Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет

ДМИТРИШИН ОЛЕКСАНДР ВАСИЛЬОВИЧ

УДК 004.056.55; 681.3.06

МЕТОДИ І ЗАСОБИ БЛОКОВОГО ШИФРУВАННЯ ПІДВИЩЕНОЇ СТІЙКОСТІ НА ОСНОВІ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ЗА МОДУЛЕМ

Спеціальність 05.13.05 – Комп’ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Вінниця – 2012

Дисертацією є рукопис.

Робота виконана у Вінницькому національному технічному університеті Міністерства освіти і науки, молоді та спорту України.

Науковий керівник: доктор технічних наук, професор
Лужецький Володимир Андрійович,
Вінницький національний технічний університет,
завідувач кафедри захисту інформації

Офіційні опоненти: доктор технічних наук, професор
Борисенко Олексій Андрійович,
Сумський державний університет,
завідувач кафедри електроніки і комп'ютерної техніки

доктор технічних наук, професор
Рудницький Володимир Миколайович,
Черкаський державний технологічний університет,
завідувач кафедри системного програмування

Захист відбудеться «18» травня 2012 р. о 12^{00} годині на засіданні спеціалізованої вченої ради Д 05.052.01 у Вінницькому національному технічному університеті за адресою: 21021, м. Вінниця, вул. Хмельницьке шосе, 95, ГНК, ауд. 210.

З дисертацією можна ознайомитись у бібліотеці Вінницького національного технічного університету за адресою: 21021, м. Вінниця, вул. Хмельницьке шосе, 95.

Автореферат розісланий «13» квітня 2012 р.

Учений секретар
спеціалізованої вченої ради С. М. Захарченко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми

В умовах глобальної комп'ютеризації, проблема захисту інформації в комп'ютерних системах та мережах набуває вагомого значення, оскільки побічним продуктом комп'ютеризації є поява комп'ютерної злочинності. Комп'ютер, який є складовою комп'ютерних систем та мереж, у наш час стає найбільш вразливим засобом стосовно здійснення протиправних дій, що направлені на розкрадання не тільки грошей, але й на порушення цілісності, конфіденційності та доступності інформації різного роду. Метою таких дій є отримання несанкціонованого доступу до комерційної таємниці, компрометація або підміна конфіденційних відомостей про конкретних осіб, факти, події тощо.

Одним з ефективних засобів боротьби з перекрученням та несанкціонованим доступом до інформації, що зберігається, обробляється та передається в комп'ютерних системах та мережах є використання криптографічних засобів. Основним напрямом прикладної криптографії є розроблення високошвидкісних та криптографічно стійких методів симетричного блокового шифрування, які повинні легко інтегруватися в комп'ютерні системи. На сьогоднішній день існує ряд блокових шифрів, які забезпечують достатньо високий рівень криптографічної стійкості, але обсяг інформації, яка обробляється, зберігається та передається в комп'ютерних системах з кожним днем збільшується, тому і підвищуються вимоги як до стійкості, так і до швидкості блокового шифрування. Окрім того, сучасні блокові шифри повинні забезпечувати ефективну програмну та апаратну реалізації криптографічних методів захисту.

Одним з перспективних підходів є використання в якості базового примітиву для криптографічних перетворень арифметичних операцій за сталим модулем, які реалізовані в більшості сучасних мікропроцесорів. Такі операції виконуються швидко і, зокрема, в операції множення кожен біт результату множення здебільшого нелінійним чином залежить від усіх бітів перетворюваного блоку даних, а в операції додавання – кожен біт результату залежить від попереднього біту, що є дуже важливим з точки зору криптографічної стійкості. Однак дослідження відомих симетричних блокових шифрів, які базуються на арифметичних операціях за модулем показують, що такі шифри є потенційно вразливими до диференційного криптографічного аналізу на основі мультиплікативних диференціалів. Одним з підходів, який дозволяє протидіяти даному виду аналізу та зокрема лінійному і класичному диференційному криптоаналізу є використання перестановок, дзеркального відображення бітів. Проте, такі операції не є природними для мікропроцесорів і як наслідок – трудомісткими.

Тому актуальною задачею є підвищення криптографічної стійкості блокового шифрування на основі арифметичних операцій за модулем і водночас забезпечення високої швидкості шифрування, яка притаманна даним шифрам.

Важливий внесок у розвиток криптографії та захисту інформації зробили такі вітчизняні та зарубіжні науковці: А. Я. Білецький, О. А. Борисенко, І. Д. Горбенко, В. К. Задірака, І. М. Коваленко, О. Г. Корченко, О. О. Кузнецов, В. М. Рудницький, Е. Біхам, О. Керкгоффс, Л. Кнудсен, М. Мацуї, А. А. Молдовян, Р. Рівест, К. Шеннон, Б. Шнайер, Х. Фейстель та інші.

Зв'язок роботи з науковими програмами, планами, темами

Наукова робота виконувалася відповідно до державної програми про «Інформаційні та комунікаційні технології в освіті і науці» на 2006-2010 роки в Україні, що затверджена постановою Кабінету Міністрів України від 7 грудня 2005 р. № 1153, пункт «Розроблення систем забезпечення інформаційної безпеки функціонування мереж та інформаційних ресурсів» та відповідає підпункту 1.2.5.9 «Розробка теоретичних основ і прикладних методів створення комп'ютерних інформаційно-аналітичних систем, дослідження та розробка методів захисту інформації в комп'ютерних системах і мережах. Методи та системи підтримки прийняття рішень» «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі

природничих, технічних і гуманітарних наук на 2009–2013 роки» (затверджено спільним наказом Міністерства освіти і науки та Національної академії наук України від 26.11.2009 р. № 1066/609).

Результати дисертаційної роботи отримані при виконанні науково-дослідних робіт кафедри захисту інформації Вінницького національного технічного університету в 2008-2011 роках: «Розробка програмного засобу для криптографічного захисту інформації» (ДР №0111U001773) та «Розробка програмного засобу для захисту конфіденційних даних» (договір про творчу співдружність №51/3), у яких автор брав участь як відповідальний виконавець.

Мета і задачі дослідження

Метою дослідження є підвищення рівня захищеності інформації в комп'ютерних системах шляхом розробки методів блокового шифрування підвищеної криптографічної стійкості на основі арифметичних операцій за модулем та засобів, що реалізують ці методи.

Задачі дослідження:

1. Аналіз існуючих методів блокового шифрування, що використовують операцію множення за модулем в якості криптографічного перетворення, та існуючих режимів блокового шифрування.
2. Розробка методів симетричного блокового шифрування на основі арифметичних операцій за модулем, які стійкі до криптографічного аналізу.
3. Аналіз криптографічної стійкості запропонованих методів симетричного блокового шифрування.
4. Розробка програмних та апаратних засобів симетричного блокового шифрування.
5. Експериментальні дослідження швидкості блокового шифрування в комп'ютерних системах.

Об`єкт дослідження – процес криптографічного захисту інформації в комп'ютерних системах з використанням симетричних блокових шифрів.

Предмет дослідження – методи та засоби блокового шифрування підвищеної стійкості на основі арифметичних операцій за модулем.

Методи дослідження

При розв'язанні поставлених наукових задач в дисертаційній роботі були використані методи криптографії – при розробці методів блокового шифрування; методи теорії чисел – для побудови моделей блокових шифрів та методики формування пар взаємно простих чисел; методи криптології – при аналізі криптографічної стійкості блокового шифрування; методи математичної статистики – при дослідженні розподілу вихідних значень під час експерименту; методологія об'єктно-орієнтованого програмування – для створення програмних засобів блокового шифрування; методи теорії цифрових автоматів – для побудови спеціалізованого процесора.

