Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Безпека інформаційних систем і технологій

«Допущено до захисту»
Зав.кафедрою БІСТ
Сватовський І.І._____
« » червня 2023р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

спеціальність: 125 Кібербезпека

на тему: «Оцінка стійкості сучасних блокових шифрів до атак диференціального криптоаналізу»

оцінка « » Керівник ст. викладач Лисицький. К

Голова ЕК Рецензент к.т.н. Нарєжній О.П.

Лемешко О.В._____ Виконавець студент групи КБ-42

Чубар А.Ю.

Харків – 2023

РЕФЕРАТ

Пояснювальна записка містить 43 сторінки, 5 рисунків, 13 таблиць, 21 джерело.

Актуальність теми. Диференціальний криптоаналіз є одним з основних методів атак на блокові шифри і може дозволити зламати шифр, якщо він не є достатньо стійким. Цей вид атаки базується на використанні статистичних відмінностей між парою зашифрованих текстів, що були отримані з різними ключами. Оцінка стійкості сучасних блокових шифрів до атак диференціального криптоаналізу важлива для забезпечення безпеки комунікаційних систем та захисту конфіденційності даних. Дослідження в цій області дозволяють виявити слабкі сторони шифрів, розробити вдосконалені алгоритми та рекомендації щодо використання блокових шифрів у реальних застосуваннях. Це і формує актуальність нашого дослідження.

Метою дипломної роботи є проведення досліджень та аналізу, спрямованих на визначення рівня стійкості сучасних блокових шифрів до диференціального криптоаналізу.

Для реалізації поставленої мети були сформульовані наступні задачі дослідження:

1) описати поняття сучасних симетричних блокових шифрів;

2) здійснити розгляд сучасних алгоритмів AES та «Калина»;

3) проаналізувати види криптоаналізу сучасних симетричних блокових шифрів;

4) описати диференціальний криптоаналіз сучасних симетричних блокових шифрів;

5) розробити програмну реалізацію шифрів «Калина» та AES;

6) на основі різних видів тестувань оцінити стійкість заданих шифрів;

7) порівняти стійкість шифрів «Калина» та AES та зробити висновки;

Об'єктом дослідження дипломної роботи є сучасні блокові шифри, які використовуються для захисту конфіденційності інформації.

Предметом дослідження є оцінка стійкості сучасних блокових шифрів до атак диференціального криптоаналізу.

Методи дослідження: математичне моделювання та комп’ютерні експерименти із варіантами технологічної схеми.

Практичне значення одержаних результатів визначається тим, що отримані результати досліджень можуть використовуватись для розробки рекомендацій щодо використання блокових шифрів, покращення їхніх алгоритмів, внесення змін у стандарти криптографічного захисту та розробки нових шифрів з більшою стійкістю до диференціального криптоаналізу.

Ключові слова: СИМЕТРИЧНИЙ БЛОКОВИЙ ШИФР, ДИФЕРЕНЦІАЛЬНИЙ КРИПТОАНАЛІЗ, AES, КАЛИНА, АЛГОРИТМ, S-БЛОК, КЛЮЧ, СИМЕТРИЧНЕ ШИФРУВАННЯ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І СИМВОЛІВ

DES	-	Data Encryption Standard
AES	-	Advanced Encryption Standard
GSM	-	Groupe Spécial Mobile
SPN	-	Substitution-Permutation Network
EDE	-	Encrypt-Decrypt-Encrypt
RSA	-	Rivest Shamir Adleman
DSA	-	Digital Signature Algorithm
ECDSA	-	Elliptic Curve Digital Signature Algorithm
MD	-	Message Digest
SHA	-	Secure Hash Algorithm

ВСТУП

Актуальність теми. З настанням інформаційного століття, кодування та шифри стали необхідними для нормального функціонування суспільства, а постійне вдосконалення інформаційних технологій сприяло інтенсивному розвитку криптографічних та алгебраїчних алгоритмів. Забезпечення властивостей інформаційної безпеки, таких як конфіденційність, цілісність, цілісність і т. д. зазвичай передбачає використання симетричного шифрування. Оскільки симетричні криптографічні перетворення мають низку переваг при практичному використанні з точки зору їх ефективності, швидкості та надійності.

Диференціальний криптоаналіз є одним з основних методів атак на блокові шифри і може дозволити зламати шифр, якщо він не є достатньо стійким. Цей вид атаки базується на використанні статистичних відмінностей між парою зашифрованих текстів, що були отримані з різними ключами. Оцінка стійкості сучасних блокових шифрів до атак диференціального криптоаналізу важлива для забезпечення безпеки комунікаційних систем та захисту конфіденційності даних. Дослідження в цій області дозволяють виявити слабкі сторони шифрів, розробити вдосконалені алгоритми та рекомендації щодо використання блокових шифрів у реальних застосуваннях. Це і формує актуальність нашого дослідження.

На сьогодні теорія аналізу та обґрунтування стійкості блокових шифрів до зазначених атак досить сильно розвинена, їх у свої працях висвітлювали такі вітчизняні і закордонні вчені як: Л.Ковальчук, О.Беспалов, П.Огнев, Н.Лисенко, Л.Скрипник, А.Фесенко, С. Яковлєв, С.Водене, М.Канда, Дж.Демен, В.Реймен та ін.

У багатьох блокових шифрах при шифруванні використовуються декілька різних таблиць замін, послідовність використання яких наперед фіксована (наприклад, алгоритм шифрування Калина та інші). Існують також

БШ, в яких операції підстановок визначаються раундовими ключами (наприклад, ADE).

Мета дослідження є проведення досліджень та аналізу, спрямованих на визначення рівня стійкості сучасних блокових шифрів до диференціального криптоаналізу.. Відповідно до мети, поставлені наступні завдання:

1) описати поняття сучасних симетричних блокових шифрів;

2) здійснити розгляд сучасних алгоритмів AES та «Калина»;

3) проаналізувати види криптоаналізу сучасних симетричних блокових шифрів;

4) описати диференціальний криптоаналіз сучасних симетричних блокових шифрів;

5) розробити програмну реалізацію шифрів «Калина» та AES;

6) на основі різних видів тестувань оцінити стійкість заданих шифрів;

7) порівняти стійкість шифрів «Калина» та AES та зробити висновки;

Об'єкт дослідження є сучасні блокові шифри, які використовуються для захисту конфіденційності інформації.

Предмет дослідження – оцінка стійкості сучасних блокових шифрів до атак диференціального криптоаналізу.

Методи дослідження. У цій роботі застосовується аналіз наукової літератури та практичного досвіду, проводиться систематизація раніше отриманих результатів із проблеми дослідження. Порівнюються існуючі підходи до вирішення поставлених завдань та сучасній оцінці блокових шифрів.

Наукова новизна роботи. Розроблено та узагальнено алгоритми, вивчено атаки на побудовані шифри та показано ступінь стійкість цих шифрів.

Практичне значення одержаних результатів визначається тим, що отримані результати досліджень можуть використовуватись для розробки рекомендацій щодо використання блокових шифрів, покращення їхніх

алгоритмів, внесення змін у стандарти криптографічного захисту та розробки нових шифрів з більшою стійкістю до диференціального криптоаналізу.

1 ДОСЛІДЖЕННЯ СУЧАСНИХ СИМЕТРИЧНИХ БЛОКОВИХ ШИФРІВ

1.1 Поняття сучасних симетричних блокових шифрів

Криптографічний алгоритм – це математична функція, яка використовується для шифрування та дешифрування інформації. До появи комп'ютерів в основі криптографії лежали алгоритми, побудовані за допомогою операцій заміни одних символів іншими – це алгоритми підстановки, або перестановки символів місцями – це алгоритми перестановки [10].

Сучасні криптосистеми використовують обидва типи алгоритмів [13, с.196]. Більше того, існують досить складні перестановні шифри, але сучасні комп'ютери з ними швидко працюють. Використання таких кодів вимагає великого обсягу пам'яті. Основою сучасної криптографії є модульна арифметика та теорія чисел, зокрема, її розділ, присвячений простим числам.

На сьогоднішній день існують перевірені алгоритми шифрування, які при використанні ключа достатньої довжини та при правильній реалізації відносяться категорії криптостійких алгоритмів Однією з найпоширеніших криптографічних класифікацій алгоритмів зображена на рисунку 1.1.

Рисунок 1.1 - Криптографічна класифікація алгоритмів

Джерело: побудовано автором на основі [11;15;18].

