УДК 044.056

АНАЛІЗ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Савич Ю.О., к.т.н., доцент Вовк Р.Б., к.т.н., доцент Пасєка М.С.
Івано-Франківський національний технічний університет нафти і газу, http://nung.edu.ua/,
E-mail: julliasavych@gmail.com

В даному дослідженні виконано аналітичний огляд методів застосування криптографічного та стеганографічного захисту інформації в програмних додатках та комп'ютерних системах. Проведено групування алгоритмів шифрування даних на дві групи з подальшим їх аналізом та описом перспектив використання.

Ключові слова – криптографія, стеганографія, алгоритм, програма, алгоритм шифрування, стійкість.

ВСТУП

Проблема захисту інформаційних ресурсів набуває все більш важливого значення, хоча вона є однією із найскладніших задач. В першу чергу, це пояснюється прискореними темпами науково-технічного прогресу, результатом якого є нові технічні та електронні засоби, які становлять небезпеку виникнення каналів витоку інформації. Також одним із факторів, які визначають трудомісткість вирішення завдань захисту інформації, є розширення кола користувачів, що мають доступ до ресурсів комп'ютерної системи і масивів даних, які знаходяться в ній.

Для вирішення цієї проблеми потрібна система заходів, головною ціллю якої є попередження від несанкціонованого доступу, наслідком якого може бути втрата, модифікація і витік інформації. Проведений аналіз літератури [1-3] показав, що серед багатьох організаційних, програмних і системних мір криптографія є одним з основних інструментів, що забезпечують секретність і цілісність інформації, авторизацію, електронні платежі, оперативний контроль за процесами управління й обробки даних.

Швидкий розвиток інформаційних технологій привів до нових досягнень в сфері безпеки інформації, яка є дуже важливою для сучасного суспільства. Питання розроблення та впровадження методів захисту інформації є актуальними не лише для криптографії та стеганографії, а й для майже всіх галузей науки, враховуючи високу автоматизацію різних сфер людської діяльності. До початку XX століття криптографія була пов'язана з лінгвістичними схемами. Довгий час криптографія залишалася секретною діяльністю спецслужб і державних структур. Вона також сприяла розвитку електронно-обчислювальної техніки – перші такі машини були створені для злому шифрів військових [1]. Перетворившись на загальнопоширений інструмент передачі та захисту даних, сучасна криптографія базується на математичному апараті, що включає теорію ймовірності та абстрактну алгебру. Основним завданням математики в криптографії є забезпечення криптографічної стійкості, тобто здатності протистояти практичному злому. Криптографічна стійкість визначається кількістю затраченого часу і ресурсів, щоб із шифр тексту відновити вихідний відкритий текст. Результатом стійкої криптографії є шифртекст, що винятково складно зламати без володіння визначеними інструментами по дешифруванню.

ОСНОВНА ЧАСТИНА

Криптографія – наука про способи перетворення інформації з метою її захисту від несанкціонованого доступу. Одним із видів такого перетворення є шифрування, яке забезпечує практичну неможливість читання або модифікації інформації зловмисниками. Існує цілий ряд алгоритмів шифрування даних, які можна розбити на дві великі групи, що показано на рис. 1.

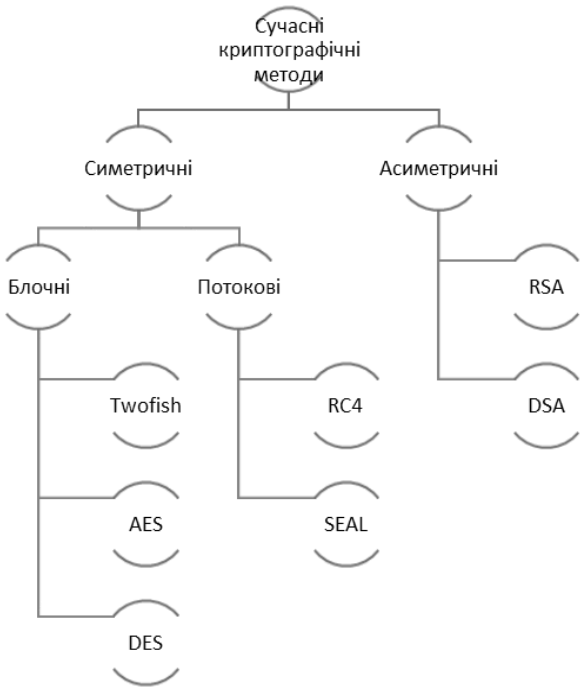

Рисунок 1. Алгоритми криптографії

Проведемо порівняльний аналіз симетричної та асиметричної криптографії. Характерною рисою симетричної системи є використання одного і того ж ключа для виконання операції шифрування і розшифрування, яке можливе лише тоді, якщо існує безпечний канал передачі інформації. Це не стосується військової справи, розвідки, фінансово-кредитних операції тощо. У таких ситуаціях використовують асиметричні алгоритми шифрування. Дані системи криптографічних перетворень характеризуються тим, що для шифрування даних

використовується один ключ (відкритий, тобто доступний користувачам), а для розшифрування – інший (секретний) ключ. Ця властивість дозволяє в певній мірі вирішити проблему розподілу ключів між користувачами, яка є основним недоліком симетричних систем. Для гарантії захисту даних, до асиметричних систем шифрування ставляться дві найважливіші умови [2]:

- перетворення відкритого тексту повинно бути незворотнім і виключати його відновлення на основі відкритого ключа;
- визначення секретного ключа на основі відкритого має бути неможливим для сучасного рівня розвитку обчислювальних засобів.

