, захищених авторським правом, і захищають програмне забезпечення від зворотного інжинірингу, є іншим прикладом використання шифрування даних, що зберігаються.

Основна частина

Стандарт шифрування даних – це алгоритм із симетричним ключем для шифрування цифрових даних. Хоча його коротка довжина ключа в 56 біт робить його занадто небезпечним для додатків, він мав великий вплив на розвиток криптографії.

DES – це архетиповий блочний шифр – алгоритм, який бере рядок бітів відкритого тексту фіксованої довжини і перетворює його на інший бітовий рядок зашифрованого тексту такої ж довжини. Алгоритм було розроблено на початку 1970-х років фірмою IBM, він базувався на розробці Хорста Файстеля. У випадку DES розмір блоку становить 64 біта. DES також використовує ключ для налаштування перетворення, щоб розшифровка виконувалася лише тими, хто знає конкретний ключ, що використовується для шифрування. Ключ складається з 64 біт, однак лише 56 із них фактично використовуються алгоритмом. Вісім бітів використовуються виключно для перевірки парності, а потім відкидаються. Отже, ефективна довжина ключа становить 56 біт.

У криптографії відбілювання ключа – це техніка, призначена для підвищення безпеки повторюваного блочного шифру, що складається з кроків, які об'єднують дані з частинами ключа.

У криптографії DES-X (або DESX) – це варіант блочного шифру із симетричним ключем DES (стандарт шифрування даних), призначеним для підвищення складності атаки грубої сили за допомогою техніки, що називається відбілюванням ключа [1]. Оригінальний алгоритм DES був визначений в 1976 р. із розміром ключа 56 біт: 256 можливостей для ключа. DESX доповнює DES шляхом XOR, додаючи додаткові 64 біти ключа (K1) до відкритого тексту, перед застосуванням DES, а потім XOR, використовуючи ще 64 біти ключа (K2) після шифрування. Застосування DESX також підвищує міцність DES проти диференційного криптоаналізу та лінійного криптоаналізу, хоча покращення набагато менше, ніж у випадку атак грубої сили. Доведено, що для диференційного криптоаналізу знадобиться 261 вибраний відкритий текст (проти 247 для DES), тоді як для лінійного криптоаналізу знадобиться 260 відомих відкритих текстів (проти 243 для DES або 261 для DES з незалежними підключами) [2].

Хоча диференційні та лінійні атаки на даний момент є найбільшою атакою на DES-X, є атака слайдів із відомим відкритим текстом, виявлена Бірюковим-Вагнером, яка має складність 232,5 відомих відкритих текстів і 287,5 часу аналізу. Крім того, атака легко перетворюється на атаку лише зашифрованого тексту з такою ж складністю даних і 295 офлайн-часовою складністю.

Висновки

Авторами було вивчено поняття захисту інформації на основі шифрування, алгоритм шифрування DES, метод відбілювання ключа та алгоритм шифрування інформації DESX. Було доведено доцільність застосування криптоалгоритму шифрування DESX, що представляє собою алгоритм DES із методом відбілювання ключа.

Отже, у даному дослідженні було обґрунтовано актуальність використання криптоалгоритму шифрування DESX для захисту інформації від несанкціонованого доступу.

Список використаної літератури

1. Столінгс В. Криптографія та захист мереж: принципи та практика: посібник. Харків, 2017.
2. Рябко Б. Я., Фіонов О. М. Криптографічні методи захисту інформації.

Азарова Анжеліка Олексіївна − к.т.н., професор кафедри МБІС Вінницького національного технічного університету, м. Вінниця, e-mail: azarova.angelika@gmail.com

Крохмаль Роман Олександрович – ст. гр. КІТС-18б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: romakrohmal23455@gmail.com

Azarova Anzhelika A. – PhD in technique, professor of department of Management and information security of Vinnytsia National Tecnical University, Vinnytsia, e-mail: azarova.angelika@gmail.com

Krokhmal Roman O. - student, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: romakrohmal23455@gmail.com