Приклади найпоширеніших типів алгоритмів:

1) симетричні алгоритми:

а) блокові алгоритми: DES, $DESX$, $RC5$, Blowfish, «Калина», AES, $3DES$,Twofish, Магма, $IDEA$, Камелія та інші;

б) поточні алгоритми: $RC4$, $A5/1$, $A5/2$,Sober-128, Pike, Wake, SEAL;

2) асиметричні алгоритми: RSA,DSA, ElGamal, $ECDSA$ та ін;

3) хеш-функції: $MD4$, $MD5$, $MD6$, SHA-2, SHA-3, $SWIFF$ [11;15]

У контексті нашого дослідження, детальніше зупинимось на симетричному шифруванні. Так, симетричне шифрування було єдиним методом шифрування до винаходи шифрування з відкритим ключем. Багато країн прийняли свої власні національні стандарти шифрування [3, с.86].

Симетричне шифрування виконується за допомогою лише одного секретного ключа, що називають "симетричним ключем", яким володіють

обидві сторони. Саме цей ключ застосовується для шифрування та розшифрування інформації. Відправник використовує цей ключ перед надсиланням повідомлення, і отримувач використовує його для розшифровки повідомлення. Загальна схема роботи алгоритму симетричного шифрування зображена на рисунку 1.2.

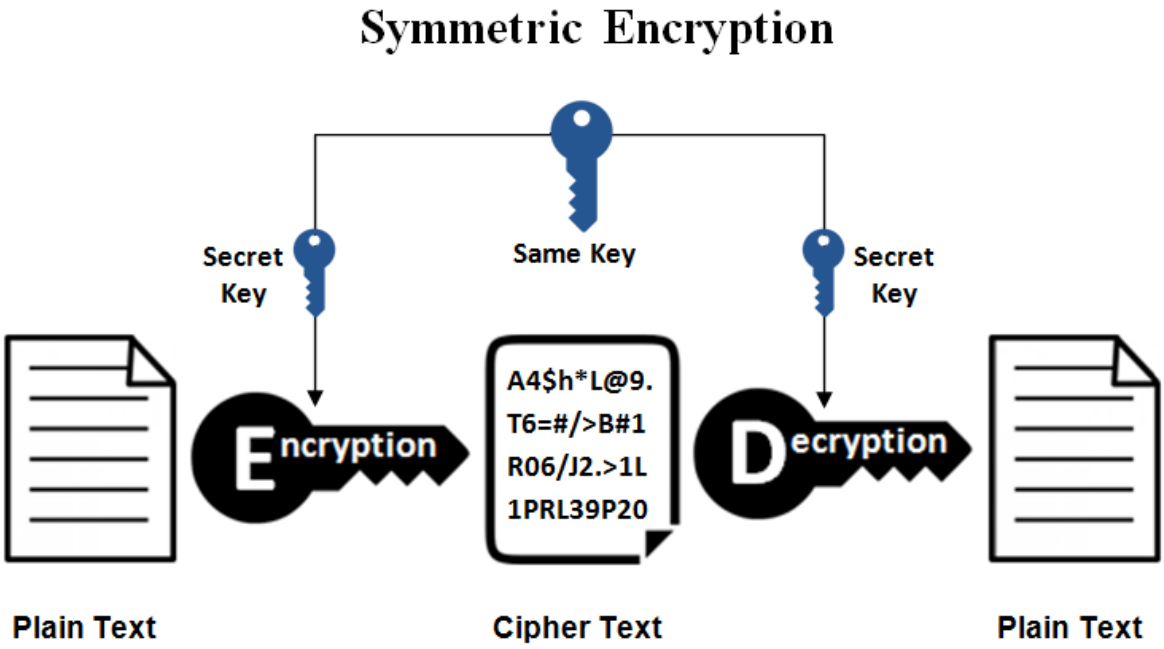

Рисунок 1.2 – Схема симетричного шифрування

Найпоширеніша форма симетричного шифрування відбувається після того, як зашифроване з'єднання було встановлене між клієнтом і сервером із встановленим сертифікатом SSL. Після підключення створюються і обмінюються два 256-бітні сеансові ключі, таким чином може бути утворено зашифроване з’єднання. На відміну від симетричних алгоритмів шифрування, де для шифрування та розшифрування використовується один і той же ключ, в асиметричних це робиться за допомогою двох різних ключів.

У 1976 році в США було затверджено стандарт DES (Data Encryption Standard). Цей стандарт використовувався доти, доки у 2001 році не був прийнято новий стандарт симетричного шифрування AES (Advanced Encryption Standard) на основі алгоритму Rijndael з довжиною ключа 128, 192 та 256 біт [6].

Алгоритм AES замінив попередній алгоритм DES, який рекомендовано використовувати лише у режимі Triple DES, в основному для захисту фінансової інформації. Методи 2DES та 3DES на основі DES відрізняються збільшеною довжиною ключа (2DES − 112 біт, 3DES − 168 біт), у зв'язку з чим зросла їхня криптостійкість [9, с.435].

Алгоритми симетричного шифрування характеризуються такими властивостями:

1) використання одного алгоритму для шифрування та дешифрування;

2) використання одного ключа, що тримається у секреті [12, с.249].

Сучасні алгоритми симетричного шифрування поділяються на блокові та поточні. Для блокових алгоритмів шифрування виконується невеликими порціями – блоками (кратними 32 біт). У блоковому шифрі з двох однакових блоків відкритого тексту виходять однакові блоки шифротексту, що, безумовно, є одним із недоліків таких алгоритмів. Щоб уникнути цього, використовуються потокові шифри, яких перетворення шифрування одного символу відкритого тексту змінюється від одного елемента до іншого.

Поточний шифр – це, по суті, симетричний шифр, у якому кожен символ відкритий текст перетворюється на символ зашифрованого тексту. Перетворення залежить не тільки від ключа, але й від положення символу в потоці відкритого тексту. Такі шифри зазвичай шифрують інформацію в режимі реального часу та використовують для шифрування спеціально згенеровану псевдовипадкову послідовність. Таким чином, потокові шифри підходять для шифрування безперервних потоків. даних (наприклад, голоси або відео) [1, с.75].

Посимвольне шифрування не вносить затримок у криптосистему, тому найважливішою перевагою потокових шифрів є висока швидкість шифрування, еквівалентна швидкості вхідного введення.

Приклад потокового шифру є добре відомий шифр A5/1, який використовується для шифрування повідомлень GSM (Groupe Special Mobile). Через те що спецслужби завжди цікавилися можливістю прослуховування у

своїх цілях, у алгоритм внесено зміни, що дозволяють зламати їх у розумні терміну.

Алгоритм A5/3, розроблений у 2001 році, повинен замінити A5/1 у мобільних системах третього покоління. Його також називають алгоритмом KASUMI (він використовує 64-бітний розмір блоку та 128-бітний ключ у 8-раундовій схемі Фейстеля). В даний час доступно велика кількість різних потокових шифрів [3].

Блокові та поточні шифри реалізовані по-різному. Поточні шифри не дуже підходять для програмної реалізації, але найбільше підходять для апаратної реалізації. У них довжина шифротексту набагато більша за довжину секретного ключа, а послідовність ключів псевдовипадкова і має певний період. Основне завдання потокових шифрів – згенерувати деяку послідовність для шифрування. Очевидно, що якщо послідовність гамма-бітів не має періоду та обрана випадково, то зламати шифр неможливий. Але здається проблематичним мати ключ, рівний за розміром даних, що шифруються.

Практично всі канали передачі для систем потокового шифрування схильні до перешкод. Тому для запобігання втраті інформації вирішується проблема синхронізації шифрування та дешифрування тексту. За способом вирішення цього завдання шифрувальні системи діляться на синхронні та самосинхронізуються [6].

1.2 SP-мережа

Алгоритми шифрування «Калина» та AES, що будуть досліджуватися, побудовані за схемою SP-мережі. Тому потрібно спочатку розібратися в цьому понятті.

SP-мережа (або Substitution–Permutation Network) — це клас блокових шифрів, що складаються з раундів, у яких повторюються серії математичних операцій. Основою агоритму AES та «Калина» є SP-мережа. Раунди шифрування мають структуру зображену на рисунку 1.3, кожен з яких складається з трьох етапів: додавання ключа, нелінійна заміна бітів та лінійна перестановка бітів. Розшифрування виконується у зворотньому напрямку.

