УКРАЇНА **(19) UA** **(11) 129836** **(13) U**

(51) МПК (2018.01)
G09C 1/00

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2018 06350**

(22) Дата подання заявки: **06.06.2018**

(24) Дата, з якої є чинними права на корисну модель: **12.11.2018**

(46) Публікація відомостей про видачу патенту: **12.11.2018, Бюл.№ 21**

(72) Винахідник(и):
Кучеренко Віктор Григорович (UA),
Пєнкін Юрій Михайлович (UA),
Литвинов Олександр Григорович (UA),
Хара Георгій Іванович (UA)

(73) Власник(и):
Кучеренко Віктор Григорович,
вул. Дружби Народів, 232-В, кв. 102, м. Харків, 61184 (UA)

(74) Представник:
Бойко Дмитро Віталійович

(54) СПОСІБ ГЕНЕРАЦІЇ КЛЮЧІВ ДЛЯ СИМЕТРИЧНИХ БЛОЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ

(57) Реферат:

Спосіб генерації ключів для симетричних блочних алгоритмів шифрування включає в себе використання керованих операцій нелінійних матричних трансформацій. Створюють дві взаємно однозначні за місцем розташуванням елементів квадратні матриці F та U, кожна з яких має розміри N*N, де N = n*n, а $n \geq 4$ - ціле число, в результаті чого кожна з матриць F та U складається з N - суміжних квадратних матриць n*n. При цьому матрицю F рівномірно заповнюють випадковими цілими числами з інтервалу $[0 \ldots N^2-1]$, а матрицю U заповнюють цілими числами з інтервалу [1….N] за принципом латинського квадрату таким чином, щоб в кожному рядку, кожному стовпчику та в кожному із суміжних квадратних матриць n*n не було однакових чисел. Після чого до кожної суміжної квадратної матриці n*n у складі матриці U застосовують функцію перестановок $R(V,P)$, де $\overline{V}$ - вектор розмірності N, який задає вихідне місце розташування елементу суміжної квадратної матриці n*n, а $\overline{P}$ - вектор розмірності N, кожний компонент якого має свій номер і, який вказує на те, який порядковий компонент вихідного вектора $\overline{V}$ вибирається при перестановці, та значення k, яке вказує те, на яке порядкове місце слід поставити цей елемент в результаті перестановки. В результаті необхідної кількості ітерацій застосування функції перестановок R отримують нову форму матриці U, що внаслідок однозначності розташування елементів призводить до відповідної трансформації матриці F, після чого з необхідної кількості елементів останньої і формують ключі шифрування.

UA 129836 U

Корисна модель належить до способів криптографічного перетворення інформації на базі формування закритих ключів для блочних симетричних алгоритмів шифрування.

Засобом підвищення криптостійкості блочних алгоритмів шифрування, особливо при шифруванні блоків квазістатичної інформації, є періодична зміна ключа шифрування. В свою чергу необхідність періодичної зміни криптографічних ключів висуває додаткові вимоги до способів формування таких ключів. З одного боку, способи формування ключів мають забезпечувати високу криптостійкість таких ключів, а з іншого - мають забезпечувати високу швидкість їх реалізації.

Одним з напрямків вирішення вказаної задачі є створення інфраструктури динамічної зміни криптографічних ключів.

З попереднього рівня техніки є відомим спосіб управління генерацією криптографічних ключів, який описано в патенті РФ на винахід "Ефективне управління генераціями криптографічних ключів" №2351078 [1].

Вказаний винахід спрямовано на вирішення задачі генерації послідовності криптографічних ключів таким чином, щоб за умов використання останнього ключа та певної додаткової інформації можна було б відновити всі попередні ключі. Зазначене, за задумом авторів патенту, дозволяє зберігати зашифровані старими ключами дані, не шифруючи їх заново при зверненні до нового ключа. Реалізація вказаного винаходу передбачає зберігання ключа та додаткової інформації до нього на зовнішньому (відносно задіяного інформаційного каналу) сервері.

Основним недоліком вказаного способу є те, що внаслідок достатньо високої обчислювальної та алгоритмічної складності, він вимагає застосування значних обчислювальних ресурсів, а також вжиття додаткових заходів із обмеження доступу та захисту задіяних для його реалізації програмно-апаратних комплексів.

Найбільш близьким по своїй суті до запропонованої корисної моделі, що вибрано за прототип, є "Спосіб криптографічного перетворення цифрових даних", відомий з патенту Російської Федерації №2309549 [2].

Зазначений винахід базується на апаратній реалізації контрольованих операцій перестановок - криптографічних примітивів, що дозволяє суттєво прискорити процеси шифрування. Для цього вихідні дані представляються у вигляді двійкового вектора з розмірністю n, де n - ступінь двійки. При цьому кожний примітив визначає виконання операції над обмеженою кількістю бітів. Для одержання n-розрядного ключа з необхідними властивостями використовується багаторівнева мережа з блоків управління перестановками.

