ДОПОВІДЬ НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ТЕМОЮ

«РОЗРОБКА СТІЙКИХ ДО ЛІНІЙНОГО ТА ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ ЗАСОБІВ ШИФРУВАННЯ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ»

Студента групи 1КСУА-14м
Яровенко Анастасії Олексіївни
Спеціальності 8.05020101
"Комп'ютеризовані системи управління та автоматика"

ВСТУП

Актуальність теми

На сьогоднішній день, з розвитком сучасних технологій, з’являється все більше інформаційних сервісів та служб, складних обчислювальних систем, і, окрім очевидних переваг, водночас проявляється все більше вразливостей їх щодо забезпечення інформаційної безпеки.

З цього випливає необхідність захисту інформації, що реалізується за рахунок використання засобів криптографії – алгоритмів шифрування інформації.

З іншої сторони існує поняття криптоаналізу, що направлений на виявлення слабкостей криптографічних алгоритмів. На сьогоднішній день уже існує велика кількість алгоритмів шифрування інформації.

Вони уже були досить добре досліджені, деякі із них уже не становить складності взламати.

ВСТУП

Мета дослідження

Мета даного дослідження полягає у підвищенні стійкості шифру до найпоширеніших видів криптоаналізу: диференційного та лінійного.

Задачі дослідження

- проаналізувати сучасний стан розвитку криптографічних методів захисту інформації і розглянути основні принципи побудови блочних шифрів;

- розробити метод підстановки з високим ступенем стійкості;

- розробити метод перестановки з високим показником стійкості;

- застосувати розрблені методи підстановки та перестановки для створення блочного шифру, що зберігатиме їх високі криптографічні та обчислювальні властивості.

ВСТУП

Об’єкт дослідження

Об’єктом даного дослідження є процес обробки даних в комп’ютерних системах та мережах.

Предмет дослідження

Предметом дослідження є методи шифрування, які забезпечують високу стійкість до лінійного та диференційного криптоаналізу.

Методи досліджень

У даній роботі використовуються методи лінійної алгебри для формування гніздових мереж, теорія імовірності для визначення лінійної апроксимації та абстрактної алгебри для визначення нелінійних блоків підстановки.

ВСТУП

Наукова новизна одержаних результатів

1. Запропоновано метод для формування блоків перестановки на основі використання трьохрівневих гніздових мереж, який, на відміну від існуючих, дозволяє збільшити кількість активних блоків підстановки на кожному раунді шифрування, що збільшує стійкість шифру до лінійного та диференційного криптоаналізу.

2. Запропоновано метод для побудови 16-бітних блоків підстановки, який базується на трикратному псевдовипадковому перемішуванні, що, на відміну від існуючих, забезпечує підвищену стійкість шифрувального перетворення до криптоаналізу.

ВСТУП

Практичне значення одержаних результатів

Практична цінність даної дипломної роботи полягає у тому, що розроблено новий алгоритм та ПЗ для шифрування тексту, які, у зрівнянні з аналогами, забезпечують підвищені обчислювальні та криптографічні властивості. Розроблений додаток може бути використаний для вирішення задач захисту інформації у КС.

Особистий внесок здобувача

В роботі “Підвищення стійкості шифрування інформації в оптико-електронних системах блочними шифрами на основі використання багаторівневих гніздових підстановочно-перестановочних мереж” у співавторстві розроблено модифікацію гніздової підстановочно-перестановочної мережі, досліджено різні комбінації блоків перестановки і визначено найбільш ефективні. Було досліджено різні типи нелінійних перетворень для застосування їх у якості S-боксів. Було вирішено сформувати S-бокси шляхом псевдовипадкового перемішування. Також магістрантом було розроблено ПЗ для S-боксів, побудови таблиць лінійної апроксимації та програмний додаток для виконання шифрування інформації.