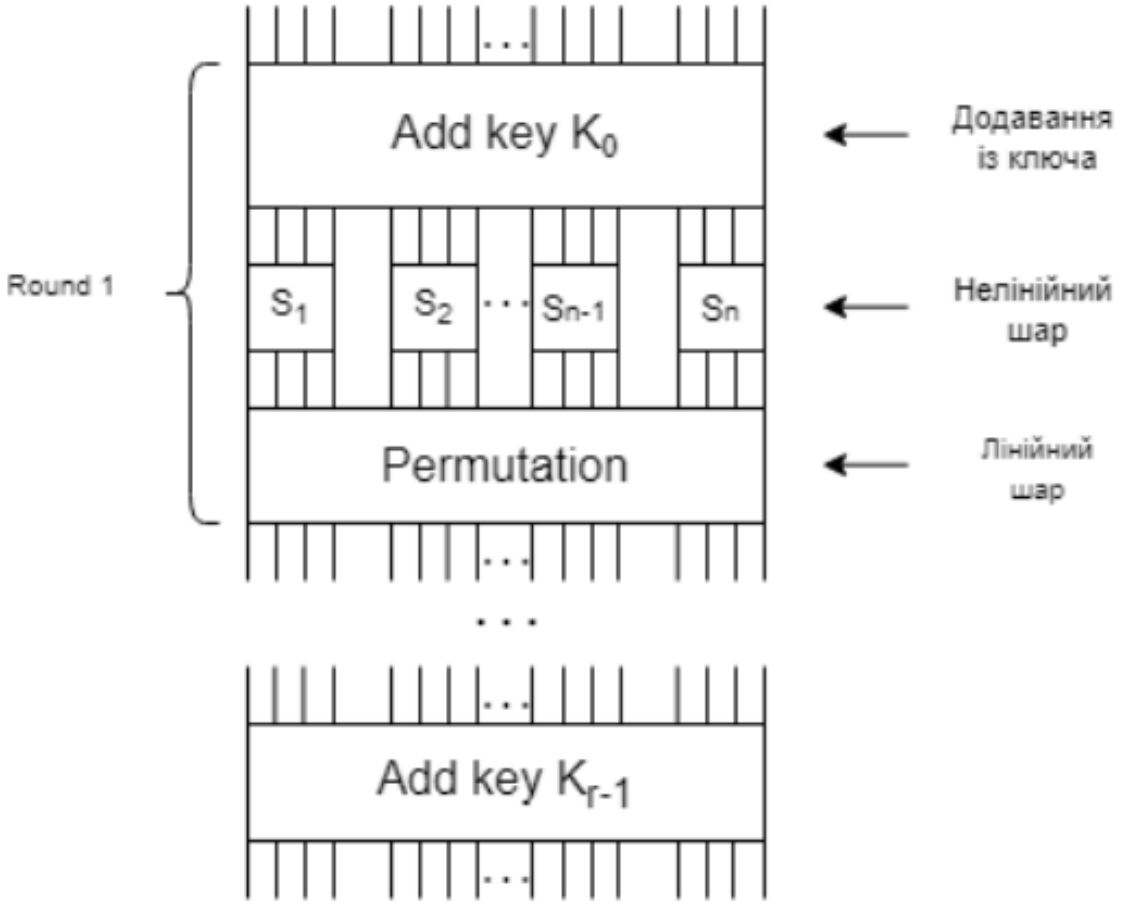

Рисунок 1.3 – Схема шифрування SP-мережі

Розглянемо детальніше принцип роботи SP-мережі. Нехай l та m є цілими натуральними числами. ВТ та ШТ будуть двійковими векторами довжини lm (тобто, lm довжина блоку шифру). SP-мережа складається з двох компонентів, які ми будемо позначати як π_s, π_p:

$$\pi_s : \{0,1\}^l \to \{0,1\}^l \tag{1.1}$$

що є перестановкою 2^l бітових рядків довжини l та

$$\pi_p : \{0, \dots, lm\} \to \{0, \dots, lm\}, \tag{1.2}$$

що являє собою також перестановку цілих чисел від 1 до lm.

Перестановка π_s називається *S-блоком*. Використовується для заміни l бітів на інший набір бітів довжини l, в той же час як π_p використовується для перестановки lm бітів, змінюючи їх порядок. Розглядаючи lm-бітний двійковий рядок, скажімо $x = (x_1, x_2, \dots, x_{lm})$, ми можемо розцінювати x як конкатенацію з m l-бітних підрядків. Які позначимо $x_{\langle 1 \rangle}, x_{\langle 2 \rangle}, \dots, x_{\langle m \rangle}$. Таким чином:

$$x = x_{\langle 1 \rangle} \parallel x_{\langle 2 \rangle} \parallel \cdots \parallel x_{\langle m \rangle} \tag{1.3}$$

SP-мережа складається з N раундів, в кожному з яких (окрім останього) виконується m замін, використовуючи π_s, після чого йде перестановка π_p. Перед кожною операцією заміни буде відбуватися додавання раундового ключа. Зазвичай, це проста операція XOR. Розглянемо алгоритм шифрування SP-мережі. На вході ми маємо ВТ x, на виході маємо отримати ШТ y.

Вхід: $x, \pi_s, \pi_p, (K^1, K^2, \dots, K^{N+1})$.

1) Визначаємо наш ВТ x як $\omega^0 (x \to \omega^0)$.
2) Для r від 1 до $N - 1$ виконуємо:
   а) $\omega^{r-1} \oplus K^r \to u^r$.
   б) Для i від 1 до m виконуємо:
   в) $\pi_s(u^r_{\langle i \rangle}) \to u^r_{\langle i \rangle}$.
   г) $(u^r_{\pi_p(1)}, u^r_{\pi_p(2)}, \dots, u^r_{\pi_p(lm)}) \to \omega^r$.
3) $\omega^{N-1} \oplus K^N \to u^N$.
4) Для i від 1 до m виконуємо:
   а) $\pi_s(u^N_{\langle i \rangle}) \to u^N_{\langle i \rangle}$.
5) $v^N \oplus K^{N+1} \to y$.

Вихід: *y.*

У алгоритмі u^r – вхідні дані для *S-блоку,* а v^r – вихідні дані за нього на раунді *r.* Далі, ω^r отримуємо з v^r шляхом застосування перестановки π_p, після чого u^{r+1} рахуємо *XOR*ом ω^r та раундового ключа K^{r+1}. В останньому раунді перестановка π_p не застосовується. Таким чином, алгоритм шифрування

можна використовувати як алгоритм для розшифрування ШТ, якщо змінити порядок раундових ключів та S-блоки замінити оберненими.

Варто також звернути увагу, що першою та останньою операцією в SP-мережі є додавання ключа, що називається «відбілюванням», і це розглядається як корисний спосіб запобігти тому, щоб зловмисник почав виконувати операції шифрування або дешифрування, якщо ключ йому невідомий.

1.3 Розгляд сучасних алгоритмів AES та «Калина»

Advanced Encryption Standard (AES), також відомий як Rijndael, – симетричний алгоритм блочного шифрування (розмір блоку 128 біт, ключ 128/192/256 біт), прийнятий як стандарт шифрування урядом США за наслідками конкурсу AES [1].

AES-128, AES-192, AES-256 обробляють блоки даних за 10, 12 або 14 ітераціями відповідно. Кожна ітерація є певною послідовністю трансформацій. Усі ітерації однакові крім останньої, з якої виключено одне з перетворень.

Кожен раунд працює з двома 128-бітними блоками: «Поточний» та «ключ раунду». Усі раунди використовують різні «ключі раунду», які виходять з допомогою способу розширення ключа. Цей алгоритм не залежить від даних, що шифруються, та може виконуватися незалежно від фази. шифрування/дешифрування [2].

Алгоритм AES відноситься до симетричних систем шифрування, основою якого є математичний апарат поля Галуа GF (2^8) з породжуючим поліномом $m(x) = x^8 + x^4 + x^3 + x + 1$. Вибір такого породжуючого полінома дозволяє виконувати криптографічні операції над байтами, які розглядаються як елементи кінцевого поля GF(2^8). Використання ПСКВ дозволяє перейти до аналогічних операцій, які можна ефективно реалізувати в полях меншої розмірності GF(2^4).

На рисунку 1.4 представлено структуру алгоритму AES [12].