Наукова новизна одержаних результатів

В результаті виконаних досліджень отримано низку результатів в напрямку підвищення ефективності захисту інформації в комп`ютерних системах та мережах шляхом застосування арифметичних операцій за модулем, методів розгортання ключів та псевдовипадкового зав'язування блоків даних:

– вперше запропоновано метод симетричного блокового шифрування на основі арифметичних операцій за модулем, який передбачає використання комбінованого розгортання ключів, що забезпечує підвищення рівня стійкості блокового шифрування до відомих криптографічних атак за рахунок ускладнення аналізу в 2^p раз (p – кількість блоків, що зашифровуються);

– вперше запропоновано метод симетричного блокового шифрування на основі арифметичних операцій за модулем з псевдовипадковим зав'язуванням блоків даних, який дозволяє підвищити стійкість шифрування до відомих криптографічних атак за рахунок ускладнення аналізу в 2^N раз (N – кількість блоків, що зав'язуються) і забезпечує необмежене поширення помилок на блоки відкритого тексту, у разі підміни блоку зашифрованого тексту;

– вперше запропоновані структурні моделі спеціалізованих процесорів для блокового шифрування, які враховують особливості виконання операцій за модулем і забезпечують підвищення швидкості шифрування порівняно з реалізацією на основі універсальних мікропроцесорів у L разів (L – кількість раундів шифрування);

– удосконалено метод симетричного блокового шифрування на основі арифметичних операцій за модулем шляхом використання однієї з складових секретного ключа як модуля, який забезпечує, порівняно з відомими шифрами підвищення швидкості шифрування в 1,27-7 рази при збереженні рівня стійкості до криптографічного аналізу.

Практичне значення одержаних результатів

Практичне значення отриманих результатів полягає в тому, що запропоновані:

– програмні засоби, які реалізують методи симетричного блокового шифрування на основі арифметичних операцій за модулем і мають високу практичну стійкість до криптографічних атак;

– структури спеціалізованих процесорів для симетричного блокового шифрування на основі арифметичних операцій за модулем, які забезпечують високу швидкість шифрування.

Програмний засіб для криптографічного захисту інформації на основі методу симетричного блокового шифрування на базі арифметичних операцій за модулем та методу розгортання блокових ключів впроваджено у ТОВ «ВІАТЕЛ» (м. Вінниця) у комп'ютерній системі підприємства при криптографічному захисту конфіденційних даних (акт про впровадження результатів дисертаційної роботи від 08 серпня 2011 р.). Програмний засіб для захисту конфіденційних даних на основі методу симетричного блокового шифрування на базі псевдовипадкового зав'язування блоків даних впроваджено у ПП «ВІНБУДІЗОЛ» (м. Вінниця) у комп'ютерній системі підприємства для захищеного зберігання інформації в базі даних підприємства (акт про впровадження результатів дисертаційної роботи від 10 серпня 2011 р.).

Методи симетричного блокового шифрування на основі арифметичних операцій за модулем, а також структури спеціалізованих процесорів, які їх реалізують, впроваджені в навчальний процес Вінницького національного технічного університету на кафедрі захисту інформації в курсах лекцій і курсовому проектуванні з дисциплін «Криптографія та криптоаналіз» і при виконанні кваліфікаційних робіт студентами кафедри (акт про впровадження результатів дисертаційної роботи від 20 червня 2011 р.).

Особистий внесок здобувача

Основні теоретичні та практичні результати, висновки та рекомендації отримані автором самостійно під час проведення досліджень у Вінницькому національному технічному університеті. У друкованих працях, що опубліковані у співавторстві, автору належать: аналітичні вирази для оцінки можливостей використання операції множення за модулем у симетричному блоковому шифруванні [1]; аналіз підходів до використання операції множення в симетричних блокових шифрах, дослідження статистичних властивостей операції множення за довільним модулем у комбінації з іншими групами несумісних операцій [2]; аналіз режимів електронної кодової та зчеплення блоків зашифрованого тексту, методи симетричного блокового шифрування на основі розгортання ключів [3]; методи блокового шифрування на основі псевдовипадкового зав'язування блоків даних [4, 6]; метод генерування взаємно простих чисел, метод розгортання ключів для змінних значень складових секретних підключів [5]; спосіб шифрування на основі операції множення за змінним значенням модуля та пристрої що, його реалізує [14]; спосіб шифрування на основі несумісних груп арифметичних операцій та пристрої що, його реалізує [15-18]; спосіб шифрування на основі арифметичних операцій за модулем із псевдовипадковим зчепленням блоків даних та пристрої що, його реалізує [19, 20].

Усі дослідження проводилися у Вінницькому національному технічному університеті.

Апробація результатів дисертації

Основні положення дисертаційної роботи доповідалися та обговорювалися на:

– 6-й міжнародній науково-практичній конференції «Інтернет-Освіта-Наука», Вінниця, 2008 р.;

– 9-й міжнародній конференції «Контроль і управління в складних системах», Вінниця, 2008 р.;

– міжнародних науково-практичних конференціях «Методи та засоби кодування, захисту й ущільнення інформації», Вінниця, 2009 р., 2011 р.;

– міжнародних науково-технічних конференціях «Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування», Вінниця, 2009 р., 2011 р.;

– 3-й міжнародній науково-практичній конференції «Інформаційна та економічна безпека», Харків, 2010 р.;

– 4-й міжнародній науковій конференції «Комп'ютерні науки та інженерія», Львів, 2010 р.;

– міжнародній науково-практичній конференції «Інформаційні технології та комп'ютерна інженерія», Вінниця, 2010 р.

Публікації. За результатами виконаних досліджень опубліковано 20 робіт, з яких 5 статей у фахових виданнях з переліку ВАК України, 8 тез доповідей, 7 патентів на корисну модель.

Структура і обсяг дисертації

Дисертація складається з вступу, чотирьох розділів, списку використаних джерел та додатків. Загальний обсяг дисертації складає 180 сторінок, з них основний зміст викладений на 135 сторінках, містить 51 рисунки та 16 таблиць. Список використаних джерел складається з 133 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Вступ до дисертації містить обґрунтування актуальності теми, визначення об`єкта і предмета дослідження, формулювання мети і задач роботи, опис основних наукових результатів, їхньої новизни та практичної цінності, надано інформацію про впровадження, апробацію і публікації результатів роботи.

У першому розділі визначено основні області застосування криптографічних методів захисту інформації в комп`ютерних системах і мережах. Визначено основні методи шифрування.

Аналіз сучасних підходів до проектування блокових шифрів дозволив визначити, що блоковий шифр складається з певної кількості раундів. На кожному раунді перетворення виконується перемішування та розсіювання бітів відкритого тексту та секретного ключа з метою встановлення складних статистичних залежностей між відкритим і зашифрованим текстом та перерозподілу надлишковості відкритого тексту на весь зашифрований текст.

Основні методи, які на сьогоднішній день широко використовуються та забезпечують принципи розсіювання та перемішування під час за шифрування кожного блоку даних на одному й тому ж наборі раундових ключів є методи, які побудовані на основі мережі Фейстеля або її модифікаціях, еластичній мережі та підстановочно-перестановочних мережах.

Спільним недоліком мереж Фейстеля та еластичної мережі є низький ступінь розсіювання. Недоліком підстановочно-перестановочних мереж є неефективність реалізації в сучасних комп`ютерних системах та мережах. Встановлено, що режими блокового шифрування не дозволяють захистити вхід функції шифрування від атак на основі пар відомих відкритих текстів і відповідних зашифрованих тестів. Окрім того, режими блокового шифрування ECB, CBC і CFB є вразливими до атаки «дня народження», що призводить до зменшення стійкості блокового шифрування та спричинює пошук альтернативних режимів блокового шифрування. Аналіз методів об'єднання блокових шифрів показав, що у випадку їх використання виконується підвищення криптографічної стійкості методів симетричного блокового шифрування в 2^n разів за рахунок збільшення обсягу ключової інформації, часу шифрування, апаратної та програмної складності реалізації методів симетричного блокового шифрування, що не завжди є припустимим.