ВСТУП

Апробація результатів роботи

Результати досліджень доповідались на XLIV регіональній науково-технічніій конференції професорсько-викладацького складу, співробітників та студентів університету з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та області, та на Всеукраїнському конкурсі студентських наукових робіт у 2014 - 2015 н.р.

Публікації

За темою магістерської роботи опублікована стаття “Підвищення стійкості шифрування інформації в оптико-електронних системах блочними шифрами на основі використання багаторівневих гніздових підстановочно-перестановочних мереж” – видання: Оптико-електронні інформаційно-енергетичні технології. Також за результатами XLIV регіональної науково-технічної конференції професорсько-викладацького складу, співробітників та студентів було опубліковано тези доповіді.

ДОСЛІДЖЕННЯ АНАЛОГІВ

Проаналізувавши найближчі аналоги до розробленого шифру було визначено необхідність реалізації шифру, що мав би високу криптографічну стійкість та розмір ключа не менший за ті, якими володіє шифр AES. Було вирішено використати комбінації S-боксів, що забезпечуватимуть високі показники криптографічної стійкості.

Для реалізації поставлених цілей потрібно вирішити наступні задачі:

- розробити метод підстановки з високим ступенем стійкості до лінійного та диференційного криптоаналізу;

- розробити метод перестановки з високим показником стійкості;

- застосувати обрані методів підстановки та перестановки для створення блочного шифру, що зберігатиме їх позитивні властивості.

ЛІНІЙНИЙ КРИПТОАНАЛІЗ

Лінійний криптоаналіз використовує високу імовірність появи лінійних виразів, що включають вхідні нешифровані, шифровані біти та біти підключа при наявності деякої кількості текстів з відповідними до них шифротекстами.

Сенс алгоритму полягає в отриманні співвідношень наступного вигляду:

$$P_{i1} \oplus P_{i2} \oplus \ldots \oplus P_{ia} \oplus C_{j1} \oplus C_{j2} \oplus \ldots \oplus C_{jb} = K_{k1} \oplus K_{k2} \oplus \ldots \oplus K_{kc},$$

де P_{in} - n-тий біт i-того тексту;

C_{jn} - n-тий біт j-того шифротексту;

K_{kn} - n-тий біт k-того ключа.

ЛІНІЙНИЙ КРИПТОАНАЛІЗ

Дані співвідношення називаються лінійними апроксимаціями. Для довільно обраних біт відкритого тексту, шифротекста і ключа ймовірність справедливості такого співвідношення P приблизно дорівнює 1/2. Такими співвідношеннями, ймовірність яких помітно відрізняється від 1/2 можна застосувати для подальшого аналізу.

ДИФЕРЕНЦІЙНИЙ КРИПТОАНАЛІЗ

Диференційний криптоаналіз заснований на вивченні перетворення різниць між зашифрованими значеннями на різних раундах шифрування.

В ідеально рандомізованому шифрі імовірність того, що конкретній вихідній різниці ΔY відповідає вхідна різниця ΔX становить $1/2^n$, де n – кількість бітів, над якими виконується перетворення.

Розглядаючи лінійний та диференційний криптоаналіз можна помітити їх значну подібність. Дослідження доводять звязок між ними, тому виявилося, що немає необхідності окремо досліджувати стійкість шифру до кожного із цих методів криптоаналізу.