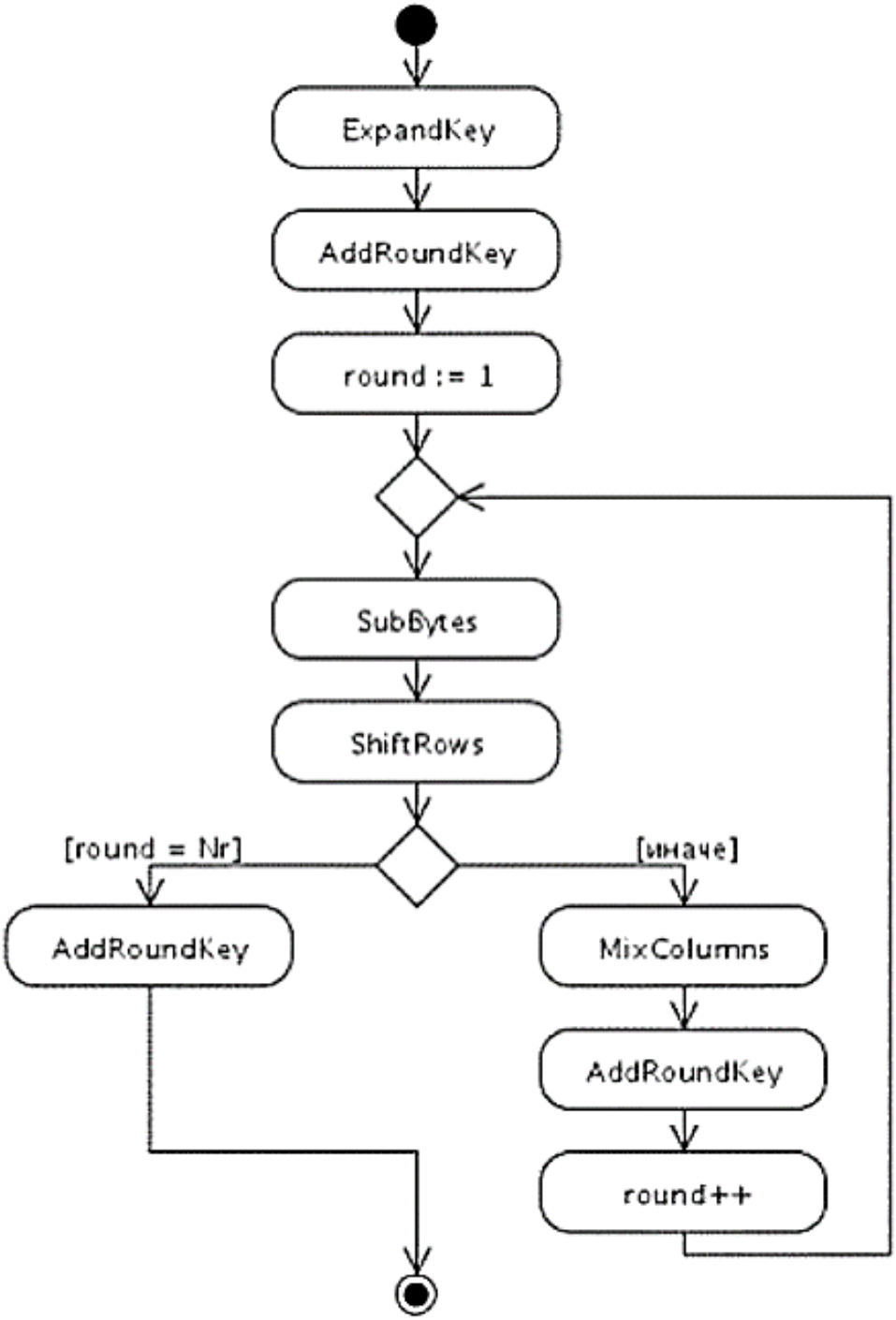

Рисунок 1.4 - Структура алгоритму AES

«Калина» – симетричний блоковий шифр, розроблений на базі ЗАТ «Інститут інформаційних технологій» м. Харкова [15]. Алгоритм має розмір блоку 128, 256 і 512 бітів і підтримує такі ж довжини ключів.

Алгоритм шифрування «Калина» є ітеративною процедурою, що складається з попередньої та фінальної рандомізації та двох різних ітеративних послідовних шифруючих перетворень.

Структура алгоритму аналогічна структурі AES, забезпечує хороше розсіювання та перемішування. Схема шифрування зображена на рисунку 1.5.

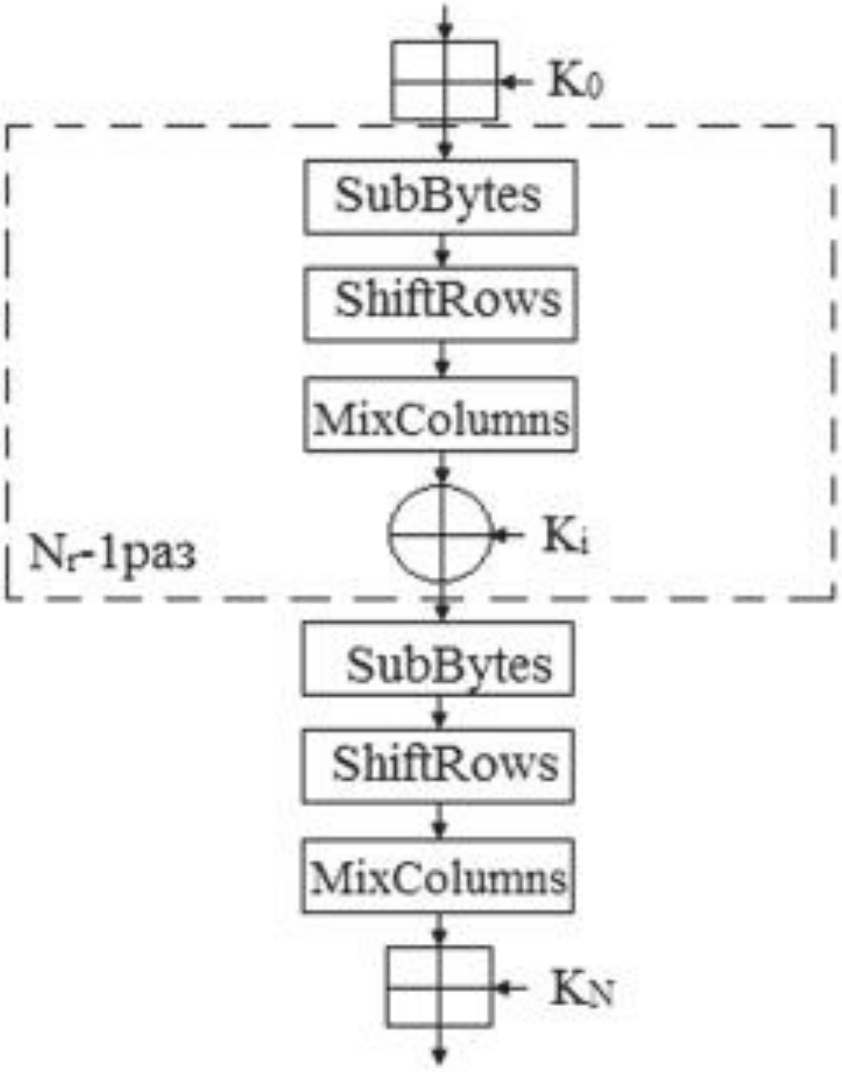

Рисунок 1.5 - Схема шифрування шифру «Калина»

Джерело: [15].

Схема шифрування «Калина» має такі особливості:

– процедура забілювання виконується з допомогою додавання з нульовим підключенням по модулю 264;

– у циклах від першого до Nr-1 циклові підключи вводяться за допомогою операції побітового додавання по модулю 2;

– на останньому циклі шифрування виконується чергове циклове перетворення SubBytes, ShiftRows, MixColumns та додавання з цикловим підключенням за модулем 264;

– у шифрі «Калина» застосовується чотири різних S-блоку [15, с.63].

На вхід кожного шифруючого перетворення подається поточний стан та необхідна кількість ключових даних (під ключ). Відкритий текст копіюється у поточний стан перед початком зашифрування, а після його завершення у поточному стані знаходиться шифртекст. Кількість циклів шифрування залежить від довжини ключа (майстер-ключ), при цьому довжина ключа не може бути менше розміру блоку, що шифрується.

Процес шифрування за допомогою алгоритму «Калина» може бути описаний за допомогою наступної формули:

$$T_{l.k}^{(K)} = \eta^{(K_t)} \circ \psi_l \circ \tau_l \circ \pi_l' \circ \prod_{v=1}^{t-1}(K_l^{(K_v)} \circ \psi_l \circ \tau_l \circ \pi_l') \circ \eta^{(K_0)} \qquad (1.4)$$

де K – ключ шифрування розміром k біт,

$\eta^{(K_t)}$ - функція додавання раундового ключа до матриці за модулем 2^{64},

π_l' - заміна байтів у матриці станів,

τ_l - перестановка елементів матриці станів (циклічний зсув байт вправо),

ψ_l - лінійне перетворення елементів матриці стану над скінченим полем,

$K_l^{(K_v)}$ - додавання за mod 2 матриці стану і раундового ключа K_v.

Генерація раундових ключів відбувається у два етапи:

1) Визначення проміжного ключа з ключа шифрування;

2) Визначення раундових ключів з проміжного ключа.

Розмір проміжного ключа K_σ дорівнює розміру блока і представлений у вигляді матриці розмірами $8 \times c$. Даний ключ генерується з ключа шифрування K за допомогою наступного перетворення:

$$\theta^{(K)} = \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(K_\alpha)} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(K_\omega)} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(K_\alpha)} (1.5)$$

Якщо розмір блока і ключа шифру однакові тоді $K_\alpha = K_\omega = K$. Якщо ж розмір ключа в два рази більший за розмір блока, то $K_\alpha \parallel K_\omega = K$.