Аналіз сучасних методів симетричного блокового шифрування, які використовують операцію множення за модулем як одну з основних операцій криптографічного перетворення показав, що такі методи є вразливими до диференційного криптоаналізу на основі мультиплікативних диференціалів. Тому є актуальним пошук нових методів шифрування, які були б стійкими до даного виду криптографічного аналізу.

На основі результатів проведеного аналізу сформульовано завдання дисертаційних досліджень.

У другому розділі дисертаційної роботи розроблено метод шифрування блоку даних на основі арифметичних операцій за модулем, методи розгортання блокових ключів, методи псевдовипадкового зав'язування блоків даних та методику формування взаємно простих чисел.

Метод шифрування блоку даних на основі арифметичних операцій за модулем базується на використанні операції множення за модулем *m*. Автор пропонує використовувати набір значень множників та модулів, які є секретними і формуються на основі секретного ключа. Крім того *A* і *m* є взаємно простими цілими додатними числами ($A < m$). Розглянуто два підходи щодо обрання цих значень. Перший підхід передбачає використання модуля $m \in \left[2^n; 2^{n+1} - 1\right]$ (*n* – розрядність блока даних). У такому випадку значення модуля на наступному раунді шифрування має бути більшим за попереднє, що зменшує обсяг ключів, які можуть бути обрані на наступних раундах шифрування і призводить до зменшення криптографічної стійкості блокового шифрування.

Тому запропоновано другий підхід, який передбачає використання модуля, значення якого змінюється залежно від значення блоку даних та обирається з діапазону $\left[2^{n-2}; 3 \cdot 2^{n-2}\right)$. Нехай значення обраного модуля m_O, тоді якщо значення блоку відкритого тексту $P < m_O$, то як модуль *m* використовується це значення, тобто $m' = m_O$. Коли $P \geq m_O$, то значення модуля обчислюється за формулою $m'' = 2^n - m_O$. Для кожного з модулів m' і m'' формуються взаємно прості числа A' і A'', відповідно. Тоді операція множення при обчисленні значення блоку зашифрованого тексту *C* описується таким виразом:

$$C = \begin{cases} (P \cdot A') \bmod m', \text{ якщо } P < m_O; \\ ((P - m_O) \cdot A'') \bmod m'' + m_O, \text{ якщо } P \geq m_O, \end{cases} \quad (1)$$

а при розшифруванні:

$$P = \begin{cases} \left(C \cdot (A')^{-1}\right) \bmod m', \text{ якщо } C < m_O; \\ \left((C - m_O) \cdot (A'')^{-1}\right) \bmod m'' + m', \text{ якщо } C \geq m_O, \end{cases} \quad (2)$$

де $(A')^{-1}$, $(A'')^{-1}$ – обернено мультиплікативні A' і A'' за модулями m' та m'', відповідно.

При виконанні такої операції множення в $\left(2^n - \left|2^{n-1} - m_O\right|\right)$ випадках старший біт блоків відкритого тексту *P*, які знаходяться в діапазонах $[0; m_O]$ і $\left[2^n - m_O; 2^n - 1\right]$ не змінить свого значення. Тому для модифікації старшого біту до та після виконання операції множення використовуються дві несумісні операції: додавання за модулем два та додавання за модулем 2^n.

З урахування вище сказаного розроблено метод шифрування окремого блоку даних, який передбачає реалізацію чотирьох процедур: формування раундових ключів для зашифрування, формування раундових ключів для розшифрування, зашифрування і розшифрування.

Процедура зашифрування блоку відкритого тексту *P* описується виразом:

$$C_j = \begin{cases} \left[\left(\left[C_{j-1} \oplus A_j^{(1)}\right] \cdot A'_j\right) \bmod m'_j + A_j^{(2)}\right] \bmod 2^n, \text{ якщо } C_{j-1} < m'_j; \\ \left[\left(\left[C_{j-1} \oplus A_j^{(1)}\right] - m'_j\right) \cdot A''_j\right) \bmod m''_j + m'_j + A_j^{(2)}\right] \bmod 2^n, \text{ якщо } C_{j-1} \geq m'_j, \end{cases} \quad (3)$$

де C_j – значення блоку зашифрованого тексту після *j*-го раунду перетворення, $j = \overline{1; L}$, $C_0 = P$, $C = C_L$;

$A_j^{(1)}$, $A_j^{(2)}$, A'_j, A''_j – цілі додатні числа, які використовуються на *j*-му раунді;

m'_j, m''_j – модулі, які використовуються на *j*-му раунді перетворення.

Якщо зашифруванню підлягає неповний блок даних, то він доповнюється нулями. Процедура розшифрування блоку зашифрованого тексту *C* описується таким виразом

$$P_j = \begin{cases} \left(\left[P_{j-1} - A_{L-j+1}^{(2)}\right] \bmod 2^n \cdot \left(A'_{L-j+1}\right)^{-1}\right) \bmod m'_{L-j+1} \oplus A_{L-j+1}^{(1)}, \text{ якщо } P_{j-1} < m'_{L-j+1}; \\ \left(\left(\left[P_{j-1} - A_{L-j+1}^{(2)}\right] \bmod 2^n - m'_{L-j+1}\right) \cdot \left(A''_{L-j+1}\right)^{-1}\right) \bmod m''_{L-j+1} + m'_{L-j+1} \oplus \\ \oplus A_{L-j+1}^{(1)}, \text{ якщо } P_{j-1} \geq m'_{L-j+1}, \end{cases} \quad (4)$$

де P_j - значення блоку розшифрованого тексту після *j*-го раунду перетворення, $P_0 = C$, $P = P_L$;

$\left(A'_j\right)^{-1}$, $\left(A''_j\right)^{-1}$ – *j*-ті мультиплікативні обернені A'_j і A''_j за модулями m'_j та m''_j, відповідно.

У процедурах зашифрування і розшифрування для *j*-го раунду шифрування спочатку виконується формування трьох складових $A_j^{(1)}$, $A_j^{(2)}$ і Z_j. На основі значення Z_j обчислюється A'_j і m'_j та залежно від значення модуля m'_j обчислюються m''_j і A''_j, а в процедурі формуванні раундових ключів розшифрування – $\left(A'_j\right)^{-1}$ і $\left(A''_j\right)^{-1}$ для модулів m'_j і m''_j, відповідно.

Для формування трьох основних складових $A_j^{(1)}$, $A_j^{(2)}$ і m_{O_j} раундового ключа RK_j генеруються три псевдовипадкових числа за допомогою генератора на основі регістру зсуву з лінійним зворотним зв'язком (РЗЛЗЗ), який пропонується використовувати не для генерування псевдовипадкових послідовностей нулів та одиниць, а для формування псевдовипадкових чисел.

Початковий стан кожного РЗЛЗЗ формується на основі модифікованого секретного ключа шифрування $K_0 = X_0 \| Y_0 \| Z_0$, який трансформується таким чином, щоб $X_0 \neq 0$, $Y_0 \neq 0$ і $Z_0 \neq 0$. Для формування *j*-го раундового ключа RK_j використовується проміжний ключ

$$KM_j = S_j^{(1)} \| S_j^{(2)} \| S_j^{(3)}, \; KM_0 = K_0, \quad (5)$$

де $S_j^{(1)}$, $S_j^{(2)}$, $S_j^{(3)}$ – значення станів 1-го, 2-го та 3-го РЗЛЗЗ на *j*-му кроці, відповідно.

