УДК 004.056

М.С. Ціхоцький
Ю.В. Баришев

Підхід до побудови псевдонедетермінованого блокового шифру

Вінницький національний технічний університет

Анотація

Проаналізовано відомі мережі для побудови блокового шифру. На основі даного аналізу запропоновано новий підхід для побудови шифрів, який за рахунок псевдонедетрмінованості дозволяє покращити показники стійкості шифрування.

Ключові слова: шифрування, блоковий шифр, криптографія, шифротекст, псевдонедетермінований.

Annotation

Block cipher networks were analyzed. New approach for stronger ciphers designing was proposed on the basis of performed analyses, which allows to improve cipher's infeasibility parameters.

Keywords: encryption, block cipher, cryptography, ciphertext, pseudonondeterministic.

Вступ

Захист інформації – невід'ємна частина сучасного світу, одним з основних напрямків захисту інформаційних ресурсів – це шифрування. Методи шифрування інформації поділяються на симетричні та асиметричні алгоритми шифрування [1]. Найпоширенішим типом симетричних шифрів є блокові шифри. Незважаючи на те, що існує велика кількість блокових шифрів, більшість з них мають низку недоліків або є недостатньо стійкими. Кожного дня зростають вимоги до шифрів, в зв'язку з розвитком сучасної техніки та збільшенням швидкості обчислювальної техніки. Дані зміни обумовлюють потребу у розробці нових підходів до реалізації блокових шифрів.

Метою дослідження є підвищення рівня захисту блокових шифрів. Для її досягнення:

- проаналізовано відомі мережі блокових шифрів;
- виконано порівняння обраних шифрів;
- розроблено підхід до реалізації блокового шифру підвищеної стійкості.

Основні елементи блокового шифру

Блоковий шифр зазвичай складається з простих перетворень над відкритим текстом, що виконуються в певній послідовності деяку кількість разів. В основі майже усіх блокових шифрів лежать математичні операції та функції перетворення [2]. До основних перетворень блокового шифру:

- блок-підстановок (S-блок), який складається з наступних частин: дешифратор, система з'єднань та шифратор;
- блок-перестановок (P-блок), який змінює положення цифр і є лінійним пристроєм;
- циклічний зсув – в найпростішій реалізації (зсув на 1 біт), крайній біт від'єднується і переміщується у другий кінець регістру.

- сума за модулем n – ця операція визначається як $(A + B) \bmod n$ і представляється залишком від ділення суми $A + B$ на n .
- множення за модулем n, визначається як $(A * B) \bmod n$ і представляється залишком від ділення результату добутку $A * B$ на n .

Аналіз мереж для побудови блокових шифрів

Проаналізуємо основні мережі, які використовуються для побудови блокових шифрів [3].

Для аналізу було обрано чотири види мереж – мережа Фейстеля, розширена мережа Фейстеля, мережа SPN, мережа Lai-Massey).

Вибір мережі впливає на стійкість отриманого блокового щифру. Криптографічна стійкість шифру залежить від складності реалізації атаки на блоковий симетричний шифр. Показниками складності криптоаналізу, як правило, слугують [4]:

- часовий – математичне сподівання часу (безпечний час), необхідного для реалізації атаки на доступних / перспективних обчислювальних засобах.
- просторової складності – обсяг пам'яті, що необхідний для виконання криптографічного аналізу.
- мінімально необхідна для успішної реалізації атаки кількість пар зашифротекст/ відкритий текст чи кількість пар відкритий текст/ шифротекст.

Попередній аналіз дає підстави зробити висновок, що якщо хоча б щодо одного із зазначених показників реалізація атаки на практиці неможлива зі значним запасом стійкості, то алгоритм шифрування можна вважати стійким.

Опис підходу для побудови блокового шифру

Для покращення стійкості блокового шифру було запропоновано наступний підхід. Під час шифрування в залежності від значення ключа буде обиратись відповідна мережа (мережа Фейстеля, розширена мережа Фейстеля, SPN-мережа, мережа Lai-Massey).

Секретний ключ k на початку шифрування розгортається у $k_i = k_i^{\text{оп}} \,||\, k_i^{\text{керув}}$, де $k^{\text{оп}}$ – частина ключа, яка подається на вхід ключа у поточну мережу використовуючи наступну функцію $k_i = f(k_{i-1})$, $k^{\text{керув}}$ – частина ключа, яка визначає мережу для наступного блоку шифрування.

Використання декількох мереж можливе за умови їх сталості на кожній ітерації, що ускладнить реалізацію. При апаратній реалізації такий підхід буде невиправданим, але для програмної – таке ускладнення лише несуттєво збільшить кількість програмного году відповідного модуля програмного засобу.

Висновки

Було проаналізовано відомі підходи до побудови блокових шифрів, з чого з’ясовано, що наявні підходи потребують удосконалення для досягнення більшого захисту інформаційних ресурсів.

Запропонований блоковий шифр теоретично має значні переваги над відомими шифрами у зв’язку з постійною випадковою зміною, з точки зору зловмисника, варіантів мережі шифрування. Такий підхід ускладнить використання відомих методів криптоаналізу блокових шифрів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. О. Поліщук, А. Лагун – Дослідження блокових шифрів та розроблення на основі перетворення Фейстеля модифікованого блокового шифру, 2011.
2. Cusick, Thomas W. & Stanica, Pantelimon. Cryptographic Boolean functions and applications.
3. Брюс Шнайер – Прикладная криптография, 2-е издание, 2002.
4. О. О. Кузнецов, Р. В. Олійников, Ю. І. Горбенко, А. І. Пушкарьов, О. В. Дирда, І. Д. Горбенко – Обґрунтування вимог, побудування та аналіз перспективних симетричних криптоперетворень на основі блочних шифрів, 2014.

Ціхоцький Микита Сергійович — студент, факультет інформаційних технологій та комп'ютерної інженерії, технічний університет, Вінниця, e-mail: nik.tsikhotskiy15@gmail.com

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, email: yuriy.baryshev@gmail.com

Tsikhotskyi Mykyta Serhiyovych — student, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: nik.tsikhotskiy15@gmail.com

Baryshev Yurii — Cand. Sc. (Eng), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, yuriy.baryshev@gmail.com