ФОРМУВАННЯ БЛОКУ ПЕРЕСТАНОВКИ

$$B = FA,$$

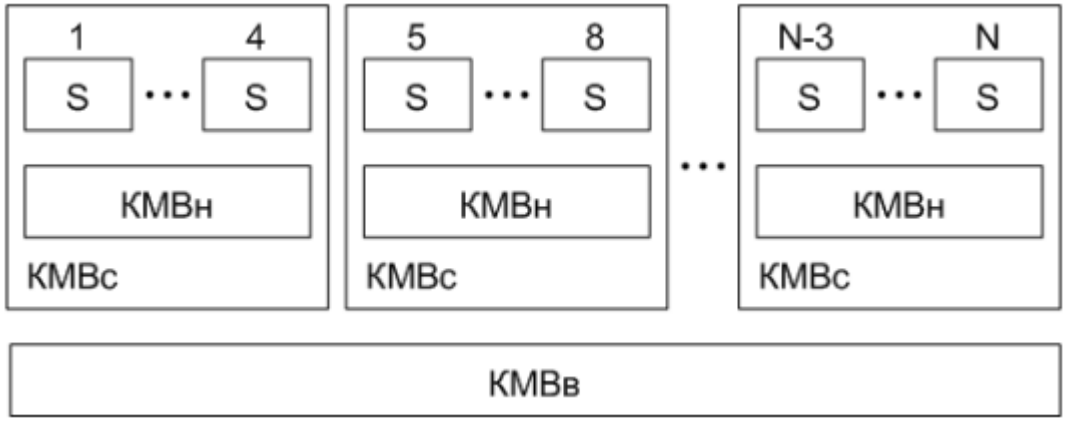
де $B = \begin{bmatrix} b_0 \\ \dots \\ b_{m-1} \end{bmatrix}$, $A = \begin{bmatrix} a_0 \\ \dots \\ a_{m-1} \end{bmatrix}$, $F = \begin{bmatrix} f_{n-1,n-1} & \dots & f_{n-1,0} \\ \dots & \dots & \dots \\ f_{0,n-1} & \dots & f_{0,0} \end{bmatrix}$.

$$f_{n-1,j}x^{n-1} + \dots + f_{0,j} = x^j(c_{n-1}x^{n-1} + \dots + c_0) mod\ Px),$$

де $c_{n-1}, \dots, c_0$ – константи

Кількість активних S-боксів раундового перетворення, що складається із трьох рівнів (верхнього, середнього і нижнього), на кожному з яких застосовані коди з максимальною відстанню з довжиною слова m_1 – на нижньому рівні, m_2 – на середньому та m_3 – на верхньому, визначається виразом :

$$N = (m_3 + 1)(m_1m_2 + m_1 + m_2 + 2).$$



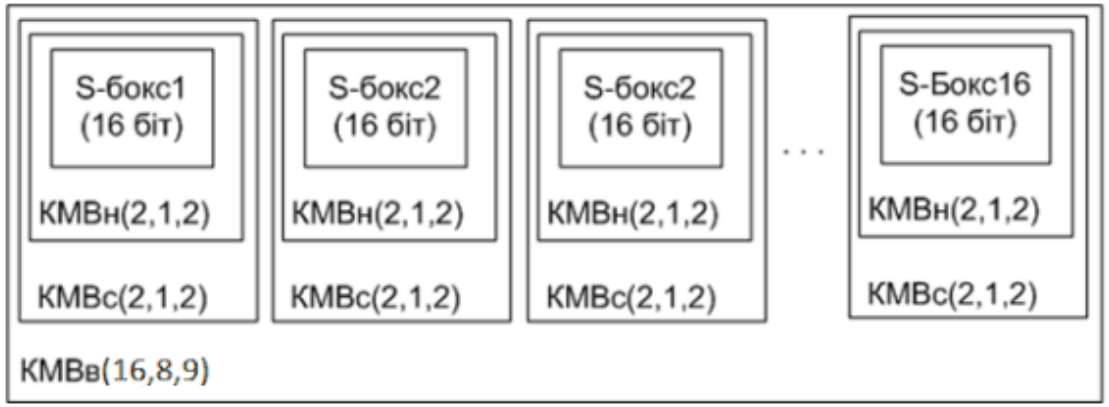
ЗАЛЕЖНІСТЬ КІЛЬКОСТІ АКТИВНИХ S-БОКСІВ ВІД ТИПУ SPN-МЕРЕЖІ ДОВЖИНОЮ 128 БІТ З ТРЬОМА РІВНЯМИ І РОЗМІРОМ S-БОКСУ – 8 БІТ