Перетворення значень станів РЗЛЗЗ описується виразами:

$$A_j^{(1)} = \left(S_j^{(1)} \cdot S_j^{(3)}\right)_L \oplus \left(S_j^{(1)} \cdot S_j^{(3)}\right)_R, \quad (6)$$

$$A_j^{(2)} = \left(S_j^{(1)} \cdot S_j^{(2)}\right)_L \oplus \left(S_j^{(1)} \cdot S_j^{(2)}\right)_R, \quad (7)$$

$$Z_j = \left(S_j^{(2)} \cdot S_j^{(3)}\right)_L \oplus \left(S_j^{(2)} \cdot S_j^{(3)}\right)_R, \quad (8)$$

де $(.)_L$ – старші *n* бітів результату множення значень двох станів РЗЛЗЗ;

$(.)_R$ – молодші *n* бітів результату множення значень двох станів РЗЛЗЗ.

Розглянутий метод блокового шифрування на основі арифметичних операцій за модулем дозволяє забезпечити стійкість до диференційного криптоаналізу на основі мультиплікативних диференціалів.

З метою підвищення криптографічної стійкості блокового шифрування даних запропоновано методи розгортання блокових ключів: ітеративного, групового ітеративного та послідовного.

Суть методу ітеративного розгортання блокових ключів полягає в тому, що блоковий ключ BK_i формується на основі останнього раундового ключа $(i-1)$-го блоку. Блоковим ключем BK_1 є секретний ключ шифрування *K*. У загальному випадку процес формування *i*-го блокового ключа BK_i та раундових ключів описується такими чином:

$$BK_1 = K,\ BK_i = RK_{i-1,L-1}, \tag{9}$$

$$RK_{1,1} = KT(BK_1),\ RK_{i,j} = KT(RK_{i,j-1}),\ RK_{i,1} = BK_i, \tag{10}$$

де $RK_{i,j}$ – *j*-й раундовий ключ для шифрування *i*-го блоку даних, $i = \overline{1; p}$;

$KT(.)$ – функція перетворення *q*-розрядного коду.

Перевага такого методу розгортання ключів полягає в тому, що використовується єдина функція перетворення. Проте, поки не завершиться перша ітерація неможливо виконувати розгортання наступних блокових ключів.

Метод групового ітеративного розгортання блокових ключів передбачає одночасне формування *D* блокових ключів на основі відповідних значень останніх раундових ключів, які використовуються для шифрування *D* попередніх блоків даних. Секретний ключ шифрування *K* складається з *D* початкових блокових ключів, тобто $K = BK_1 \,\|\, BK_2 \,\|\, \ldots \,\|\, BK_D$. Такий секретний ключ шифрування на відміну від ключа, що використовується в методі ітеративного розгортання ключів, має в *D* разів більшу розрядність.

Особливістю запропонованого методу є обчислення *i*-го раундового ключа одночасно для *D* блоків даних, що дозволяє підвищити швидкість шифрування в *D* разів за рахунок використання *D* обчислювальних каналів.

За допомогою методу послідовного розгортання блокових ключів виконується формування кожного наступного блокового ключа на основі попереднього, а обчислення раундових ключів для *i*-го блоку даних на основі *i*-го блокового ключа. У загальному випадку процес формування *i*-го блокового ключа BK_i та раундових ключів описується такими чином:

$$BK_0 = K,\ BK_i = CKT(BK_{i-1}), \tag{11}$$

$$RK_{i,1} = KT(BK_i),\ RK_{i,j} = KT(RK_{i,j-1}). \tag{12}$$

де $CKT(.)$ – функція перетворення *q*-розрядного коду.

Такий метод розгортання блокових ключів дозволяє організувати конвеєрну обробку даних в комп'ютерних системах

Запропоновані методи розгортання ключів забезпечують підвищення рівня стійкості блокового шифрування до відомих криптографічних атак за рахунок ускладнення аналізу в 2^p раз (*p* – кількість блоків, що зашифровуються).

Наприклад, у разі використання РЗЛЗЗ розрядністю *n*=64 та блоків даних довжиною 64 розряди, обсяг даних, який може бути зашифрований в комп'ютерних системах з використанням унікальних ключів буде складати ~ 2^{67} байт. Такий обсяг даних може задовольнити практичні потреби не тільки в теперішній час, але і в майбутньому.

Запропоновані методи блокового шифрування на основі псевдовипадкового зав'язування блоків даних, які базуються на керованому зав'язуванні поточного і декількох

попередніх блоків відкритого та (або) зашифрованого текстів. У загальному випадку функція зашифрування *i*-го блоку відкритого тексту має такий вигляд:

$$C_i = E_K\left(P_i^*\right) \oplus C_i^*, \tag{13}$$

де P_i^* – результат зав'язування блоків відкритого тексту:

$$P_i^* = P_i \oplus P_{i-u} \cdot v_{i,1} \oplus \ldots \oplus P_{i-1} \cdot v_{i,u}; \tag{14}$$

C_i^* – результат зав'язування блоків зашифрованого тексту:

$$C_i^* = C_{i-w} \cdot v'_{i,1} \ldots \oplus C_{i-1} \cdot v'_{i,w}; \tag{15}$$

$\{P_{i-u}, \ldots, P_{i-1}\}$ – множина попередніх блоків відкритого тексту, $i = \overline{1; N}$;

$\{C_{i-w}, \ldots, C_{i-1}\}$ – множина попередніх блоків зашифрованого тексту;

$\{v_{i,1}, \ldots, v_{i,u}, v'_{i,1}, \ldots, v'_{i,w}\}$ – *i*-й вектор керування, $v_{i,j}, v'_{i,j} \in \{0,1\}$.

Початкові групи даних $\{P_{1-u}, \ldots, P_0\}$ та $\{C_{1-w}, \ldots, C_0\}$ формуються на основі вектора ініціалізації, тобто $P_{1-u} = IV_{u-1}$, $P_{2-u} = IV_{u-2}$, …, $P_0 = IV_0$ і $C_{1-w} = IV'_{w-1}$, $C_{2-w} = IV'_{w-2}$, …, $C_0 = IV'_0$. Залежно від обраних параметрів *u* та *w* кількість одночасно пов'язуваних блоків відкритих і зашифрованих текстів може бути як однаковою, так і різною.

Залежно від джерела даних, що використовується у зав'язуванні автором запропоновано три методи блокового шифрування із зав'язуванням блоків: відкритого, зашифрованого і одночасно відкритого та зашифрованого текстів.

Методи блокового шифрування на основі арифметичних операцій за модулем, які передбачають псевдовипадкове зав'язування блоків відкритого та зашифрованого текстів дозволяють забезпечити стійкість блокового шифрування до відомих криптографічних атак за рахунок ускладнення аналізу в 2^N раз (N – кількість блоків, що зав'язуються) і забезпечують необмежене поширення помилок на блоки відкритого тексту, у разі підміни блоку зашифрованого тексту під час передачі даних через незахищені канали зв'язку.

Запропоновано методику формування чисел *A* взаємно простих з деяким *n*-розрядним числом $m = \{m_{n-1}, \ldots, m_1, m_0\}$, $m > 4$ передбачає формування числа *A* за таким правилом:

$$A = \begin{cases} (m + s_1)/2, \textit{ якщо } m_0 = 1; \\ (m + s_2)/2, \textit{ якщо } m_1 = 0, m_0 = 0; \\ (m + s_3)/2, \textit{ якщо } m_1 = 1, m_0 = 0, \end{cases} \tag{16}$$

де $s_1 = \pm 1$, $s_2 = \pm 2$, $s_3 = \pm 4$.