Кожен раундовий ключ представлений у вигляді матриці розмірами $8 \times c$. Генерація раундових ключів залежить від ключу шифру, проміжного ключу та індексу раунду.

Раундові ключі K_i з парними індексами ($i \in \{0,2, \dots ,t\}$) обчислюються за допомогою наступного перетворення:

$$\Xi^{(K,K_\sigma.i)} = \eta_l^{(\varphi_i^{(K_\sigma)})} \circ \psi_l \circ \tau_l \circ \pi'_l \circ k_l^{(\varphi_i^{(K_\sigma)})} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(\varphi_i^{(K_\sigma)})} \quad (1.6)$$

де $\varphi_i^{(K_\sigma)} = \eta_l^{(K_\sigma)}(\vartheta \ll (\frac{i}{2}))$, де $\vartheta = \mu_l^{(0x00010001\dots0001)}$.

Якщо розмір ключа дорівнює розміру блока, то $K \gg 32 * i$ – вхідний аргумент для перетворення $\Xi^{(K,K_\sigma.i)}$.

Якщо розмір ключа не дорівнює розміру блока, то як вхідні аргументи для перетворення $\Xi^{(K,K_\sigma.i)}$ використовуються:

$L_{k,l}(K \gg 16 * i)$, для генерації раундових ключів з парними індексами, що діляться на 4 ($i \in \{0,4,8, \dots \}$);

$R_{k,l}(K \gg 64 * [\frac{i}{4}])$, для генерації раундових ключів з парними індексами, що не діляться діляться на 4 ($i \in \{2,6,10, \dots \}$).

Раундові ключі з непарними індексами обчислюються за допомогою раундового ключа минулого раунду з використанням формули:

$$K_i = K_{i-1} \ll \left(\frac{l}{4} + 24\right). \quad (1.7)$$

Варто відмітити дослідження вітчизняних вчених Д.Калинина, Г.Козиної, які провели порівняння швидкодії шифрів «Калина» та «AES». Так, науковці встановили, що шифр «Калина» значно поступається шифру AES у швидкодії. Однак, він може бути успішно використаний при шифруванні інформації тривалого зберігання, й навіть у ситуаціях, коли швидкодія шифру перестає бути критичною [15, с.65].

1.4 Види криптоаналізу сучасних симетричних блокових шифрів

Ключовим завданням захисту є створення стійких алгоритмів шифрування. Будь-який алгоритм, що конструюється, піддається ретельному аналізу з метою виявлення його слабких місць та можливості злому. Алгоритм є відносно стійким доти, доки не будуть виявлено методи та шляхи його аналізу, що дозволяють отримати секретний ключ шифрування значно швидше, ніж це можна зробити з використанням методу «грубого перебору».

До основних видів криптоаналізу сучасних симетричних блокових шифрів відносять:

- лінійний криптоаналіз;
- диференційний криптоаналіз;
- алгебраїчний криптоаналіз;
- метод бумерангу;
- метод зрізаних диференціалів;
- метод неможливих диференціалів;
- теорема;
- інтегральний криптоаналіз [1;2;18;20].

Розглянемо детальніше найпоширеніші. Так, одним із основних методів криптоаналізу є диференціальний криптоаналіз. Для оцінки стійкості проти диференціальної атаки використовується таблиця розподілу різниці або XOR-таблиця.

Диференційна атака використовує нерівномірний розподіл вихідних різниць, коли вхідні дані вибираються з фіксованою різницею. Хоча лінійні

компоненти у криптографічних алгоритмах можуть ефективно розсіювати відмінності, вони можуть допомогти зменшити нерівномірність щодо різниць.

Таким чином, рівномірний диференціальний розподіл в основному виходить з нелінійних компонентів, таких як S-блоки. Оскільки цей вид аналізу буде детально розглянутий у подальшій роботі, не будемо поглиблюватися у його опис на цьому етапі дослідження.

Наступний важливий метод криптоаналізу – лінійний криптоаналіз. Властивість нелінійності S-блоку є показником стійкості проти лінійної атаки. Також для оцінки стійкості використовується таблиця лінійного розподілу чи таблиця лінійної апроксимації. Лінійний криптоаналіз використовує переваги лінійних виразів, що пов'язують між собою біти вхідних даних, біти вихідних даних шифру та біти ключів, які справедливі з високою ймовірністю [19, с.116].

При умові $X = [X_1, X_2, ..., X_n]$ и $Y = [Y_1, Y_2, ..., Y_n]$ - n-бітні вхідні та відповідні вихідні дані шифру, де X_i представляє i-й біт вхідного вектора X, а Y_j представляє j-й біт вихідного вектора Y. При лінійному криптоаналізі шифр апроксимується за допомогою лінійного виразу виду $X_{i1} \oplus X_{i2} \oplus ... \oplus X_{ik} \oplus Y_{j1} \oplus Y_{j2} \oplus ... \oplus Y_{jm} = 0$.

Це рівняння є сумою за модулем 2 k вхідних бітів і m вихідних бітів. Під час проведення лінійної атаки зловмисник визначає подібні лінійні вирази, які мають високу чи низьку ймовірність появи. Знаходження вищевказаних лінійних виразів, що виконуються з великою ймовірністю, або невиконані з великою ймовірністю, показує слабкість шифру. Імовірність виконання лінійного виразу для випадкових значень k + m k вхідних бітів та m вихідних бітів дорівнює 1/2.

При лінійному криптоаналізі використовується відхилення або усунення ймовірності виконання лінійного виразу, що дорівнює ½ [16, с.60]. Наявність очевидного лінійного виразу всім вхідних і вихідних значень свідчить про тривіальну слабкість шифру. Лінійна атака відноситься до атак з використанням відкритого тексту, при яких передбачається, що зловмисник

має інформацію про набір вхідних даних та відповідних вихідних даних шифру, але не може вибрати, які вхідні дані (і відповідні вихідні) доступні. Оцінка імунітету проти лінійного криптоаналізу є суттєвою при розробці безпечних блокових шифрів.

Ще один важливий метод криптоаналізу – алгебраїчний криптоаналіз. Алгебраїчна ступінь і алгебраїчна імунність є показниками стійкості проти атак алгебри. Алгебраїчний криптоаналіз використовує внутрішні математичні структури, які є в криптографічних алгоритмах і намагається визначити вразливості в них. При алгебраїчному криптоаналіз для опису всього криптографічного алгоритму будується алгебраїчна система рівнянь над кінцевим [2].

Немає універсальних методів на вирішення систем алгебраїчних нелінійних рівнянь над кінцевими полями. Це у свою чергу забезпечує практичну криптографічну стійкість алгоритмів. При алгебраїчній атаці будується система алгебри рівнянь над кінцевим полем низького ступеня, яка описує криптографічний алгоритм, і знаходиться її рішення. Основні етапи алгебраїчного криптоаналізу можна описати наступним чином:

1) будується максимальна кількість алгебраїчних рівнянь, які описують криптографічний алгоритм з мінімальним ступенем складових їх термів;

2) вирішується отримана система. В результаті рішення знаходяться біти раундових ключів [1;8].

Щоб представити криптографічний алгоритм шифрування як системи рівнянь необхідно виконати такі дії:

1) розділити деякі складові криптографічного алгоритму на частини, окремо групувати лінійні і нелінійні операції;

2) побудувати у кожній структурній частині алгоритму систему, яка пов'язуватиме вхідні і вихідні дані цієї частини алгоритму;

3) знайти зв'язок вхідних і вихідних даних кожної із структурних частини алгоритму, де відбуваються процеси з іншими частинами, і навіть бітами ключа, вхідних і вихідних даних всього алгоритма. Після представлення

окремих структурних частин алгоритму необхідно записати загальну систему, що описує весь алгоритм.

Алгебраїчна ступінь і імунітет алгебри є показниками стійкості проти алгебраїчних атак. Оптимальними значеннями алгебраїчної міри є значення не нижче 7. Максимальним значенням імунітету алгебри вважається 3 при 441 рівняннях [4].

Такі методи, як метод бумеранга, метод усічених диференціалів, метод неможливих диференціалів є модифікаціями, є посиленими моделями диференціального криптоаналізу.

1.5 Розгляд диференціального криптоаналізу сучасних симетричних блокових шифрів

Метод диференціального криптоаналізу вперше було запропоновано на початку 90-х років минулого століття Е. Біхамом та А. Шаміром для аналізу алгоритм шифрування DES. Хоча у книзі Б. Шнайєра [20] згадується про те, що розробники алгоритму DES знали про можливість такого аналізу ще під час розробки алгоритму у 70-х роках XX століття, широкий загал дізналася про диференціальний криптоаналіз саме з робіт Е. Біхама та А. Шаміра.