Вирішення задач автентифікації, розповсюдження ключів відкритими каналами зв'язку, застосування електронного підпису реалізується лише засобами асиметричної криптографії. Однак слід зазначити, що алгоритми асиметричних криптосистем настільки трудомісткі в порівнянні зі звичайними симетричними алгоритмами, що на практиці раціонально їх використовувати там, де обсяг шифрованого інформації незначний, але дуже важливий. Практичний досвід показує, що застосування асиметричних алгоритмів шифрування не дозволяє забезпечити інтерактивний режим роботи сучасних інформаційно-телекомунікаційних систем. Таким чином, очевидна необхідність використання в таких системах пристроїв шифрування, які побудовані на симетричних криптографічних алгоритмах.

Симетричні алгоритми шифрування можна розділити на потокові та блочні. Потокові алгоритми шифрування послідовно обробляють текст повідомлення, блочні алгоритми, в свою чергу, працюють з блоками фіксованого розміру. Як правило, довжина блоку дорівнює 64 бітам, але, в алгоритмі AES використовуються блоки довжиною 128 біт. Симетричні алгоритми шифрування не завжди використовуються самостійно. В сучасних криптоситемах, використовуються комбінації симетричних та асиметричних алгоритмів, для того, аби отримати переваги обох схем. До таких систем належить SSL, PGP та GPG. Асиметричні алгоритми використовуються для розповсюдження ключів швидших симетричних алгоритмів. До деяких відомих, поширених алгоритмів з гарною репутацією належать: Twofish, Serpent, AES, Blowfish, CAST5, RC4 та IDEA [3].

В цілому ряді задач для повноцінного забезпечення інформаційної безпеки використання лише криптографічних методів є недостатнім, оскільки вони не дозволяють приховати власне факт передачі й зберігання конфіденційної інформації. Подібні задачі можливо вирішувати з застосуванням методів крипто-стеганографічних алгоритмів. Крипто-стеганографічна система захисту інформації – це складний інформаційний комплекс методів та засобів, загальна стійкість якого залежить від правильного узгодження криптографічної і стеганографічної складових системи. Ключову роль при цьому відіграють алгоритми узгодження, які дають змогу перетворити рівномірно розподілені бітові послідовності, отримані на виході криптографічних алгоритмів, на бітові послідовності, аналогічні тим, що використовуються для вкраплення стеганографічними алгоритмами у пусті контейнери. Вимогою коректного використання цих алгоритмів є точна статистична відповідність вхідних і вихідних даних. Інтеграція крипто-стеганографічних алгоритмів дає можливість позбутися вразливих сторін відомих методів захисту інформації та розробити ефективніші з позицій обчислювальної складності і стійкості до зламу нові методи розв'язання задач інформаційної безпеки як програмного додатку так і інформаційних потоків даних.

ВИСНОВОК

Автоматизація призводить до зростання загроз несанкціонованого доступу до інформації, як наслідок, до необхідності постійної підтримки і розвитку системи захисту. Захист інформації є не разовим заходом і навіть не сукупністю заходів, а безперервним процесом, який повинен реалізовуватися на всіх етапах життєвого циклу автоматизованої системи обробки інформації. Підвищення продуктивності обчислювальної техніки і поява нових видів атак на шифри веде до зниження стійкості відомих криптографічних алгоритмів. Таким чином, використовувані криптографічні засоби повинні постійно оновлюватися. Підтримка і забезпечення надійного функціонування механізмів системи захисту інформації може здійснюватися лише висококваліфікованими фахівцями, які можуть гарантувати надійність використовуваних алгоритмів і програмних засобів, що реалізують функції захисту інформації.

Отже, в пропонованому дослідженні виконано порівняльний аналіз методів криптографічного захисту інформації, наведена їх класифікація, визначено переваги та недоліки і здійснено опис практичного використання описаних методів у різних системах.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

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. Дошина А. Д., Михайлова А. Е., Карлова В. В.

2. Криптография. Основные методы и проблемы. Современные тенденции криптографии [Текст] // Современные тенденции технических наук: материалы IV междунар. науч. конф. (г. Казань, октябрь 2015 г.). – Казань: Бук, 2015.

3. Венбо Мао 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