Для знаходження значення оберненого мультиплікативного A^{-1} за модулем *m* автором пропонується такий набір правил, який враховує особливості методики визначення *A* для заданого *m*:

$$A^{-1} \bmod m = \begin{cases} 2, \textit{ якщо } s_1 = 1, m_0 = 1; \\ (m - 2), \textit{ якщо } s_1 = -1, m_0 = 1; \\ (m + s_2)/2, \textit{ якщо } m_0 = 0, m_1 = 0; \\ (m + 4)/4, \textit{ якщо } s_3 = 4, m_0 = 0, m_1 = 1, m_2 = 0; \\ m/2 + (m + 4)/4, \textit{ якщо } s_3 = 4, m_0 = 0, m_1 = 1, m_2 = 1; \\ m/2 + (m - 2)/4, \textit{ якщо } s_3 = -4, m_0 = 0, m_1 = 1, m_2 = 0; \\ (m - 2)/4, \textit{ якщо } s_3 = -4, m_0 = 0, m_1 = 1, m_2 = 1. \end{cases} \tag{17}$$

Для реалізації запропонованих правил визначення A і A^{-1} за модулем m потрібно виконати 1 операцію додавання (віднімання) і зсув коду вправо на 1 (2 або γ) розряди. Це значно простіше порівняно зі складністю обчислень за алгоритмом Евкліда та методом редукції, які вимагають для своєї реалізації виконання до $\log_\alpha 2^n$ операцій, де $\alpha = \left(\sqrt{5}+1\right)/2$.

У третьому розділі дисертаційної роботи виконаний аналіз властивостей перемішування та розсіювання арифметичних операцій за модулем та досліджено 16-розрядний блоковий шифр на основі арифметичних операцій за модулем, практична стійкість блокового шифрування в комп'ютерних системах на основі методів розгортання ключів та псевдовипадкового зав'язування блоків даних.

Аналіз властивостей перемішування та розсіювання арифметичних операцій за модулем показав, що при виконанні операції побітового додавання за модулем два *i*-й розряд результату c_i залежить лише від відповідних *i*-х розрядів двійкових чисел *a* і *b*. В операції додавання за модулем 2^n (*i*-1)-й розряд чисел *a* і *b* приймає участь у формуванні *i*-го розряду результату шляхом формування одиниці переносу в *i*-й розряд, а в операції множення за модулем 2^n значення модуля не впливає на значення розрядів результату множення. Це свідчить про недостатній рівень зав'язування бітів відкритого та зашифрованого текстів. Проте, якщо виконувати множення за довільним значенням модуля *m*, то результат множення буде розраховуватися таким чином:

$$a \cdot b \bmod m = \left(c_{мол.} + c_{ст.}\left(2^n - m\right)\right) \bmod m, \tag{18}$$

де $c_{мол.}$ – n молодші розряди добутку *a* і *b*.

$c_{ст.}$ – n старші розряди добутку *a* і *b*.

У такому випадку *i*-й розряд результату залежить не лише від попередніх розрядів множеного та множника, а ще й від відповідних розрядів модуля. Це дозволяє підвищити криптографічну стійкість шифрування до диференційного криптоаналізу на основі мультиплікативних диференціалів та забезпечити більший рівень розсіювання бітів порівняно з операцією множення за фіксованим значенням модуля.

Перевірка властивостей розсіювання при реалізації запропонованого методу симетричного шифрування блоку даних з використанням множників обчислених за формулою (16) показав, що показник повноти перетворення (d_c), показник лавинного ефекту (d_a), показник відповідності строгому лавинному критерію (d_{sa}) та середня кількість розрядів блоку зашифрованого тексту, яка змінюється при зміні одного розряду коду блоку відкритого тексту (d_1) не досягають своїх оптимальних значень ($d_c = 1$, $d_a \approx 1, d_{sa} \approx 1$ і $d_1 \approx 32$) навіть після 32 раундів перетворень. Тому була запропонована модифікована методика для формування множників A'_j і A''_j, значень модулів m'_j і m''_j, обернено мультиплікативних A'^{-1}_j і A''^{-1}_j за модулем m'_j і m''_j.

Ця методика передбачає такі обчислення:

$$A'_j = 2^{\gamma_j} \cdot q_j + 1, \tag{19}$$

$$m'_j = A'_j \cdot p_j + 2^{\gamma_j},\ m''_j = 2^n - m'_j,\ A''_j = \left(m''_j - 1\right)/2, \tag{20}$$

$$A'^{-1}_j = q_j \cdot p_j + 1,\ A''^{-1}_j = m''_j - 2. \tag{21}$$

Тут γ_j і q_j визначаються з секретного проміжного ключа Z_j, а p_j формується за певним правилом.

Дослідження показали, що при використанні в операції множення множника *A* та модуля *m*, які формуються за допомогою вище наведеної модифікованої методики, після 4-го раунду $d_c = 1,\ d_a \approx 1,\ d_{sa} \approx 1$ та $d_1 \approx 32$. При зашифруванні кожного блоку даних на унікальному ключі, який формується за допомогою методу розгортання блокових ключів, вже після 1-го раунду перетворень $d_c = 1,\ d_a \approx 1,\ d_{sa} \approx 1$ і $d_1 \approx 32$. Для порівняння, в блокових шифрах MARS, RC6 дані показники приймають рекомендовані значення лише після 4-го раунду перетворень, а в Rijndael, Serpent і Twofish після 3-го. Це свідчить про те, що запропонований метод симетричного шифрування блоку даних забезпечує високий рівень розсіювання бітів відкритого тексту.

Дослідження 16-розрядного шифру з розміром відкритих і зашифрованих текстів $n = 16$ розрядів та розміром секретного ключа – $k = 48$ розрядів показали, що кількість раундів шифрування має бути не меншою за 8, щоб протистояти лінійному криптоаналізу.

Результати експериментальних досліджень також показали, що якщо виконувати зашифрування всіх блоків даних на одному й тому ж наборі раундових ключів за допомогою запропонованого методу шифрування блоку даних, то такий метод є вразливим до диференційного криптоаналізу. Проте, якщо використовувати запропонований метод на основі арифметичних операцій за модулем в поєднанні із одним з методів розгортання блокових ключів, то забезпечується високий рівень стійкості.

Для дослідження запропонованих методів блокового шифрування на псевдовипадковість результатів використані емпіричні статистичні дослідження згідно методики, яка пропонувалася для досліджень під час проведення конкурсу на новий стандарт симетричного блокового шифрування AES за допомогою аналізу 7 зашифрованих тестових наборів даних. Результати досліджень наведені в табл. 1.

Аналіз результатів досліджень показує, що запропонований метод шифрування задовольняє основним вимогам, які висуваються до симетричних блокових шифрів.

Таблиця 1 – Результати досліджень 64 бітної реалізації методу шифрування

Порядковий номер тесту	Метод розгортання блокових ключів								
	Ітеративний			Групо ітеративний			Послідовний		
	Кількість тестів, які пройдені з ймовірністю								
	≥ 96,33%	≥ 99%	*P-value* ≥ 0,0001	≥ 96,33%	≥ 99%	*P-value* ≥ 0,0001	≥ 96,33%	≥ 99%	*P-value* ≥ 0,0001
1	188	109	188	188	118	188	188	129	188
2	188	115	188	188	120	188	188	103	188
3	188	124	188	188	107	188	188	102	188
4	188	140	188	188	119	188	188	110	188
5	188	115	188	188	119	188	188	107	188
6	188	109	188	188	118	188	188	119	188
7	188	120	188	188	129	188	188	113	188

Для дослідження запропонованого методу блокового шифрування на основі псевдовипадкового зав'язування блоків даних на псевдовипадковість результатів шифрування використано таку саму методику, що і при дослідженні методів розгортання блокових ключів. При цьому, сукупна кількість блоків даних, що зав'язувалася для кожного з досліджуваних методів дорівнювала 8.

Аналіз отриманих результати показав, що надлишковість відкритого тексту перерозподіляється на зашифрований текст за рахунок зав'язування поточного блоку відкритого тексту з попереднім блоком даних вже з 3-го раунду шифрування. Крім того, складність криптографічного аналізу ускладнюється за рахунок зчеплення з 8 попередніми блоками даних в 2^8 раз.

У четвертому розділі дисертаційної роботи розроблено алгоритми та програмні засоби для реалізації запропонованих методів шифрування мовою C++ відповідно до вимог, які висувалися до блокових шифрів, що були конкурсантами на стандарт шифрування AES.