Метод диференційного криптоаналізу виявився першим методом, що дозволяє зламати DES в оцінці складності завдань менше 2^{55}. Відповідно до досліджень Е.Біхама, за допомогою даного методу можна провести криптоаналіз DES при зусиллях порядку 2^{37}, але за наявності 2^{47}варіантів вибраного відкритого тексту. Хоча 2^{47} очевидно, значно менше, ніж 2^{55}, необхідність при цьому мати 2^{47}варіантів обраного відкритого тексту перетворює даний варіант схеми криптоаналізу на суто теоретичну вправу [3;4].

Це пов’язано з тим, що метод диференційного криптоаналізу був відомий ще у момент розробки DES, але засекречений з очевидних міркувань, що підтверджується громадськими заявами самих розробників [3].

У дослідженнях Е.Біхама показано, що й змінити порядок слідування блоків заміни в алгоритмі шифрування DES або використовувати інші набори

таблиць підстановок та перестановок, то алгоритм стає відразу набагато слабшим і може бути зламаний менш ніж за половину часу, необхідного для аналізу алгоритму DES за допомогою повного перебору. Це показує значимість знання можливих шляхів аналізу алгоритму, що розробляється. Загалом диференціальний аналіз блокових алгоритмів шифрування зводиться до наступних основних пунктів:

1) знаходження алгоритму шифрування характеристик, які мають максимальні характеристики. Пошук характеристик ведеться на основі диференціальних властивостей нелінійних криптографічних примітивів, що входять до складу алгоритму шифрування;

2) пошук правильних пар текстів із використанням знайдених характеристик;

3) аналіз правильних пар текстів та накопичення статистики про можливі значення секретного ключа шифрування.

Перший пункт, який полягає у пошуку кращих характеристик для більшості алгоритмів, виконується один раз і є теоретичним завданням. Значення характеристик повністю залежить від структури алгоритму шифрування та криптографічних примітивів. Інакше питання постає лише до тих алгоритмів, які мають нефіксовані елементи. До таких алгоритмів можна, наприклад, віднести алгоритм шифрування «Калина», у якого S-блоки заміни можуть вибиратися довільним чином. Для таких алгоритмів пошук характеристик необхідно щоразу починати спочатку, ґрунтуючись на диференціальних властивостях вибраних S-блоків.

Для автоматизації процесу аналізу можна розробити алгоритм пошуку найкращих характеристик, ґрунтуючись на алгоритмах пошуку по дереву. Для таких алгоритмів можна використати паралельні моделі для прискорення пошуку характеристик.

Другий крок аналізу є обчислювально стійким завданням для будь-якого алгоритму шифрування, при цьому не важливо, має він фіксовані або нефіксовані елементи. Аналіз полягає у випробуванні великої кількості пар

текстів з метою визначення правильної пари текстів, тобто тією парою текстів, яку надалі можна використовувати для аналізу та пошуку секретного ключа шифрування.

Даний крок може бути легко представлений у вигляді паралельних обчислень для скорочення часу аналізу [3;4;15;21].

Останній крок легко реалізовується та вимагає набагато менше обчислень у порівнянні з другим кроком. Він може бути реалізований як окремо у вигляді послідовного алгоритму, так і бути включеним до складу паралельних алгоритмів пошуку правильних пар текстів. В останньому, у разі знаходження правильної пари текстів відразу можна провести її аналіз із накопичення статистики про можливе значення секретного ключа.

При умові X′ = [X1′, X2′, ..., Xn′] и X″ = [X1″, X2″, ..., Xn″] - n-бітні вхідні дані шифру, де Xi′ -i-й біт вектора X′, Xi″ -i-й біт вектора X″. ΔX = X′ ⊕X″ = [ΔX1, ΔX2, ..., ΔXn] – різниця вхідних даних, де ΔXi = Xi′ ⊕Xi″, «⊕» – додавання за модулем 2 (побітове що виключає АБО (XOR)) для n-бітних векторів.

Нехай Y′ = [Y1′, Y2′, ..., Yn′] і Y″ = [Y1″, Y2″, ..., Yn″] – відповідні n-бітні вихідні дані шифру, де Yi'-i-й біт вектора Y', Yi"-i-й біт вектора Y ″. ΔY = Y′ ⊕Y″ = [ΔY1, ΔY2, ..., ΔYn] – це різниця вихідних даних, де ΔYi = Yi′ ⊕Yi″.

Імовірність того, що певна різниця вихідних даних ΔY виникає за певної різниці вхідних даних ΔX, в ідеальному випадку дорівнює 1/2n. При диференціальному криптоаналізі використовуються випадки, в яких визначені конкретні різниці вихідних даних ΔY виникають при конкретних різницях вхідних даних ΔX з дуже великою ймовірністю набагато більше, ніж 1/2n. Пари, що складаються з вхідних та відповідних вихідних різниць (ΔX, ΔY), називаються диференціалами.

Диференціальний криптоаналіз відноситься до атак за вибраним відкритим текстом. Це означає, що при проведенні такого виду атаки зловмисник може вибирати вхідні дані і потім досліджує вихідні дані, намагаючись визначити секретний ключ. При проведенні диференціальної

атаки зловмисник з'ясовує, що для певного конкретного значення вхідної різниці ΔX з високою ймовірністю зустрічається конкретне значення вихідної різниці ΔY, і вибирає пари вхідних даних X' і X", що задовольняють певної різниці ΔX. Оцінка імунітету проти диференціального криптоаналізу є суттєвою під час розробки безпечних блокових шифрів.

2 ОЦІНКА СТІЙКОСТІ БЛОКОВИХ ШИФРІВ ДО АТАК ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ

2.1 Аналіз стійкості шифру «Калина» до атак диференціального криптоаналізу

Для виконання аналізу стійкості шифрів «Калина» та AES були створені програмні реалізації цих алгоритмів на мові програмування C++. Ми припускаємо, що зменшені моделі шифрів повторюють властивості повноцінних версій цих шифрів. Такі моделі повторюють властивості динамічного приходу до стану випадкової підстановки та комбінаторні показники. Для збільшення продуктивності під час проведення тестів було використано зменшені 16-бітові моделі шифрів в режимах звичайного шифрування. Тобто вхідні значення в шифри «Калина» та AES дорівнюють 16-бітним значенням замість 128/256-бітних.

Для того, щоб оцінити стійкість цих шифрів до атак диференціального криптоаналізу, в програмні реалізації шифрів «Калина» та AES було додано алгоритм підрахунку максимумів таблиці диференціальних різниць. Значення цих максимумів для кількості циклів шифрування 1-14 зображено в таблиці 2.1.

Таблиця 2.1 - Максимуми таблиці диференціальних різниць для «Калини»

Кількість циклів	MAX
1	65536
2	448
3	18
4	18
5	18
6	20
7	20
8	20

Продовження таблиці 2.1- Максимуми таблиці диференціальних різниць для «Калини»

9	20
10	20
11	20
12	20

За результатами тестування можна побачити, що шифр «Калина» на третьому циклі шифрування приходить до значення 18. На інших кількостях циклів значення максимумів таблиці диференціальних різниць не опускається нижче 18. Це відбувається, тому що будь-який сучасний блоковий шифр через певну кількість циклів приходить до стану випадкової підстановки. Зменшена модель шифру «Калина» набуває цей стан після трьох циклів шифрування.

Для того, щоб впевнитися в результатах і об’єктивно оцінити стійкість шифру «Калина», можна змінити значення ключів та ще раз провести попереднє тестування. В таблиці 2.2 наведено значення максимумів таблиці диференціальних різниць для 10 різних ключів на різних кількостях циклів шифрування.

Таблиця 2.2 – Тестування зі зміною ключа для «Калини»

Кількість циклів	Номер версії ключа									
	1	2	3	4	5	6	7	8	9	10
1	65536	65536	65536	65536	65536	65536	65536	65536	65536	65536
2	384	352	384	448	512	352	352	384	448	384
3	20	20	18	18	20	18	18	20	18	18
4	20	18	18	20	20	18	18	18	20	18
5	20	20	20	18	20	20	18	20	18	20
6	20	20	18	18	20	18	20	18	18	18
7	18	18	18	20	18	20	18	18	20	18
8	20	18	18	18	20	18	18	18	20	20

Продовження таблиці 2.2 – Тестування зі зміною ключа для «Калини»

9	20	18	20	18	20	20	18	18	18	20
10	20	18	18	20	18	20	20	20	18	18
11	18	20	18	20	18	18	18	20	18	20
12	20	20	20	18	18	18	20	18	20	18

Таблиця 2.3 показує середні значення максимумів таблиці диференціальних різниць для 10 різних ключів на різних кількостях циклів шифрування.

