Засіб криптографіно захищеного зв’язку на базі AES-128(Rijndael)

Колесник Антон Олегович
науковий керівник О.Г.Чолишкіна, к.т.н., доцент.
ІІДС, Національний авіаційний університет
Київ, Україна
e-mail antonkolesnik61@gmail.com

Анотація — Розроблено програмний продукт для забезпечення криптографічно-захищеного зв’язку між двома абонентами за використанням сучасних алгоритмів.

Ключові слова — криптологія, захист інформації, захищений зв'язок, алгоритм, шифрування.

I. Вступ

З розвитком сучасних технологій зв’язку тема безпеки передачі даних стає все більш актуальної. На сьогодні неможливо з достатнім ступенем впевненості стверджувати, що переказ даних за використанням мережі Інтернет відбувається без втручання третьої особи.

Як відомо [1], відправлене з Оксфорда через Gmail лист на Yahoo! Mail абоненту в Сан-Франциско, повідомлення може бути перехоплено мінімум 7 разів.

II. Постановка задачі

Для забезпечення цілісності даних та аутентифікації абонента запропоновано використання шифрованого зв’язку. В якості алгоритму шифрування було обрано сучасний метод, який є лідером на світовому ринку криптографічної безпеки, а саме AES-128 (Rijndael) [2] в парі з протоколом Діффі – Хеллмана із вбудованою аутентифікацією.

Стандарт шифрування AES є офіціальним стандартом уряду США для симетричного шифрування. Стандарт визначається публікацією FIPS #197 (2001) та використовується в різноманітних додатках, де пред’являються підвищені вимоги до продуктивності та безпеки. Алгоритм може використовувати ключі довжиною 128, 192 та 256 біт. При використанні 128-бітного ключа, для злому шифрування, за заявою уряду США, потрібно 149 трильйонів років.

III. Викладення основного матеріалу

AES - симетричний ітеративний блоковий алгоритм; базується на принципах нової мережі підстановок-перестановок. Має архітектуру SQUARE:

1) уявлення шифруемого блоку у вигляді двовимірного байтового масиву;

2) шифрування за один раунд всього блоку даних (байт-орієнтована структура);

3) виконання криптографічних перетворень, як над окремими байтами масиву, так і над його рядками і стовпцями. Це забезпечує дифузію даних одночасно в двох напрямках - по рядках і по стовпцях.

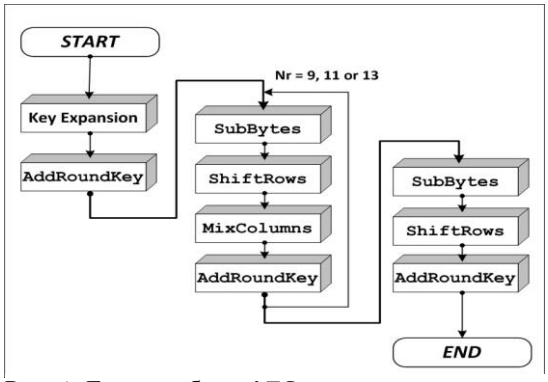

Рис. 1. Етапи роботи AES

Зв'язок між користувачами здійснюється за допомогою технології P2P (peer-to-peer – рівний до рівного).

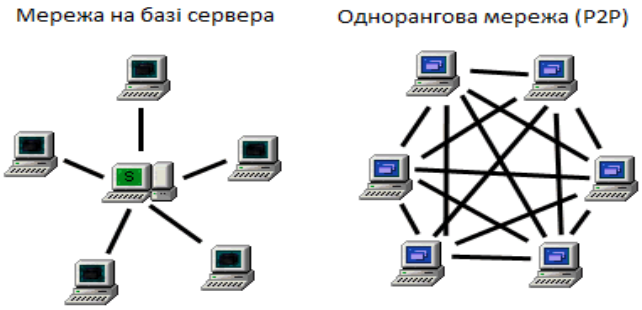

Рис. 2. Архітектури мереж

В основі технології лежить принцип децентралізації,тобто всі вузли в мережі P2P – рівноправні (рис 2). Цей принцип, забезпечив такі переваги технології P2P перед клієнт-серверних підходом, як відмовостійкість до втрати зв'язку з вузлами мережі, збільшення швидкості копіювання за рахунок копіювання відразу з декількох джерел, можливість поділу ресурсів без прив'язки до конкретних IP-адресами, величезна потужність мережі в цілому та ін.

Висновки.

Розроблене програмне забезпечення дозволяє здійснювати криптографічно захищений зв'язок між двома абонентами. Завдяки властивостям обраного алгоритму шифрування забезпечується достатньо високий рівень безпеки, що дозволяє використання запропонованого ПЗ як для бізнес сфери так і для державного рівня.

Список використаних джерел

[1] «EMail и безопасность. Можно ли защитить почтовую переписку» [Електроний ресурс] : https://habrahabr.ru/company/pechkin/blog/276761/

[2] Брюс Шнайер, "Прикладная криптография", 2 издание, М: «ТРИУМФ», 2012, с. 816.