№	Тип $КМВ_н$	Тип $КМВ_с$	Тип $КМВ_в$	Кількість активних S-боксів
1	(2,1,2)	(2,1,2)	(32,16,17)	85
2	(2,1,2)	(4,2,3)	(16,8,9)	63
3	(2,1,2)	(8,4,5)	(8,4,5)	55
4	(2,1,2)	(32,16,17)	(2,1,2)	70
5	(2,1,2)	(16,8,9)	(4,2,3)	57
6	(4,2,3)	(16,8,9)	(2,1,2)	56
7	(4,2,3)	(4,2,3)	(8,4,5)	50
8	(16,8,9)	(2,1,2)	(4,2,3)	57
9	(16,8,9)	(4,2,3)	(2,1,2)	56
10	(32,16,17)	(2,1,2)	(2,1,2)	70

ЗАЛЕЖНІСТЬ КІЛЬКОСТІ АКТИВНИХ S-БОКСІВ ВІД ТИПУ SPN-МЕРЕЖІ ДОВЖИНОЮ 128 БІТ З ТРЬОМА РІВНЯМИ І РОЗМІРОМ S-БОКСУ – 16 БІТ

№	Тип КМВ$_н$	Тип КМВ$_с$	Тип КМВ$_в$	Кількість активних S-боксів
1	(2,1,2)	(2,1,2)	(16,8,9)	45
2	(2,1,2)	(4,2,3)	(8,4,5)	35
3	(2,1,2)	(8,4,5)	(4,2,3)	33
4	(2,1,2)	(16,8,9)	(2,1,2)	38
5	(4,2,3)	(2,1,2)	(8,4,5)	35
6	(4,2,3)	(4,2,3)	(4,2,3)	30
7	(8,4,5)	(2,1,2)	(4,2,3)	33
8	(8,4,5)	(4,2,3)	(2,1,2)	32
9	(16,8,9)	(2,1,2)	(2,1,2)	38

МЕРЕЖА, ЩО ВИКОРИСТОВУЄТЬСЯ У РОЗРОБЛЕНОМУ ШИФРІ



Імовірність лінійної P та диференційної Q характеристик раунду, утвореного трьохрівневою гніздовою SPN мережею розраховується за наступною формулою

$$P = \left(\frac{n}{2^{n-1}}\right)^{(m_3+1)(m_1m_2+m_1+m_2+2)}.$$

Імовірність лінійної та диференційної характеристик раунду трьохрівневої гніздової SPN мережі з S-боксами розміром 8 біт становить:

$$P = \left(\frac{8}{2^{8-1}}\right)^{85} = (2^{-4})^{85} = 2^{-340}.$$

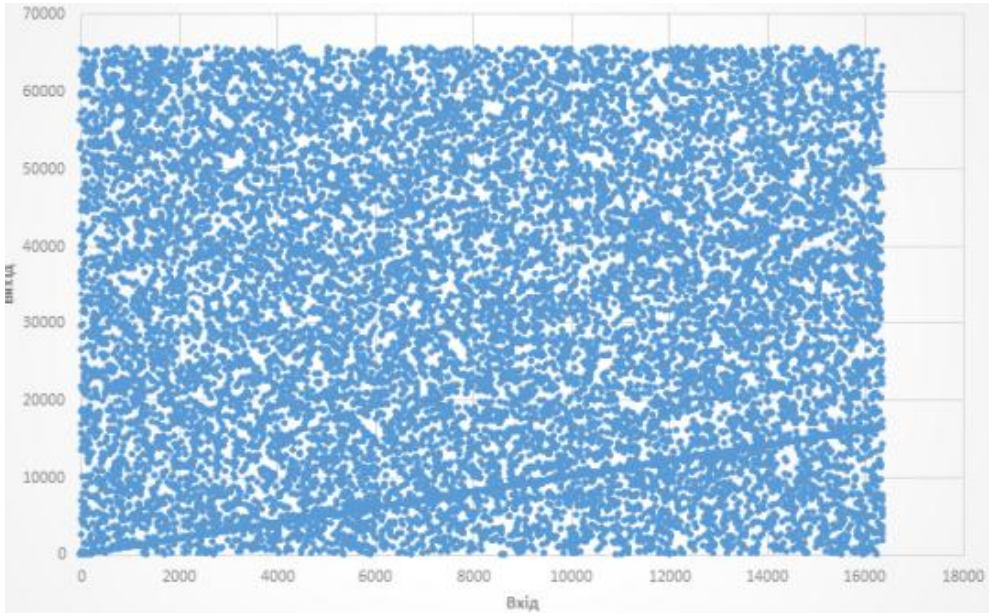
Імовірність лінійної та диференційної характеристик раунду трьохрівневої гніздової SPN мережі з S-боксами розміром 16 біт становить:

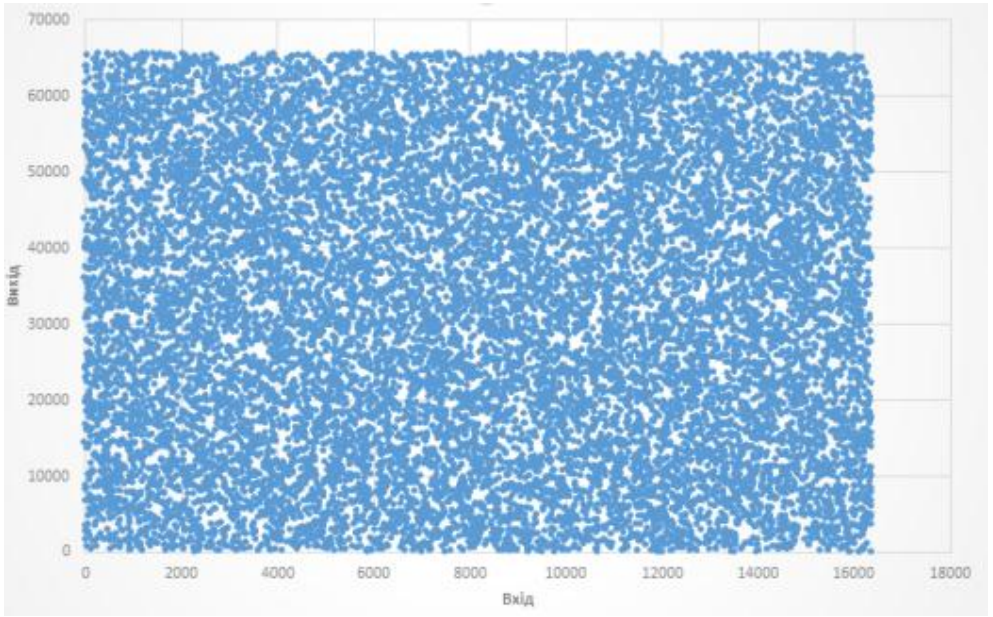
$$P = \left(\frac{16}{2^{16-1}}\right)^{45} = (2^{-11})^{45} = 2^{-495}.$$

Імовірність лінійної та диференційної характеристик раунду шифру Rijndael становить:

$$P = \left(\frac{8}{2^{8-1}}\right)^{25} = (2^{-4})^{25} = 2^{-100}.$$

ГРАФІК ЗАЛЕЖНОСТІ ВИХОДУ ВІД ВХОДУ ДЛЯ ПСЕВДОВИПАДКОВО ЗГЕНЕРОВАНОГО БЛОКУ ПІДСТАНОВКИ: (1 ТА 3 ЗМІШУВАННЯ)





