ЗАСТОСУВАННЯ КОМБІНАТОРНИХ МЕТОДІВ ГЕНЕРАЦІЇ КЛЮЧІВ ДЛЯ ШИФРУВАННЯ ІНФОРМАЦІЇ

Казбан М. О., магістр; Дем'яненко П. О., к.т.н., доцент
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна

Вступ

На теперішній час Україна глибоко інтегрована у світовий інформаційний простір, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Існує потреба у нових алгоритмах шифрування для захисту інформаційних ресурсів.

Актуальними проблеми захисту інформації залишаються питання проектування, створення і використання сучасних інтегрованих інформаційних систем за рахунок алгоритмів шифрування даних.

Симетричний блочний алгоритм на базі мережі Фейстеля

Під мережею Фейстеля розуміють розбиття оброблюваного блоку на кілька субблоків, один з яких оброблюється деякою функцією $f(x)$, що далі накладається на один або декілька інших субблоків. На рис. 1 приведена структура на основі мережі Фейстеля [1].

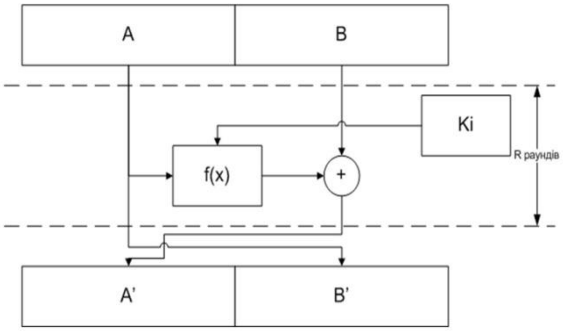

Рисунок 1. Структура алгоритмів на основі мережі Фейстеля

Додатковий аргумент функції $f(x)$, що позначено на рис. 1 як *Ki* називається ключем раунду. Ключем раунду є результат обробки ключа процедурою розширення. Задача цієї процедури — отримання необхідної кількості ключів *Ki* з вхідного ключа відносно невеликого розміру. В простих випадках розширення ключа передбачає його розбивання на фрагменти, які використовуються по черзі в раундах шифрування. Як правило процедура розширення ключа є доволі складною, а ключі K_i залежать від значень більшості біт вхідного ключа шифрування [2].

Застосовуваний алгоритм передбачає симетричність, так як вимагається використання одного і того самого ключа для шифрування та дешифрування. Нехай довжина блоків алгоритму дорівнює 32 біта. Також використаємо хеш-функцію для шифрування та дешифрування, що дає змогу приймати довільний блок даних і повертати рядок встановленого розміру. Для кодування вихідного повідомлення використовується алгоритм шифрування «base64». На рис. 2 наведено загальну схему шифрування. Дешифрування можливе тільки для тих повідомлень, які були зашифровані за допо-

могою симетричного алгоритму. Особливістю застосування цього алгоритму є потреба у локальних серверах, через які виконуються операції криптографії у веб-браузері.

Рисунок 2. Загальна схема шифрування

Для зменшення ймовірності підбору ключа під час атаки «брут-форс», потрібно використовувати обмеження для довжини ключа, який не перевищуватиме 32 символи.

В табл. 1. наведені етапи шифрування та дешифрування.

Таблиця 1

Шифрування	Дешифрування
1.Перетворення ключа	
2.Перетворення вхідного повідомлення	2.Декодування повідомлення зі стану «base64», перетворення шістнадцякової в двійкову форму
3. Генерування додаткових послідовностей для перетворення блоків вхідного повідомлення	
4. Підготовка вхідного повідомлення до шифрування	
5. Перетворення кожного блоку вхідного повідомлення	
6. Перетворення в послідовність шістнадцяткових чисел	
7. Перетворення шістнадцяткових чисел в символи з використанням «base64»	7. Перетворення шістнадцяткових чисел в символи відповідно до таблиці ASCII

Для досягнення стійкості парольної фрази пропонується використовувати подвійне хешування, яке захистить від атак та константну довжину парольної фрази для шифрування. Для унікальності створюються блоки шифрування нестандартної довжини, що дає змогу зменшити довжину блоку з 32 біт та перетворення виконувати з субблоками по 27 біт. Завдяки цьому вдається під час криптозахисту варіювати довжиною вихідного повідомлення та вхідного повідомлення, що суттєво ускладнює процес підбору ключа.

Висновки

Запропоновано модифікований алгоритм шифрування текстової інформації. Створена аналітична модель алгоритму шифрування застосовує при криптозахисті варіювання довжини вхідного та вихідного повідомлення. При цьому зберігається ефективність математичних операцій шифрування та дешифрування інформації. Криптографічний алгоритм не використовує стандартні розміри блоків, що суттєво ускладнює процедуру підбору ключа.

Перелік посилань

1. Нечаев В.И. Элементы криптографии (Основы теории защиты информации)*: учеб. [учеб. пособие для ун-ов и пед. вузов]* / В.А. Садовничьего — Москва: М-во.высш. шк., 1999 — 109с.

2. Нильс Фергюсон Практическая криптография = *Practical Cryptography: Designing and Implementing Secure Cryptographic Systems*. — М.: «Диалектика», 2004. — 432 с.

Анотація

Проведено розробку алгоритму для шифрування та дешифрування тестових повідомлень. Створена аналітична модель алгоритму шифрування. Проаналізовано процес виконання шифрування та дешифрування. Визначена схема роботи алгоритму.

Ключові слова: криптографічні методи захисту, алгоритми шифрування та дешифрування , кодування символів.

Аннотация

Проведена разработка алгоритма для шифрования и дешифрования тестовых сообщений. Создана аналитическая модель алгоритма шифрования. Проанализировано процесс выполнения шифрования и дешифрования. Определена схема работы алгоритма.

Ключевые слова: криптографические методы защиты, алгоритмы шифрования и дешифрования, кодирования символов.

Abstract

Handpainted develop an algorithm to encrypt or decrypt test messages. Created an analytical model of the encryption algorithm. Handpainted perform encryption and decryption. A scheme of the algorithm.

Keywords: cryptographic security techniques, encryption and decryption, character encoding.