Таблиця 2.3 – Середні значення максимумів для «Калини»

Кількість циклів	Середнє значення MAX
1	65536
2	400
3	18,8
4	18,8
5	19,4
6	18,8
7	18,6
8	18,8
9	19
10	19
11	18,8
12	19

Тепер змінимо 10 різних значень S-блоків та знову проведемо тестування. Результати максимумів таблиці диференціальних різниць для різних S-блоків показано у таблиці 2.4.

Таблиця 2.4 – Тестування зі зміною S-блоків для «Калини»

Кількість циклів	Номер версії S-блоків									
	1	2	3	4	5	6	7	8	9	10

Продовження таблиці 2.4 – Тестування зі зміною S-блоків для «Калини»

1	65536	65536	65536	65536	65536	65536	65536	65536	65536	65536
2	352	448	512	448	384	352	352	384	352	448
3	18	20	18	18	20	18	18	20	20	18
4	20	18	20	18	18	18	20	20	18	20
5	20	18	18	20	18	20	18	20	20	20
6	18	20	18	20	20	18	18	18	20	18
7	18	18	20	20	20	18	18	18	20	18
8	20	18	18	18	20	20	18	20	18	18
9	18	18	20	20	18	18	20	18	20	20
10	20	20	20	18	18	18	18	20	18	18
11	18	20	18	20	20	20	20	18	18	18
12	20	18	18	20	18	20	18	18	20	20

Таблиця 2.5 показує середні значення максимумів таблиці диференціальних різниць для 10 різних S-блоків на різних кількостях циклів шифрування.

Таблиця 2.5 – Середні значення максимумів для «Калини»

Кількість циклів	Середнє значення MAX
1	65536
2	403,2
3	18,8
4	19
5	19,2
6	18,8
7	18,8
8	18,8
9	19
10	18,8
11	19

Продовження таблиці 2.5 – Середні значення максимумів для «Калини»

12	19

Виходячи з результатів таблиць можна зробити висновок, що при зміні ключа або S-блоків все одно на третьому циклі блоковий шифр «Калина» переходить у стан випадкової підстановки. Тобто стійкість ніяким чином не залежить від зміни цих параметрів.

Побудуємо загальну таблицю 2.6 середніх значень максимумів таблиці диференціальних різниць після проведення тестів по зміні ключа та S-блоків.

Таблиця 2.6 – Середні значення максимумів після тестів для «Калини»

Кількість циклів	Середнє значення MAX після тесту зі зміною ключа	Середнє значення MAX після тесту зі зміною S-блоків	Загальне середнє значення MAX
1	65536	65536	65536
2	400	403,2	401,6
3	18,8	18,8	18,8
4	18,8	19	18,9
5	19,4	19,2	19,3
6	18,8	18,8	18,8
7	18,6	18,8	18,7
8	18,8	18,8	18,8
9	19	19	19
10	19	18,8	18,9
11	18,8	19	18,9
12	19	19	19

2.2 Аналіз стійкості шифру AES до атак диференціального криптоаналізу

Проведемо аналогічні тести з аналізу стійкості шифру AES до атак диференціального криптоаналізу. Для розрахунків використовувалася зменшена 16-бітова модель шифру в режимі звичайного шифрування. Тобто вхідні значення в шифр AES дорівнюють 16-бітним значенням.

Значення максимумів таблиці диференціальних різниць для кількості циклів шифрування 1-14 зображено в таблиці 2.7.

Таблиця 2.7 - Максимуми таблиці диференціальних різниць для AES

Кількість циклів	MAX
1	65536
2	3652
3	18
4	18
5	20
6	20
7	18
8	20
9	18
10	18
11	20
12	20

В результаті тестування можна зробити висновок, що шифр AES на третьому циклі шифрування приходить до значення 18. На інших кількостях циклів значення максимумів таблиці диференціальних різниць не опускається нижче 18. Тобто зменшена модель шифру AES, як і зменшена модель шифру «Калина» набуває стан випадкової підстановки після трьох циклів шифрування.

Для того, щоб точно оцінити стійкість шифру AES, змінимо значення ключів та ще раз проведемо попереднє тестування. В таблиці 2.8 наведено

значення максимумів таблиці диференціальних різниць для 10 різних ключів на різних кількостях циклів шифрування.

Таблиця 2.8 – Тестування зі зміною ключа для AES

Кількість циклів	Номер версії ключа									
	1	2	3	4	5	6	7	8	9	10
1	65536	65536	65536	65536	65536	65536	65536	65536	65536	65536
2	3652	3864	3394	3624	3512	3512	3624	3652	3512	3864
3	18	18	20	20	18	20	18	18	18	20
4	20	18	20	18	18	20	20	20	18	18
5	18	20	18	18	18	20	18	20	18	20
6	18	20	20	20	20	20	18	18	20	18
7	20	18	20	20	18	18	20	20	20	20
8	20	20	20	18	20	20	18	18	18	20
9	20	18	18	20	18	20	20	20	18	18
10	20	18	20	18	20	18	18	20	20	20
11	20	20	18	20	20	20	20	18	18	20
12	20	18	20	18	18	20	20	18	20	18

Таблиця 2.9 показує середні значення максимумів таблиці диференціальних різниць для 10 різних ключів на різних кількостях циклів шифрування.

Таблиця 2.9 – Середні значення максимумів для AES

Кількість циклів	Середнє значення MAX
1	65536
2	3621
3	18,8
4	19
5	18,8
6	19,2

Продовження таблиці 2.9 – Середні значення максимумів для AES

7	19,4
8	19,2
9	19
10	19,2
11	19,4
12	19

Тепер змінимо 10 різних значень S-блоків та знову проведемо тестування. Результати максимумів таблиці диференціальних різниць для різних S-блоків показано у таблиці 2.10.

Таблиця 2.10 – Тестування зі зміною S-блоків для AES

Кількість циклів	Номер версії S-блоків									
	1	2	3	4	5	6	7	8	9	10
1	65536	65536	65536	65536	65536	65536	65536	65536	65536	65536
2	3624	3512	3652	3652	3512	3864	3624	3394	3864	3512
3	20	20	18	20	18	18	18	20	18	18
4	20	20	18	18	20	18	20	18	20	20
5	18	20	20	18	20	20	18	18	18	20
6	20	18	18	18	20	18	18	20	20	18
7	18	18	20	20	18	18	20	20	18	20
8	20	20	18	18	20	20	20	18	20	20
9	20	18	20	20	18	18	20	20	18	20
10	18	20	20	18	20	20	18	18	20	18
11	20	20	18	20	18	18	20	20	18	20
12	20	20	20	18	18	20	18	20	18	18

Таблиця 2.11 показує середні значення максимумів таблиці диференціальних різниць для 10 різних S-блоків на різних кількостях циклів шифрування.

Таблиця 2.11 – Середні значення максимумів для AES

Кількість циклів	Середнє значення MAX
1	65536
2	3621
3	18,8
4	19,2
5	19
6	18,8
7	19
8	19,4
9	19,2
10	19
11	19,2
12	19

Виходячи з результатів таблиць можна зробити висновок, що при зміні ключа або S-блоків все одно на третьому циклі блоковий шифр AES, як і шифр «Калина» переходить у стан випадкової підстановки. Тобто ще раз довели, що стійкість ніяким чином не залежить від зміни цих параметрів.

Побудуємо загальну таблицю 2.12 середніх значень максимумів таблиці диференціальних різниць після проведення тестів по зміні ключа та S-блоків.

Таблиця 2.12 – Середні значення максимумів після тестів для AES

Кількість циклів	Середнє значення MAX після тесту зі зміною ключа	Середнє значення MAX після тесту зі зміною S-блоків	Загальне середнє значення MAX
1	65536	65536	65536
2	3621	3621	3621
3	18,8	18,8	18,8

Продовження таблиці 2.12 – Середні значення максимумів після тестів для AES

4	19	19,2	19,1
5	18,8	19	18,9
6	19,2	18,8	19
7	19,4	19	19,2
8	19,2	19,4	19,3
9	19	19,2	19,1
10	19,2	19	19,1
11	19,4	19,2	19,3
12	19	19	19

2.3 Порівняння аналізу шифрів «Калина» та AES

Після проведення всіх тестів можна зробити порівняння стійкості блокових алгоритмів шифрування «Калина» та AES до атак диференціального криптоаналізу відповідно до їх середніх значень максимумів таблиці диференціальних різниць. На таблиці 2.13 показано порівняння цих двох алгоритмів.