До недоліків способу-прототипу можна віднести фіксовану структуру мережі блоків управління операціями для кожного розміру ключа (блоку даних), що передбачає необхідність розробки нової структури при зміні розміру ключа.

Крім того, стійкість процедури шифрування, що визначається рівномірністю розподілення кодів та нелінійністю багатораундових перестановок, досягається складною організацією мережі блоків управління операціями та спеціальним вибором інформації, що керує роботою цієї мережі.

Технічною задачею запропонованої корисної моделі є створення простого щодо реалізації та одночасно надійного способу генерації криптографічних ключів.

Основним технічним результатом заявленого технічного рішення порівняно з відомими аналогами є спрощення алгоритму генерації закритих ключів та підвищення швидкості роботи реалізації цього алгоритму.

Додатковим технічним результатом корисної моделі, що заявляється, є забезпечення високої криптостійкості ключів шифрування, згенерованих на основі способу, що пропонується.

Поставлена задача вирішується тим, що у способі генерації криптографічних ключів, що включає в себе використання керованих операцій нелінійних матричних трансформацій, згідно з корисною моделлю, створюють дві взаємно однозначні за місцем розташуванням елементів квадратні матриці F та U, кожна з яких має розміри N*N, де N=n*n, а $n \geq 4$ - ціле число, в результаті чого кожна з матриць F та U складається з N - суміжних квадратних матриць n*n, при цьому матрицю F рівномірно заповнюють випадковими цілими числами з інтервалу [0… N^2-1], а матрицю U заповнюють цілими числами з інтервалу [1…N] за принципом латинського квадрату таким чином, щоб в кожному рядку, кожному стовпчику та в кожному із суміжних квадратних матриць n*n не було однакових чисел, після чого до кожної суміжної квадратної матриці n*n у складі матриці U застосовують функцію перестановок $R(V,P)$, де $\overline{V}$ - вектор розмірності N, який задає вихідне місце розташування елементу суміжної квадратної матриці n*n, а $\overline{P}$ - вектор розмірності N, кожний компонент якого має свій номер і, який вказує на те, який порядковий компонент вихідного вектора $\overline{V}$ вибирається при перестановці, та значення k, яке вказує те, на

яке порядкове місце слід поставити цей елемент в результаті перестановки, і в результаті обраної кількості ітерацій застосування функції перестановок R отримують нову форму матриці U, що внаслідок однозначності розташування елементів призводить до відповідної трансформації матриці F, після чого з необхідної кількості елементів останньої і формують ключі шифрування.

Детальніше суть корисної моделі пояснюється наступним.

Запропонований спосіб генерації ключів оснований на паралельному використанні двох матричних форм (F та U) та виконанню над ними трансформаційних операцій.

Обидві матриці є квадратними та мають розмір N*N, де $N=n^2$, а $n\geq 4$ - ціле число. Якщо довжина блока блочного алгоритму шифрування дорівнює M, то число n обирається таким чином, щоб забезпечувалося $n^2=N\geq M$.

Між матрицями F та U встановлюється взаємно-однозначна відповідність місця розташування їх елементів. Обидві матриці з розмірами N*N умовно розбиваються на N-суміжних квадратних матриць меншого розміру n*n.

Першу з матриць, F, яка формується і може бути відкритою, заповнюють у випадковий спосіб цілими числами з інтервалу $[0\ldots N^2-1]$ таким чином, щоб забезпечувалася рівномірність розподілу вибірки цих чисел із зазначеного інтервалу. Рядки, стовпчики та малі квадрати вказаної матриці F, які, по-суті, є векторами розмірності N в кількості 3*N, є вихідними даними для генерації множини ключів.

Друга матриця, U, яка є формуючою і закритою, являє собою латинський квадрат [3]. Елементи матриці U обираються з інтервалу цілих чисел [1…N], причому завдяки властивостям латинських квадратів в кожному рядку, кожному стовпчику та кожній із суміжних квадратних матриць n*n у складі матриці U немає однакових чисел.

У процедурі генерації ключів використовуються операції перестановок елементів матриць вихрового типу, які забезпечують нелінійні трансформації матриць.

Для реалізації керованих перестановок використовують функцію перестановок $R(V,\overline{P})$, де $\overline{V}$ - вихідний вектор розмірністю N, який однозначно задає місце розташування елементу суміжної квадратної матриці n*n, а $\overline{P}$ - вектор перестановки, який визначає результат перестановки за певним сценарієм.

Кожний компонент вектора $\overline{P}$ має свій порядковий номер і та значення k, причому забезпечуються умови ($1 \leq i, k \leq N$), які обумовлені розмірністю цього вектора. Порядковий номер і вказує на те, який компонент вихідного вектора $\overline{V}$ вибирається при перестановці, а k вказує номер місця, на яке слід поставити цей компонент у результаті перестановки. Таким чином, вектор $\overline{P}$ однозначно задає операцію перестановки компонентів вектора $\overline{V}$.

