УДК 004.056.55

Д.Н.М. Томнюк
Національний авіаційний університет, Київ

ПРОГРАМНИЙ МОДУЛЬ ШИФРУВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ

Актуальність теми. Постійно зростаючі вимоги створення нових криптостійких до різних типів атак потокових шифрів. Врахування ними особливостей сучасної елементної бази, створення нових видів атак обумовлює потребу в розробці та дослідженні нових підходів до побудови блокових шифрів.

ІНФОРМАЦІЙНИЙ РЕСУРС, КРИПТОГРАФІЧНИЙ ЗАХИСТ ДАНИХ, БЛОКОВИЙ СИМЕТРИЧНИЙ ШИФР, ІНФРАСТРУКТУРА РОЗПОДІЛУ КЛЮЧІВ, КІБЕРПРОСТІР.

Об’єкт дослідження – кіберпростір, блоковий алгоритм шифрування.

Предмет дослідження - метод блокового алгоритму шифрування.

Мета роботи – розробка системи захисту інформації на базі блокового алгоритму.

Блокові алгоритми шифрування - це основа, на якій реалізовано майже всі криптосистеми. Техніка створення ланцюгів із зашифрованих блоковими алгоритмами байт дозволяє їм шифрувати пакети інформації необмеженої довжини. Така властивість блокових шифрів, як швидкість роботи, використовуються асиметричними криптографічними алгоритмами, які повільні за своєю природою. Відсутня статистична кореляція між бітами вихідного потоку блокового шифрування використовується для обчислення контрольних сум пакетів даних та в хешуванні паролів.

Криптоалгоритм називається ідеально стійким, якщо існує можливість читати зашифрований блок даних лише переглянувши всі можливі клавіші, поки повідомлення не буде значущим. Оскільки теоретично потрібний ключ буде знайдений з імовірністю 1/2 після перебору половини всіх ключів, то для злому ідеально стійкого криптоалгоритму з ключем довжиною N потрібно в середньому

$2^{(N-1)}$ перевірки. Таким чином, у загальному випадку стійкість блокового шифру залежить лише від довжини ключа і зростає експоненціально у міру зростання. Навіть якщо припустити, що пошук ключів здійснюється за спеціально розробленою багатопроцесорною системою, в якій, завдяки діагональному паралелізму, на перевірку 1 клавіші йде лише 1 година, то для того, щоб зламати 128-бітний ключ, потрібно, як мінімум 10^{21} рік. Звичайно, все вищесказане стосується лише ідеально стійких шифрів.

Блокові алгоритми шифрування на сьогодні являються основним засобом криптографічного захисту інформації.

Основними перевагами блокових алгоритмів шифрування є:

– висока швидкість шифрування/розшифрування;

– висока гарантована стійкість, яка до того ж може бути доведена математично;

– можливість ефективної програмної реалізації.

Встановлено, що застосування блокових алгоритмів при застосуванні з іншими методами захисту інформації значно підвищує рівень кібербезпеки.

Результати, отримані в ході дослідження дипломної роботи, рекомендовано використовувати для захисту інформаційних ресурсів у кібернетичному просторі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Криптографические методы защиты информации : учебник / А.В. Бабаш, Е.К. Баранова. — Москва : КНОРУС, 2018. — 190 с. — (Бакалавриат и магистратура)

2. ГОСТ 34.310-95 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

3. ГОСТ 34.311-95 Информационная технология. Криптографическая защита информации. Функция хеширования.

4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си — М.: Триумф, 2002. — 816 с.

5. Шнайер, Брюс. Прикладная криптография (Applied Cryptography), 2-е издание.