Дані програмні засоби дозволяють формувати набори даних відповідно до методик, які використовувалися при дослідженні симетричних блокових шифрів на конкурсах AES та NESSIE. Аналіз результатів не виявив відхилення від рівномірного закону розподілу даних в зашифрованому тексті, що свідчить про наявність високої практичної стійкості блокового шифрування.

Наведено опис програмних засобів у вигляді криптографічних модулів, які описані мовою С++ і реалізують методи симетричного блокового шифрування підвищеної стійкості на основі арифметичних операцій за модулем, методи розгортання ключів та псевдовипадкового зав'язування блоків даних, що призначені для інтегрування до різних комп'ютерних систем. Програмний засіб для захисту комп'ютерної інформації на основі методів шифрування, що базуються на арифметичних операціях за модулем та розгортанні блокових ключів, впроваджено у комп'ютерну систему ТОВ «ВІАТЕЛ». Розроблений програмний засіб використовується для шифрування конфіденційних даних користувачів комп'ютерною системою під час виконання операцій запису або зчитування інформації з постійно запам'ятовуючого пристрою.

Програмний засіб для криптографічного захисту на основі арифметичних операцій за модулем і псевдовипадковому зав'язуванні блоків даних, впроваджено у ПП «ВІНБУДІЗОЛ» при захищеному зберіганні інформації в базі даних підприємства. Даний програмний засіб дозволяє виконувати розшифрування захищеної інформації перед початком оброблення даних, що зберігається в базі даних підприємства, та зашифровувати дані після завершення роботи з ними.

Розроблено структурну схему спеціалізованого процесора для блокового шифрування на основі арифметичних операцій за модулем, розгортання ключів та псевдовипадкового зав'язування блоків даних, яка враховує особливості виконання операцій за модулем. Узагальнена структурна схема спеціалізованого процесора для блокового шифрування зображено на рис. 1.

В цій структурі передбачений інтерфейс, який дозволяє інтегрувати розроблений спеціалізований процесор в комп'ютерну систему.

Розглянуто два підходи щодо реалізації блоку шифрування даних. Перший полягає в тому, що раундові перетворення виконуються в ітеративному режимів. Запропоновано структуру блоку шифрування, яка наведена на рис. 2. Другий підхід передбачає конвеєрний режим обробки, який забезпечується апаратурою, що потрібна для реалізації L раундів.

Аналіз різних реалізацій спеціалізованих процесорів показав, що вони дозволяють реалізувати багатоканальні обчислення для шифрування даних при використанні алгоритмів групового ітеративного розгортання ключів, а також для алгоритмів псевдовипадкового зав'язування блоків даних згідно схем паралельної обробки даних. Метод послідовного розгортання ключів дозволяє виконувати обчислення згідно схеми конвеєрної обробки даних. Це забезпечує підвищення швидкості шифрування порівняно з реалізацією на основі універсальних мікропроцесорів у L разів, якщо використовуються L обчислювальних каналів.

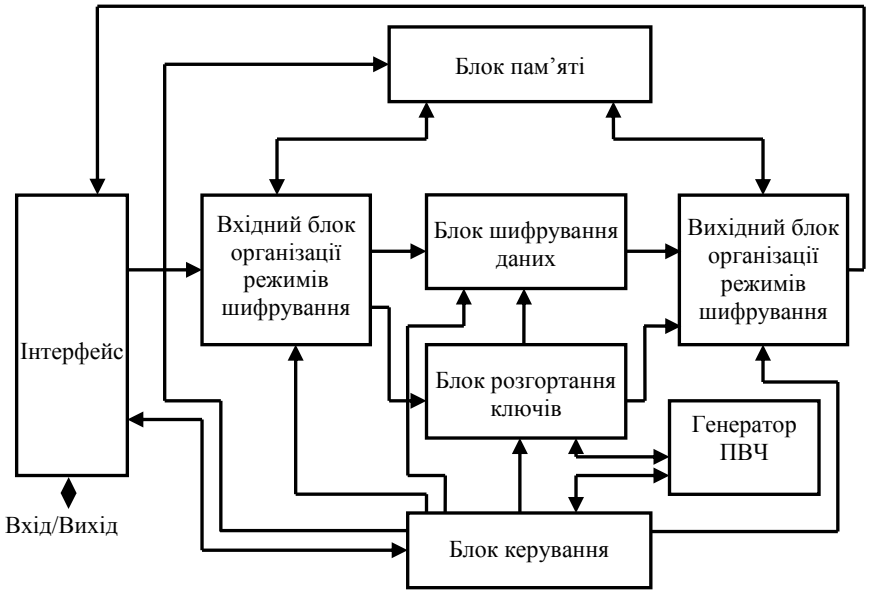

Рисунок 1 –Узагальнена структурна схема спеціалізованого процесора для блокового шифрування

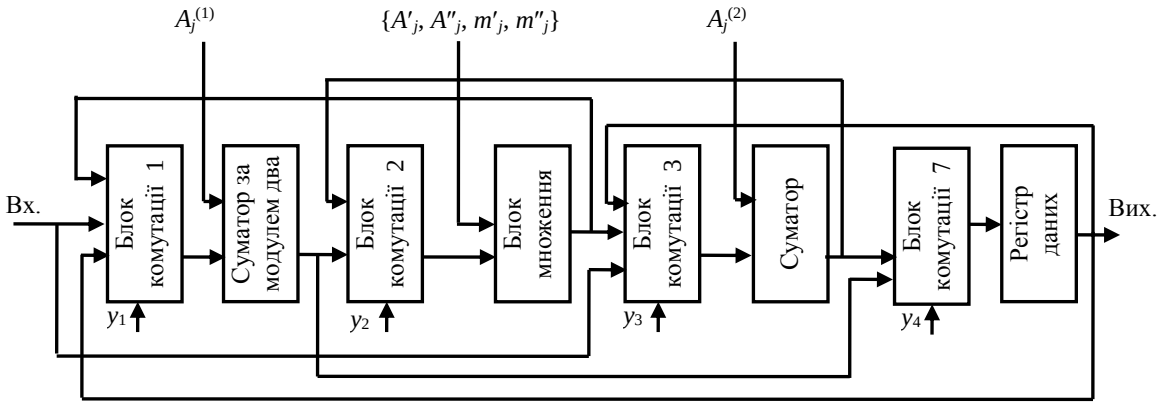

Рисунок 2 – Структура блоку шифрування даних (ітераційний режим)

ВИСНОВКИ ПО РОБОТІ

У дисертаційній роботі розв’язана важлива науково-технічна задача підвищення рівня захищеності інформації в комп’ютерних системах шляхом створення нових методів блокового шифрування на основі арифметичних операцій за модулем, що базуються на розгортанні блокових ключів та псевдовипадковому зав’язування блоків даних.

1. Проведений аналіз методів симетричного блокового шифрування, які використовують операцію множення за модулем як одну з основних операцій криптографічного перетворення показав, що такі методи є вразливими до диференційного криптоаналізу на основі мультиплікативних диференціалів, тому при побудові методів блокового шифрування підвищеної стійкості, в першу чергу, необхідно враховувати саме цей вид аналізу та загальні методи криптографічного аналізу, щоб забезпечити потрібну стійкість блокового шифрування. Основною причиною вразливості відомих блокових шифрів на основі арифметичних операцій до даного виду аналізу є відоме значення модуля, що використовується в операції множення та відсутність залежності результату обчислень від розрядів модуля.

2. Вперше запропоновано метод симетричного блокового шифрування на основі арифметичних операцій за модулем, який передбачає використання комбінованого розгортання ключів. Цей метод порівняно з відомими методами забезпечує збільшення рівня захищеності інформації в комп’ютерних системах за рахунок підвищення рівня стійкості блокового шифрування до відомих криптографічних атак шляхом ускладнення криптоаналізу в 2^p раз (p – кількість блоків, що зашифровуються). Особливість цього методу

полягає в тому, що він дозволяє одночасно виконувати обчислення ключів шифрування для декількох блоків даних. Це дозволяє забезпечувати високу швидкість шифрування даних в комп'ютерних системах за рахунок використання декількох обчислювальних каналів.

