УДК 681.3.07

Забудський Р.С.[1]

АЛГОРИТМ ЗАХИСТУ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ

[1]Вінницький національний технічний університет

Анотація
Розглянуто оновлений стандарт шифрування інформації в телекомунікаційних мережах від несанкціонованого доступу .
Ключові слова: шифрування, безпека даних, криптографія, телекомунікації.

Abstract
Considered updated information encryption standard at telecommunication networks from unauthorized access.
Keywords: encryption, data security, cryptography, telecommunications.

Вступ

Винахід алгоритму AES призвело до позитивних змін в стані прикладної криптографії.

Алгоритмм AES замінив багаторазове шифрування, наприклад, за допомогою потрійного алгоритму DES, а змінний розмір його ключа і блоків повідомлення, рівний 128, 192 і 256 біт, надає широкий вибір варінтів рішень, що забезпечують стійкість в різноманітних додатках. Оскільки в багаторазовому шифруванні використовується велика кількість ключів, поява AES полегшила управління криптографічними ключами і спростила процес розробки протоколів і систем захисту даних в інфокомунікаційних мережах, цим самим підтверджуючи свою власну актуальність[1].

Основна частина

Алгоритм Rijndael формує блоковий шифр зі змінним розміром блоків і змінною довжиною ключа. Розміри ключа і блоків можуть незалежно один від одного набувати значень 128, 192 і 256 біт. Для спрощення розглянемо лише мінімальний варіант, в якому розміри ключа і блоку рівні 128 біт. Основні принципи алгоритму Rijndael розглянемо повністю. Отже, 128-бітовий блок повідомлення (початкового або зашифрованого) розбивається на сегменти по 16 байт (один байт складається з восьми біт, тобто 128 = 16x8).

$$InputBlock = m_0, m_1, \ldots m_{15}.$$

Аналогічно операція виконується над блоком ключа.

$$InputKey = k_0, k_1, \cdot \cdot \cdot, k_{15}.$$

Для внутрішнього представлення даних використовується матриця 4x4.

$$InputBlock = \begin{pmatrix} m_0 & m_4 & m_8 & m_{12} \\ m_1 & m_5 & m_9 & m_{13} \\ m_2 & m_6 & m_{10} & m_{14} \\ m_3 & m_7 & m_{11} & m_{15} \end{pmatrix},$$

$$InputKey = \begin{pmatrix} k_0 & k_4 & k_8 & k_{12} \\ k_1 & k_5 & k_9 & k_{13} \\ k_2 & k_6 & k_{10} & k_{14} \\ k_3 & k_7 & k_{11} & k_{15} \end{pmatrix}.$$

Як алгоритм DES (і більшість сучасних симетричних блокових шифрів), алгоритм Rijndael складається з великої кількості повторюваних перетворень − раундів. У мінімальному варіанті, коли розміри блоку і ключа рівні 128 біт, кількість раундів дорівнює 10.

Для більших повідомлень і ключів кількість раундів може зростати. Перетворення, що виконується всередині раунду, позначається як

Round*(State, RoundKey).*

Змінна *State* є матрицею, що містить повідомлення раунду, і вважається як входом, так і результатом раунду, а змінна RoundKey являє собою матрицю, що містить ключ раунду та створюється на основі вхідного ключа за допомогою розкладу ключів. Перетворення всередині раунду має змінювати елементи матриці *State* (тобто змінювати стан). При шифруванні (відповідно при дешифруванні) матриця *State*, що надходить на вхід першого раунду, збігається з матрицею *InputBlock* і містить початковий текст (відповідно зашифрований текст). В свою чергу, матриця *State*, що утворюється в результаті заключного раунду, містить зашифрований текст (відповідно початковий текст). Перетворення, що виконуються в ході проміжних раундів, разбиваються на чотири операції, які є внутрішніми функціями.

Опишемо чотири внутрішні функції алгоритму Rijndael. Розглянемо лише функції, призначені для шифрування. Оскільки кожна з них є оборотної, розшифровка в алгоритмі Rijndael просто зводиться до застосування зворотних функцій в зворотному порядку[1].

