Панчук Б. В., магістрант,
спеціальність «Комп'ютерна інженерія»,
Гапак О. М., доцент кафедри комп'ютерних систем та мереж
Ужгородський національний університет

ДОСЛІДЖЕННЯ ШВИДКОСТІ, СТІЙКОСТІ ТА НАДІЙНОСТІ ГІБРИДНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Сьогодні, у добу інформаційних технологій постійно вдосконалюються технології та зростає об'єм інформації. Особливо актуальною є проблема передачі конфіденційних даних незахищеними каналами зв'язку, наприклад, через Інтернет. Для досягнення оптимальної швидкодії та надійності системи захисту інформації можна використати гібридний метод шифрування, який поєднує в собі асиметричне та симетричне шифрування. Метою роботи є дослідження параметрів гібридної криптографічної системи, а також вивчення можливості збільшення рівня захисту шляхом зміни параметрів системи.

У роботі розглядається криптосистема, що реалізує гібридний метод шифрування, який дозволяє двом сторонам передавати зашифровану інформацію без використання захищеного каналу для передачі ключів. Особливість методу полягає в тому, що разом з асиметричним алгоритмом використовується декілька симетричних алгоритмів, кожен з яких накладається послідовно, шар за шаром. Тому, в разі компрометації одного з симетричних алгоритмів, інформація буде захищена іншими. З точки зору швидкодії оптимально використовувати 3 шари симетричних алгоритмів. У запропонованому методі використовуються симетричні алгоритми *DESX, Serpent, Twofish*, та асиметричний алгоритм *RSA*. Для кожного шару генерується новий надійний випадковий пароль, який зашифровується за допомогою *RSA*. Такий ключ вирівнюється до 512 біт та записується в початок зашифрованих даних. При розшифруванні ключ зчитується з початку зашифрованих даних, розшифровується секретним ключем та використовується для дешифрування.

Опис алгоритму:

1. Стороною *X* генерується пара з відкритого та секретного ключа.
2. Відкритий ключ передається незахищеним каналом стороні *Y*, яка має надсилати конфіденційні дані стороні *X*.
3. Сторона *Y* генерує випадковий ключ для симетричного криптографічного алгоритму та зашифровує ним інформацію.
4. За допомогою відкритого ключа на стороні *X* ініціалізується асиметричний алгоритм, ним шифрується згенерований випадковий симетричний ключ, який додається до зашифрованої інформації.
5. Сторона *X* отримує зашифровану інформацію від сторони *Y* та ініціалізує асиметричний алгоритм. Симетричний ключ екстрагується з прийнятої інформації та дешифрується секретним ключем.
6. Решта даних розшифровується симетричним алгоритмом за допомогою дешифрованого симетричного ключа стороною *X*.

Для реалізації системи обрано мову програмування *C#* та середовище розробки – *Microsoft Visual Stusio 2013*.

Висновки

При використанні гібридного методу шифрування значно підвищується надійність передавання даних незахищеними каналами. З цієї причини вирішено оцінити надійність реалізованої системи. Водночас, при передачі ключів іншій стороні забезпечується прийнятна швидкодія та криптостійкість роботи всього комплексу з чотирьох задіяних алгоритмів. Однак, у поточному варіанті алгоритму все ж є певна ймовірність проведення атаки зловмисником на систему передачі. Через це вирішено оцінити реалізовану систему, і вивчити можливість підвищення параметрів захисту даних. У розробленому методі використання декількох шарів шифрування симетричними алгоритмами забезпечує захист даних навіть при компрометації одного з них. У подальшому дослідженні, будуть збільшені довжини ключів складових алгоритмів та проведено оцінку досягнення максимальної надійності системи.

Список використаної літератури

1. MHED – високоефективний метод захисту даних на основі багатошарового гібридного шифрування / О.М. Лящук // Вісник Національного технічного університету України «КПІ» Серія – Радіотехніка. Радіоапаратобудування. – 2014. — №56 – С. 144–151.
2. Чернівецький Національний Університет, Факультет математики та інформатики, кафедра прикладної математики та інформаційних технологій. Системи захисту інформації (Криптографія) [Електронний ресурс]. – режим доступу: https://pm.fmi.org.ua/files/5b16d283d4fe75.50671571.pdf
3. Панасенко С.П. Алгоритмы шифрования. Специальный справочник / С.П. Панасенко. – СПб.: БХВ-Петербург, 2009. – 576 с.
4. Прикладні аспекти захисту інформації в сучасних умовах / Ю.В. Борсуковський, В.Ю. Борсуковська // Сучасний захист інформації. – 2018. – № 2 (34) – С. 6–11.