3. Вперше запропоновано метод блокового шифрування на основі арифметичних операцій за модулем, який передбачає псевдовипадкове зав'язування блоків відкритого та зашифрованого текстів, що забезпечує стійкість блокового шифрування до відомих криптографічних атак за рахунок ускладнення аналізу в 2^N раз (N – кількість блоків, що зав'язуються). Особливість цього методу полягає в тому, що він забезпечує необмежене поширення помилок на блоки відкритого тексту, у разі підміни блоку зашифрованого тексту під час передачі даних через незахищені канали зв'язку. Це підвищує рівень захищеності інформації в комп'ютерних системах за рахунок виявлення спроб несанкціонованого втручання в процес передавання даних.

4. Вперше розроблені структурні моделі спеціалізованих процесорів для блокового шифрування, які за рахунок використання L обчислювальних каналів дозволяють виконувати розгортання ключів і псевдовипадкове зав'язування блоків даних паралельно та забезпечують підвищення швидкості шифрування порівняно з реалізацією на основі універсальних мікропроцесорів у L разів.

6. Удосконалено метод симетричного блокового шифрування на основі арифметичних операцій за модулем, який за рахунок використання однієї зі складових секретного ключа як модуля забезпечує стійкість до диференційного криптоаналізу на основі мультиплікативних диференціалів. Цей метод порівняно з відомими методами забезпечує збільшення швидкості шифрування від 1,27 до 7 разів при збереженні рівня стійкості до статистичного аналізу. Такий результат досягається за рахунок використання розробленої методики формування взаємно простих чисел та обчислення обернено мультиплікативних елементів, яка в 1,6 разів швидша за відомі алгоритми перевірки чисел на взаємну простоту.

7. Експериментальні дослідження показали практичну стійкість розроблених програмних засобів, що реалізують методи симетричного блокового шифрування на основі арифметичних операцій за модулем, методів розгортання ключів та псевдовипадкового зав'язування блоків даних до набору тестів NIST STS, які використовуються при оцінюванні сучасних блокових шифрів. Порівняння запропонованих методів з відомими за показниками швидкості шифрування даних та швидкості розгортання ключів показало, що збільшення швидкості шифрування на основі запропонованих методів досягається за рахунок використання методики формування взаємно простих чисел та можливості розпаралелення обчислень.

8. Результати проведених досліджень впроваджено в ТОВ «ВІАТЕЛ» при криптографічному захисту даних у комп'ютерній системі, ПП «ВІНБУДІЗОЛ» при захищеному зберігання інформації в базі даних підприємства, а також у навчальний процес у Вінницькому національному технічному університеті на кафедрі захисту інформації.

Основні наукові та практичні результати результати відносяться до галузі криптографічного захисту інформації і можуть бути використані в засобах шифрування та у системах обробки інформації під час передачі та зберігання даних.

СПИСОК ОСНОВНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Лужецький В. А. Блокові шифри для режиму роботи ECB / В. А. Лужецький, О. В. Дмитришин // Інформаційні технології та комп'ютерна інженерія. – 2008. – № 1. – С. 154-158. – ISSN 1999-9941.

2. Лужецький В. А. Використання операції множення за модулем в симетричних блокових шифрах / В. А. Лужецький, О. В. Дмитришин // Системи обробки інформації. – 2010. – № 5. – С. 9-14. – ISSN 1681-7710.

3. Лужецький В. А. Альтернативні режими блокового шифрування / В. А. Лужецький, О. В. Дмитришин // Наукові праці Вінницького національного технічного університету. – 2011. – № 1. – 9 с. – Режим доступу до статті: http://www.nbuv.gov.ua/e-

journals/vntu/2011_1/2011-1.files/uk/11valobc_ua.pdf.

4. Дмитришин О. В. Режим керованого зчеплення блоків зашифрованого тексту / О. В. Дмитришин, В. А. Лужецький // Вісник Вінницького політехнічного інституту. – 2009. – № 1. – С. 34-36. – ISSN 1997-9266.

5. Лужецький В. А. Процедури розгортання ключів для блокових шифрів на основі арифметичних операцій за модулем / В. А. Лужецький, О. В. Дмитришин // Інформаційні технології та комп'ютерна інженерія. – 2009. – №2. – С. 69-74. – ISSN 1999-9941.

6. Лужецький В. А. Організація зчеплення блоків для шифрів на основі арифметичних операцій за модулем / В. А., Лужецький, О. В. Дмитришин // «ІНТЕРНЕТ – ОСВІТА – НАУКА – 2008» (ІОН-2008): зб. матер. конф., 7-11 жовтня 2008 р., Вінниця. Т. 2. – Вінниця: УНІВЕРСУМ-Вінниця, 2008. – С. 396-398. – ISBN 978-966-641-268-6.

7. Дмитришин О. В. Виконання арифметичних операцій за довільним модулем / О. В. Дмитришин // Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2009): матер. IV міжн. наук-техн. конф., 8-10 жовтня 2009 р., Вінниця. Частина 1. – Вінниця: ВНТУ, 2009. – С. 14.

8. Дмитришин О. В. Операція множення як базовий криптографічний примітив в симетричних блокових шифрах / О. В. Дмитришин // Системи обробки інформації. – 2010. – № 3. – С. 112. – ISNN 1681-7710.

9. Дмитришин О. В. Використання операції множення за секретним значенням модуля / О. В. Дмитришин // Інформаційні технології та комп'ютерна інженерія: тези допов. міжн. наук-практ. конф., м. Вінниця, 19-21 травня 2010 р.. – Вінниця: ВНТУ, 2010. – С. 270-271. – ISBN 978-966-641-356-0.

10. Дмитришин О. В. Генерування пар взаємнопростих чисел / О. В. Дмитришин // Методи та засоби кодування, захисту й ущільнення інформації: тези допов. ІІ міжн. наук.-практ. конф., м. Вінниця, 22-24 квітня 2009 р. – Вінниця: УНІВЕРСУМ-Вінниця, 2009. – С.140. – ISBN 978-966-641-304-1.

11. Дмитришин О. В. Шифрування в режимі псевдовипадкового зчеплення блоків даних / О. В. Дмитришин // Методи та засоби кодування, захисту й ущільнення інформації: тези допов. ІІІ міжн. наук-практ. конф., м. Вінниця, 20-22 квітня 2011 р. – Вінниця: УНІВЕРСУМ-Вінниця, 2011. – С. 102-103. – ISBN 978-966-641-406-2.

12. Дмитришин О. В. Режими блокового шифрування на рівні розширення підключів / О. В. Дмитришин // Комп'ютерні науки та інженерія: матеріали IV міжн. конф. молод. вчених, м. Львів, 25-27 лист. 2010 р. – Л.: Видавн. Львівської політехн., 2010. – С. 340-341. – ISBN 978-966-553-999-5.

13. Дмитришин О. В. Шифрування даних в режимі зчеплення за ключем / О. В. Дмитришин // Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2011): матеріали V Міжнародної наук-техн. конф., м. Вінниця, 19-21 травня 2011 р. – Вінниця: ВНТУ, 2011. – С. 174. – ISBN 978-966-641-411-6.

14. Патент України на корисну модель № 38795 МПК(2006.01) H04L 9/06. Спосіб шифрування даних для систем обробки в ЕОМ / Лужецький В. А., Дмитришин О.В.; заявник і патентовласник Вінницький національний технічний університет. – № u200714931; заявл. 27.12.07; опубл. 26.01.09, Бюл. № 2.