Внутрішні функції шифру Rijndael визначені на кінцевому полі, яке складається з усіх поліномів по модулю неприводимого полінома

$$f(x) = x^8 + x^4 + x^3 + x + 1$$

над полем F_2. Інакше кажучи, шифр використовує поле $\boldsymbol{F}_{2[x]x^8+x^4+x^3+x+1}$. Будь-який елемент цього поля є поліномом над полем F_2, ступінь якого меньше восьми, а операції виконуються за модулем *f(x)*. Назвемо це поле «полем Rijndael» . Завдяки ізоморфізму це поле можна перепозначити як$\boldsymbol{F}_{2^8}$. Воно складається з $2^8 = 256$ елементів.

Роль внутрішніх функцій алгоритму Rijndael.

• Функція SubBytes призначена для реалізації нелінійного підстановлювального шифру. Нелінійність – важлива властивість блокового шифру, що захищає його від криптоаналіза.

• Функції ShifrRows і MixColumns призначені для змішування байтів, розміщених в різних місцях блоку вихідного повідомлення. Як правило, розподіли вихідних текстів у просторі повідомлень мають низьку ентропію завдяки високій надмірності натуральних мов і економічних даних (інакше кажучи, звичайні вихідні тексти утворюють малий підпростір в усьому просторі повідомлень). Суміш байтів, що стоять в різних позиціях блоку повідомлення, розширює розподіл повідомлень. По суті, це забезпечує можливість перемішування, сформульовану Шеноном.

• Функція AddRoundKey забезпечує необхідну секретну випадковість розподілу повідомлень. Ці функції застосовуються багаторазово (як мінімум 10 разів, якщо розмір ключа і даних дорівнює 128 біт).

Оскільки, всі чотири внутрішні функції є зворотніми, розшифровка зводиться до виконання шифрування в зворотньому порядку.

AddRoundKey(*State, RoundKey*)$^{-1}$

MixColumns(*State*)$^{-1}$;

ShiftRows(*State*)$^{-1}$;

SubBytes(*State*)$^{-1}$.

Слід зауважити, що на відміну від шифру Файстеля, в якому алгоритм шифрування і розшифровки використовують одну і ту ж електронну схему або програму, шифр Rijndael використовує різні електронні схеми і програми для шифрування і розшифровки відповідно[1].

Висновки

Використання блокових алгоритмів шифрування як однонаправлених функцій хешування стало повсякденною практикою. Як приклад можна привести протокол реєстрації користувачів в операційній системі UNIX. Іншим прикладом використання блокових алгоритмів шифрування є

реалізація однонаправлених функцій хешування з ключами. На практиці хеш-функції часто застосовуються в якості датчиків псевдовипадкових чисел для генерації ключів блокових алгоритмів шифрування.

Варто відмітити, що алгоритм AES привертає увагу криптоаналітиків, вивчаючих блокові шифри, що, безсумнівно призведе до появи нових відкриттів в даній області.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мао Венбо. Современная криптография: теория и практика. : Пер с англ. — М. : Издательский дом «Вильямс», 2005. — 768 с. : ил. – ISBN 5-8459-0847-7 (в пер.).

Забудський Роман Сергійович — студент групи ТКТ-16мс, факультет інфокомунікацій, радіоелектроніки та наносистем, Вінницький національний технічний університет, Вінниця, e-mail:h3lltv@mail.ex.ua

Науковий керівник: ***Васильківський Микола Володимирович*** – к.т.н, доцент кафедри телекомунікаційних систем і телебачення, Вінницький національний технічний університет, м. Вінниця, e-mail: mvasylkivskyi@gmail.com.

Zabudskiy Roman — Department of Infocommunication, Electronics and Nanosystems, Vinnytsia National Technical University, Vinnytsia, e-mail: h3lltv@mail.ex.ua

Supervisor: ***Vasylkivskyi Mikola***– Ph.D., Senior lecturer of the Chair of Telecommunication Systems and Television, Vinnytsia National Technical University, Vinnytsia, e-mail: mvasylkivskyi@gmail.com.