Таблиця 2.13 - Порівняння максимумів двох алгоритмів

Кількість циклів	Середнє значення MAX шифру «Калина»	Середнє значення MAX шифру AES
1	65536	65536
2	401,6	3621
3	18,8	18,8
4	18,9	19,1
5	19,3	18,9
6	18,8	19
7	18,7	19,2
8	18,8	19,3
9	19	19,1

Продовження таблиці 2.13 - Порівняння максимумів двох алгоритмів

10	18,9	19,1
11	18,9	19,3
12	19	19

Виходячи з результатів таблиці можна зробити висновок, що сучасні блокові шифри «Калина» та AES через певну кількість циклів набувають властивості випадкової підстановки за диференціальними характеристиками. У заданих алгоритмах це відбувається після третього циклу. На всіх наступних циклах значення не стає меншим.

Для більшої точності результатів було проведено тести із зміною ключів у алгоритмах шифрування. Особливих змін це не дало, максимуми таблиць диференціальних різниць залишилися приблизно такими самими. При зміні S-блоків показники також майже не змінилися, обидва шифри також набувають властивості випадкової підстановки після третього циклу. Відповідно, можна стверджувати, що диференціальні характеристики та динамічні показники приходу шифрів до стану випадкової підстановки на трьох циклах не залежать від зміни значень S-блоків і ключів.

Виходячи з результатів, можна зробити висновок, що український стандарт шифрування "Калина" не поступається стандарту шифрування AES у стійкості до атак диференціального криптоаналізу. Можна навіть підмітити, що на другому циклі шифр "Калина" швидше приходить до стану випадкової підстановки, ніж шифр AES.

ВИСНОВКИ

У дипломній роботі ми провели усебічне дослідження спрямоване на визначення рівня стійкості сучасних блокових шифрів до диференціального криптоаналізу. На основі отриманих даних, можемо зробити наступні висновки:

1) Алгоритми симетричного шифрування – це криптографічні алгоритми, що використовують один і той же ключ для як шифрування, так і розшифрування повідомлень. Основна відмінність симетричного шифрування від асиметричного полягає в тому, що для асиметричного шифрування використовуються пари ключів: публічний (для шифрування) і приватний (для розшифрування), тоді як для симетричного шифрування використовується тільки один спільний ключ.

2) Алгоритми AES і «Калина» є симетричними алгоритмами блочного шифрування та мають високий рівень стійкості і використовуються в сучасних криптографічних застосунках. Однак, AES є більш відомим та широко використовуваним алгоритмом, який набув значного визнання в криптографічній спільноті і має багато реалізацій та документації. Він стандартизований і рекомендований для використання у багатьох сферах, включаючи фінанси, комунікації та інформаційну безпеку. «Калина» є алгоритмом, розробленим в Україні, й він здобуває все більшу популярність, особливо національному рівні. Він пройшов багато криптографічних аналізів і тестувань, що підтверджують його стійкість і ефективність.

3) Симетричні блокові шифри – це криптографічні алгоритми, які використовують один ключ як для шифрування, так і для розшифрування повідомлення. Криптоаналіз симетричних блокових шифрів означає процес визначення ключа або відновлення вхідного повідомлення, використовуючи доступ до зашифрованої інформації. До основних видів криптоаналізу, які застосовуються до сучасних симетричних блокових шифрів відносяться:

лінійний криптоаналіз, диференційний криптоаналіз, алгебраїчний криптоаналіз, метод бумерангу, метод зрізаних диференціалів, метод неможливих диференціалів, теорема та інтегральний криптоаналіз.

4) Диференціальний криптоаналіз є одним з основних методів атак на блокові шифри і може дозволити зламати шифр, якщо він не є достатньо стійким. Він використовує статистичні залежності між різницями вхідних парами блоків і відповідними різницями вихідних парами блоків для виявлення слабких ключів або структурних властивостей шифру. Оцінка імунітету проти диференціального криптоаналізу є суттєвою під час розробки безпечних блокових шифрів.

5) Сучасні блокові шифри «Калина» та AES через певну кількість циклів набувають властивості випадкової підстановки за диференціальними характеристиками. У заданих алгоритмах це відбувається після третього циклу. На всіх наступних циклах значення не стає меншим.

6) Диференціальні характеристики та динамічні показники приходу шифрів до стану випадкової підстановки не залежать від зміни значень S-блоків і ключів.

7) Український стандарт шифрування "Калина" не поступається стандарту шифрування AES у стійкості до атак диференціального криптоаналізу. Обидва алгоритма досить стійкі. Можна навіть підмітити, що на другому циклі шифр "Калина" швидше приходить до стану випадкової підстановки, ніж шифр AES.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Яковлєв С.В. Методика обґрунтування стійкості немарковських симетричних блочних шифрів до диференціального криптоаналізу. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2013, №1(25). С. 74-80.
2. Biham E., Dunkelman O., Keller N. Related-Key Boomerang and Rectangle Attacks, 2005. URL: http://vipe.technion.ac.il (дата звернення 15.05.2023)
3. Biham E., Shamir A., Diff erential Cryptanalysis of DES-like Cryptosystems, Extended Abstract, Crypto'90, SpringerVelgar, 1998. 255 p.
4. Biham E., Shamir A., Diff erential Cryptanalysis of the Full 16-round DES, Crypto'92, Springer-Velgar, 1998. 487 p.
5. Daemen J., Rijmen V. Statistics of correlation and differentials in block ciphers. URL: http://eprint.iacr.org/ 2005/212 (дата звернення 15.05.2023)
6. Goldberg J. AES encryption isn't cracked. URL: https://blog.1password.com/aes-encryption-isnt-cracked/ (дата звернення 15.05.2023)
7. Kalmykov I.A., Katkov K.A., Naumenko D.O, Sarkisov A.B., Makarova A.V. Parallel modular technologies in digital signal processing. Life Science Journal. 2014. № 11(11s). P. 435–438.
8. Kanda M. Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function. Selected Areas in Cryptography. SAC 2000, Proceedings, Springer Verlag, 2001. P. 324 – 338.
9. Park J.H., Moon S.J., Choi D.H., Kang Y.S., Ha J.C. Differential fault analysis for round-reduced AES by fault injection. ETRI Journal. 2011. Vol. 33, № 3. P. 434–442.
10. Schneier B., Kelsey J., Whiting D. Et al. Performance comparisons of the AES submissions. URL: https://www.schneier.com/wp-

content/uploads/2016/02/paper-aes-performance.pdf (дата звернення 15.05.2023)

11. Tao B., Wu H. Improving the biclique cryptanalysis of AES. In: ACISP 2015. Springer, 2015. P. 39–56. URL: https://doi.org/10.1007/978-3-319-19962-7_3 (дата звернення 15.05.2023)
12. Vaudenay S. Decorrelation: a theory for block cipher security. J. of Cryptology, 2003. V. 16, № 4. P. 249 – 286.
13. Горбенко І.Д. Перспективний блоковий симетричний шифр «Калина»: основні положення та специфікації / Горбенко І.Д., Долгов В.І., Олійников Р.В. Прикладна радіоелектроніка. 2007. Т. 6, № 2. С. 195–208.
14. Долгов В.І. Подстановочные конструкции современных симметричных блочных шифров / Долгов В.І., Олійников Р.В., Лисицька І.В. Радіоелектронні і комп'ютерні системи. 2009. № 6 (40). С. 89–93.
15. Калинин Д.А. Быстродействие шифров "Калина" и AES / Калинин Д.А., Козина Г.Л. Радіоелектроніка, інформатика, управління. 2013. № 1. С. 62-65. URL: http://nbuv.gov.ua/UJRN/riu_2013_1_12 (дата звернення 15.05.2023)
16. Ковальчук Л., Беспалов О., Огнев П. Рекурентні алгоритми обчислення кореня довільного степеню у кільці лишків. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2013. №1(25). С. 58-67.
17. Ковальчук Л.В., Алексейчук А.М. Результати досліджень криптографічних властивостей алгоритму шифрування «Калина»». Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації», 2014. №1(25). С. 5-24.
18. Ковальчук Л.В., Лисенко Н.В., Скрипник Л.В. Порушення структури факторгрупи при заміні операцій модульного додавання на по компонентне додавання. Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації», 2014. №1(25). С. 24-34.

19. Фесенко А.В. Поліноміальна еквівалентність атак з відомимвідкритим текстом на довільний симетричний і ендоморфний шифри. Вісник Київського національного університету імені Тараса Шевченка. Серія кібернетика, 2014. №2. С. 115-124.
20. Шнайєр Би., Прикладна криптографія: Протоколи, алгоритми, вихідні тексти мовою Сі.: ТРІУМФ, 2002. 648 с.
21. Яковлєв С.В. Доказова та практична стійкість R-схеми блочного шифрування до диференціального криптоаналізу. Вісник Національного університету "Львівська політехніка" (секція "Комп'ютерні науки та інформаційні технології"). 2013. С. 107-113.