MHED — ВИСОКОЕФЕКТИВНИЙ МЕТОД ЗАХИСТУ ДАНИХ НА ОСНОВІ БАГАТОШАРОВОГО ГІБРИДНОГО ШИФРУВАННЯ

Ляшук О. М., магістрант
Національний технічний університет України
«Київський політехнічний інститут», м. Київ, Україна

У сучасному світі, де постійно вдосконалюються технології та зростає об'єм інформації, важливою проблемою постає захист даних. Особливо актуальним питанням є проблема передачі конфіденційних даних по незахищеним каналам зв’язку, наприклад, через мережу Інтернет. Тому, щоб убезпечити інформацію, її передають використовуючи криптографію — науку про методи забезпечення конфіденційності і автентичності інформації.

Криптографія використовується для надійної передачі та зберігання даних, доступ до який має лише людина, яка володіє секретним ключем.

Сучасні криптографічні алгоритми шифрування даних поділяються на симетричні (з одним ключом для шифрування і розшифрування) та асиметричні (з відкритим ключом). У симетричних алгоритмах використовується один ключ як для шифрування для і для розшифрування. Асиметричні алгоритми використовують відкритий (*public*) та секретний (*private*) ключі для шифрування і розшифрування відповідно.

Симетричні алгоритми є досить поширеними і зазвичай використовуються для шифрування великих об’ємів даних, таких як неперервні інформаційні потоки або файли. Сучасні симетричні алгоритми є криптостійкими та швидкодійними [1]. Найбільш відомими та захищеними алгоритмами вважаються *AES, Serpent* та *Twofish*.

У таких алгоритмах для обміну зашифрованими даними обидві сторони повинні мати ключ, яким потрібно попередньо обмінятися по захищеному каналу. При широкому розповсюдженні мережі Інтернет постає проблема передачі ключа довіреній стороні по незахищеному каналу, так як симетричний ключ може бути перехоплений і третя сторона може розшифрувати повідомлення.

Вказана проблема вирішується за допомогою гібридного методу шифрування, який поєднує в собі переваги асиметричного та симетричного шифрування. Таким чином досягається прийнятна швидкість обробки даних при використанні блочного симетричного алгоритму та вирішується проблема з передачею ключа по незахищеним каналам.

Симетричні алгоритми є досить надійними, проте існують випадки їх компроментації, як це трапилось у 1993 році, коли було зламано симетричний алгоритм національної безпеки США *DES* [1]. Тому неможливо гарантувати, що нові досягнення в галузі криптоаналізу та постійне підвищення обчислювальної потужності комп'ютерів, не виявлять вразливість у симет-

ричному алгоритмі. Для вирішення цієї проблеми постійно удосконалюють алгоритми, збільшують довжину ключа.

Покращення алгоритмів не завжди вирішує проблему, оскільки дані можуть бути перехоплені, а потім — у недалекому майбутньому, коли технічні засоби це дозволять, при необхідності буде проведений злом алгоритму та дешифрування даних.

Для вирішення вище перерахованих проблем був розроблений метод захисту даних на основі багатошарового гібридного шифрування та розшифрування даних — *MHED* (*Multilayer Hybrid Encryption and Decryption*).

Особливість розробленого методу полягає в тому, що вдалось задіяти всі вищезгадані алгоритми для комплексної обробки даних: разом з асиметричним алгоритмом використовується декілька симетричних алгоритмів, кожен з який накладається послідовно, шар за шаром. Тому, в разі компроментації одного з симетричних алгоритмів, дані будуть захищені іншим. З точки зору швидкодії оптимально використовувати 3 шари симетричних алгоритмів [2].

В запропонованому методі, в частині використання симетричних алгоритмів, були обрані *AES, Serpent* та *Twofish*, в якості асиметричного алгоритму використовується *RSA*. Для кожного шару генерується новий надійний випадковий пароль, який зашифровується *RSA*. Такий ключ вирівнюється до 512 біт за записується у початок зашифрованих даних. При дешифрації даних ключ зчитується з початку зашифрованих даних, розшифровується секретним ключем та використовується для дешифрування даних шар за шаром.

При використанні *MHED* значно підвищується надійність передавання даних по незахищеним каналам, таким як мережа Інтернет. Завдяки використанню гібридного шифрування вирішується проблема з передачею ключів іншій стороні та забезпечується прийнятна швидкодія роботи всього комплексу з чотирьох задіяних алгоритмів. В розробленому методі, використання декількох шарів шифрування симетричними алгоритмами забезпечує захист даних навіть при компроментації одного з таких алгоритмів.

Література

1. Мао В. Современная криптография: теория и практика / В. Мао — М. : Видавничий дім «Вільямс». — 2005. — 273с.

2. Використання криптографічних алгоритмів у системі «Truecrypt» [Електроний ресурс]: http://www.truecrypt.org/docs/cascades#aes-serpent-twofish.