ПОРІВНЯЛЬНИЙ АНАЛІЗ БЛОЧНИХ СИМЕТРИЧНИХ ШИФРІВ

Мартиненко Я.А.
Науковий керівник – асистент Євгеньєв А. М.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. БІТ, тел. (057) 702-14-25)
e-mail: yana.martynenko@nure.ua

The disclosure of the relevance of this topic in the XXI century. The definition of block ciphers. The description of the main difference from stream symmetric ciphers. The demonstration of the brief description (key length, block size, number of rounds, etc.) some of the most important algorithms in US history. The assessment of crypto resistance, using these ciphers as an example. The demonstration of the spreadsheet to compare their characteristics. Based on the analyzed material, the generalization of the most reliable information protection algorithm among 3 ciphers.

На сьогоднішній день існує актуальна наукова-технічна задача , яка базується на захисті конфіденційності та цілісності інформації. З'являються нові методи атак шифрів, тому важливе існування та удосконалення стійких до криптографічних атак алгоритмів.

Для розгляду було взято 3 популярних блочних симетричних шифрів: DES, Triple DES та AES.

Блочний шифр – криптографічний алгоритм, який має одиницю кодування блок з декількох байтів. Потоковий шифр, на відміну від блочного, надає ключ довільної довжини, що накладається на відкритий текст побітово. Блочні шифри поділяють на 2 групи: ті, що використовують структуру Фейстеля та ті, що використовують мережу перестановок-підстановок (SP-мережі).

DES (Data Encryption Standard) – блочний алгоритм шифрування, який має довжину блоку 64 біт, як і довжина ключа, кількість раундів становить 16. Оскільки DES заснований на структурі Фейстеля, яка була згадана раніше, то відбувається певне перетворення тексту(поділ блоку на 2 половини перед тим, як пройти етапи шифрування), при якому значення, обчислені від однієї з частин тексту, накладається на інші частини. Однак, аналізуючи крипостійкість, треба зауважити довжину ключа – 56 біт. Тому зі зростанням розрахункової потужності комп'ютерів з'явилися сумніви щодо крипостійкості алгоритму. Команда distributed.net об'єдналася з представниками Electronic Frontier Foundation і зламала шифрування DES менш ніж за добу. Таким чином, алгоритм шифрування DES достатньо таки не стійкий.

Для вирішення цієї проблеми на основі DES було створено новий, покращений варіант алгоритму – Triple DES(3DES). На відміну від DES довжина ключа становить 168 біт, довжина блоку 64 біт. Процедура шифрування аналогічна до базисного алгоритму. Щодо стійкості до атак, то

безумовно 3DES є більш надійним, однак, збільшуючи розмір ключа, засновники шифру збільшили в 3 рази кількість раундів, у такий спосіб зменшивши швидкість роботи алгоритму. І DES, і 3DES використовують 64-бітний розмір блоку. З міркувань ефективності та безпеки бажано збільшити їхній розмір.

На підставі цих міркувань було створено новий алгоритм AES (Advanced Encryption Standard). Врахувавши недоліки попередніх шифрів, засновники алгоритму створили 128-бітний блок. Довжина ключа становить 128/192/256 біт. Кількість раундів залежить від довжини блоку. Алгоритм базується на основі принципу проектування, відомого як мережа перестановки-підстановок. Спираючись на дані щодо розміру ключа, AES є стійким алгоритмом до криптографічних атак.

Таблиця 1 – Узагальнена характеристика алгоритмів

Назва алгоритму	DES	Triple DES	AES
Процедура шифрування	Структура Фейстеля	Структура Фейстеля	Мережа перестановок-підстановок
Довжина ключа	56 біт	168 біт	128/192/256 біт
Довжина блоку	64 біт	64 біт	128 біт
Швидкість виконання	Повільніше, ніж AES, швидше, ніж 3DES	Повільніше, ніж алгоритми AES та DES	Швидше, ніж алгоритми 3DES та DES
Рівень криптостійкості	Низький	Достатній	Високий

Відтак, враховуючи появу нових удосконалених методів атак DES став менш надійним. Середню позицію займає 3DES через повільну швидкість виконання. Враховуючи вищезазначені характеристичні дані, можна зробити висновок, що AES – ефективний і надійний алгоритм захисту інформації, аргументуючи відсутністю «вдалих» криптографічних атак.

Список використаної літератури:

1. Moore J.H. Cycle Structure of the DES with Weak and Semi-Weak keys//Advances in Cryptology. Berlin: Springer-Verlag,1987.pp. 2-32

2. Баричев С. Г., Гончаров В. В., Серов Р. Е. 2.4.2. Стандарт AES. Алгоритм Rijdael // Основы современной криптографии – 3-е изд.

3. Fomichev V.M., Koreneva A.M. Evaluation of the maximum performance of block encryption algoritms.2019. V.10. No.2. P. 7-16