Зазначена вище операція контрольованих перестановок виконується необхідну кількість ітерації для кожного з малих квадратних матриць n*n, які входять до матриці U. За рахунок того, що кількість компонентів вектора V та кількість елементів малих квадратних матриць n*n співпадає, функція перестановок R використовується для перестановки елементів малих квадратів n*n матриці U. На кресленні наведено приклад сценарію такої перестановки для n=4, N=16.

На прикладі, зображеному на кресленні, $\overline{V}$ = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16), а $\overline{P}$ = (5, 1,2,3,9,7, 11,4, 13,6, 10,8, 14, 15, 16, 12).

В результаті застосування функції R до кожного з малих суміжних квадратних матриць n*n у складі матриці U відбувається нелінійна трансформація матриці U, яка внаслідок взаємної однозначності розташування елементів призводить до нелінійної трансформації матриці F.

За рахунок того, що матриця U та послідовність векторів $\overline{P}$ являють собою закриту інформацію, що зберігається в постійній пам'яті задіяного контролера, вказана інформація є недоступною для читання зовні. Ця інформація використовується як для шифрування, так і для розшифрування даних.

Реалізація запропонованого способу з використанням малих квадратних матриць n*n матриці U в якості векторів, що задають операції перестановок над кожним із 3*N векторів матриці F, дозволяє одержувати одночасно множину $3*N^2$ ключів шифрування довжиною 192 біт кожний.

Можливість одержання заявленого технічного результату при здійсненні корисної моделі може бути підтверджено наступним. Для перевірки роботи алгоритму запропонованого способу генерації ключів була створена програмна модель з використанням персонального комп'ютера. Проведено експеримент з визначенням часу шифрування даних з використанням

запропонованого способу генерації ключів в сукупності з алгоритмом AES. Експеримент показав несуттєве (0.3 %) збільшення затрат процесорного часу при використанні запропонованого способу генерації ключів та зміні ключа при шифруванні кожного 16-байтового блока порівняно з використанням алгоритму AES з незмінним закритим ключем.

Джерела інформації:

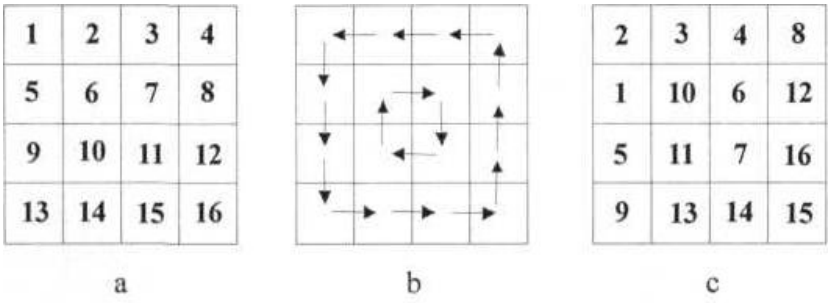
1. Патент Российской Федерации "Эффективное управление генерациями криптографических ключей" №2351078 // Бюллетень Федеральной службы по интеллектуальной собственности, патентам и товарным знакам "Изобретения. Полезные модели", 2009, №9.

2. Патент Российской Федерации "Способ криптографического преобразования цифровых данных" №2309549 // Бюллетень Федеральной службы по интеллектуальной собственности, патентам и товарным знакам "Изобретения. Полезные модели", 2007, №30.

3. Тужилин М.Э. Латинские квадраты и их применение в криптографии // Прикладная дискретная математика, 2012. - №3(17), -С. 47-52.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб генерації ключів для симетричних блочних алгоритмів шифрування, який включає використання керованих операцій нелінійних матричних трансформацій, який **відрізняється** тим, що створюють дві взаємно однозначні за місцем розташування елементів квадратні матриці F та U, кожна з яких має розміри N*N, де N = n*n, а $n \geq 4$ - ціле число, в результаті чого кожна з матриць F та U складається з N - суміжних квадратних матриць n*n, при цьому матрицю F рівномірно заповнюють випадковими цілими числами з інтервалу $[0 \ldots N^2-1]$, а матрицю U заповнюють цілими числами з інтервалу [1….N] за принципом латинського квадрату таким чином, щоб в кожному рядку, кожному стовпчику та в кожному із суміжних квадратних матриць n*n не було однакових чисел, після чого до кожної суміжної квадратної матриці n*n у складі матриці U застосовують функцію перестановок $R(V,P)$, де $\overline{V}$ - вектор розмірності N, який задає вихідне місце розташування елемента суміжної квадратної матриці n*n, а $\overline{P}$ - вектор розмірності N, кожний компонент якого має свій номер і, який вказує на те, який порядковий компонент вихідного вектора $\overline{V}$ вибирається при перестановці, та значення k, яке вказує те, на яке порядкове місце слід поставити цей елемент в результаті перестановки, і в результаті необхідної кількості ітерацій застосування функції перестановок R отримують нову форму матриці U, що внаслідок однозначності розташування елементів призводить до відповідної трансформації матриці F, після чого з необхідної кількості елементів останньої і формують ключі шифрування.



Комп'ютерна верстка В. Мацело

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601