15. Патент України на корисну модель № 53494 МПК(2006.01) H04L 9/06. Спосіб шифрування даних на основі двох несумісних груп операцій / Лужецький В. А., Дмитришин О.В.; заявник і патентовласник Вінницький національний технічний університет. – № u201003864; заявл. 06.04.10 ; опубл. 11.10.10, Бюл. № 19.

16. Патент України на корисну модель № 53505 МПК(2006.01) H04L 9/06. Спосіб шифрування даних на основі двох несумісних груп операцій / Лужецький В. А., Дмитришин О.В.; заявник і патентовласник Вінницький національний технічний університет. – № u201003895; заявл. 06.04.10; опубл. 11.10.10, Бюл. № 19.

17. Патент України на корисну модель № 53615 МПК(2006.01) H04L 9/06. Спосіб шифрування даних на основі трьох несумісних груп операцій / Лужецький В. А., Дмитришин О.В., Баришев Ю. В.; заявник і патентовласник Вінницький національний технічний університет. – № u201004697; заявл. 20.04.10; опубл. 11.10.10, Бюл. № 19.

18. Патент України на корисну модель № 54025 МПК(2006.01) H04L 9/06. Спосіб шифрування даних на основі трьох несумісних груп операцій / Лужецький В. А., Дмитришин О.В., Баришев Ю. В.; заявник і патентовласник Вінницький національний технічний університет. – № u201004698; заявл. 20.04.10; опубл. 25.10.10, Бюл. № 20.

19. Патент України на корисну модель № 61270 МПК(2006.01) H04L 9/06. Пристрій для шифрування даних в режимі зчеплення блоків даних / Лужецький В. А., Дмитришин О.В.; заявник і патентовласник Вінницький національний технічний університет. – № u201100465; заявл. 17.01.11; опубл. 11.07.11, Бюл. № 13.

20. Патент України на корисну модель № 61271 МПК(2006.01) H04L 9/06. Пристрій для шифрування даних в режимі зчеплення блоків даних / Лужецький В. А., Дмитришин О.В.; заявник і патентовласник Вінницький національний технічний університет. – № u201100469; заявл. 17.01.11; опубл. 11.07.11, Бюл. № 13.

АНОТАЦІЯ

Дмитришин О. В. Методи і засоби блокового шифрування підвищеної стійкості на основі арифметичних операцій за модулем. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп`ютерні системи та компоненти. – Вінницький національний технічний університет, Вінниця, 2012.

Дисертація присвячена розробці методів симетричного блокового шифрування підвищеної стійкості для захисту інформації в комп`ютерних системах.

На основі проведеного аналізу існуючих підходів, щодо розробки методів та режимів блокового шифрування, методів симетричного блокового шифрування на основі арифметичних операцій за модулем розроблені методи шифрування підвищеної криптографічної стійкості на основі арифметичних операцій за модулем, в яких модуль використовується як один з складників секретного ключа. Запропоновано методи симетричного блокового шифрування на основі арифметичних операцій за модулем, які передбачають використання комбінованого розгортання ключів і псевдовипадкове зав’язування блоків даних, а також засоби, що реалізують ці методи в комп’ютерних системах. Тестування програмних засобів симетричного блокового шифрування дозволило підтвердити практичну стійкість запропонованих методів шифрування, а також показало збільшення швидкості шифрування порівняно з відомими засобами симетричного блокового шифрування на основі арифметичних операцій.

Ключові слова: криптографія, криптографічна стійкість, криптоаналіз, симетричний блоковий шифр, режими шифрування.

АННОТАЦИЯ

Дмитришин А. В. Методы и средства блочного шифрования повышенной стойкости на основе арифметических операций за модулем. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – Компьютерные системы и компоненты. – Винницкий национальный технический университет, Винница, 2012.

Диссертационная работа посвящена разработке методов симметричного блочного шифрования повышенной стойкости для защиты информации в компьютерных системах.

Усовершенствован метод симметричного блочного шифрования на основе арифметических операций за модулем, который за счет использования модуля как одной из составляющих секретного ключа обеспечивает стойкость к дифференциальному криптографическому анализу на основе мультипликативных дифференциалов.

Разработаны методы развертывания ключей, которые в отличие от существующих, обеспечивают не только шифрование блоков данных на разных ключах, что повышает криптографическую стойкость блочного шифрования, а также позволяют распараллелить вычисление, что повышает скорость шифрования данных.

Разработаны методы блочного шифрования на основе завязывания блоков данных, которые в отличие от существующих, выполняют псевдослучайное завязывание блоков открытого (зашифрованного или открытого и зашифрованного) текстов. Это позволяет повысить стойкость блочного шифрования до известных криптографических атак и методов криптографического анализа и неограниченно распространять ошибки на блоки открытого текста. Последнее свойство предотвращает подмену блока зашифрованного текста во время передачи данных через незащищенные каналы связи.

Практическая реализация ускоренного шифрование на основе предложенных методов блочного шифрование требует наличия быстрых процедур формирования пар взаимно простых чисел и вычисления обратно мультипликативных элементов. Для выполнения этого требования предложенная методика формирования взаимно простых чисел и вычисления обратно мультипликативных элементов.

Установлено, что обеспечивается достаточно высокий уровень перемешивания и низкий уровень рассеивания информации, поскольку используются лишь простые линейные арифметические операции. Однако, данный недостаток блочного шифрование является критическим лишь в том случае, если используется один и тот же набор раундовых ключей при шифрование каждого блока открытого текста.

Исследована статистическая стойкость методов блочного шифрования на основе псевдослучайного завязывания блоков данных и установлено, что избыточность открытого текста во время шифрования данных предложенным методом блочного шифрования на основе метода развертывания ключей перераспределяется на зашифрованный текст за счет завязывания блоков открытого (зашифрованного) и открытого та зашифрованного текстов, начиная с 4-го раунда шифрования для 64 разрядной реализации.

Разработаны рекомендации относительно программной реализации методов симметричной блочного шифрование на основе арифметических операций за модулем, что дало возможность разработать программные средства, которые реализуют методы симметричной блочного шифрование повышенной стойкости на основе арифметических операций за модулем, развертывания ключей и псевдослучайного завязывания блоков данных.

Разработана структурная схема специализированного процессора для блочного шифрование, которая учитывает особенности выполнения операций за модулем и обеспечивает повышение скорости шифрование сравнительно с реализацией на основе универсальных микропроцессоров в L раз и выполнено функциональное описание каждого из его блоков с помощью языка аппаратного описания Verilog HDL.

Ключевые слова: криптография, криптографическая стойкость, криптоанализ, симметричный блочный шифр, режимы шифрования.

ABSTRACT

Dmytryshyn O. V. Methods and means of the block ciphers for increased security based on the arithmetic operations after the module. – Manuscript.

Thesis for the candidate degree of technical sciences on the speciality 05.13.05 – Computer systems and components. – Vinnytsia National Technical University, Vinnytsia, 2012.

The dissertation is devoted to the development of symmetric cipher methods of the increased security for the protection within computer systems.

On the basis of the conducted analysis of existent approaches, in relation to development of methods and modes of the block ciphering, methods of the symmetric block ciphering on the basis of arithmetic operations after the module are development the methods of ciphering for increased cryptographic security based on the arithmetic operations after the module, in that the module is used as one of components of the secret key, and that envisage the driven block chaining, and

combined development of the keys. These methods are implemented as software and hardware means for ciphering within computer systems. Testing of the software means of symmetric block encryption allows to prove the practical durability of the proposed methods, and it also shows increasing of encryption speed comparatively with means of symmetric block encryption based on arithmetic operations.

Keywords: cryptography, cryptographic security, cryptanalyst, symmetric block cipher, modes of cipher.

Підписано до друку 12.04.2012 р. Формат 60х84 1/16.
Наклад 100 прим. Зам. № 2012-049
Віддруковано в інформаційно-видавничому центрі
Вінницького національного технічного університету
21021, Вінниця, вул. Хмельницьке шосе, 95. Тел.: (0432) 59-81-59