ГРАФІК ПОЯВИ ЗНАЧЕНЬ У ТАБЛИЦЯХ ЛІНІЙНОЇ АПРОКСИМАЦІЇ ДЛЯ S-БОКСІВ ШИФРУ RIJNDAEL ТА РОЗРОБЛЮВАНОГО ШИФРУ

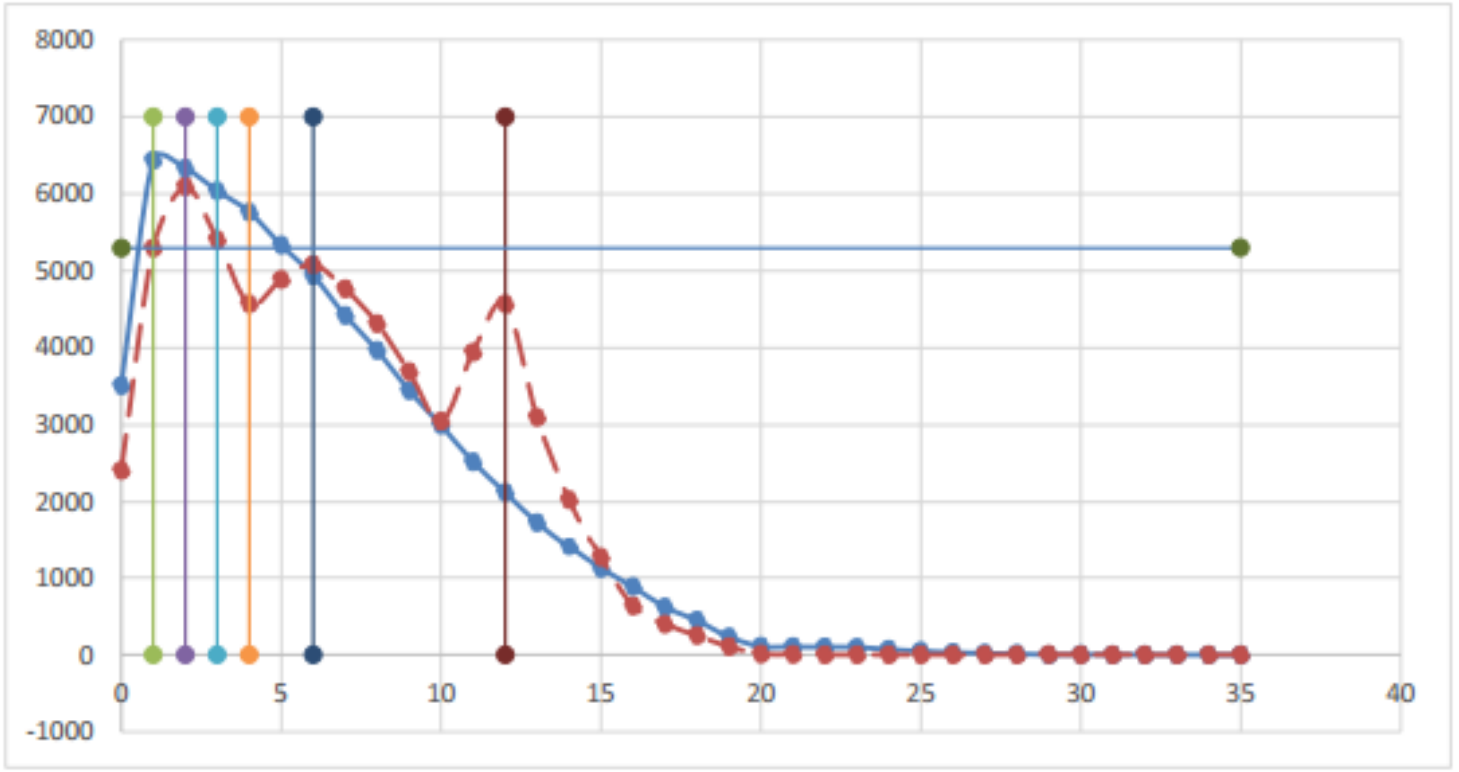


СХЕМА ПРОГРАМИ ДЛЯ ПОБУДОВИ ТАБЛИЦЬ ЛІНІЙНОЇ АПРОКСИМАЦІЇ

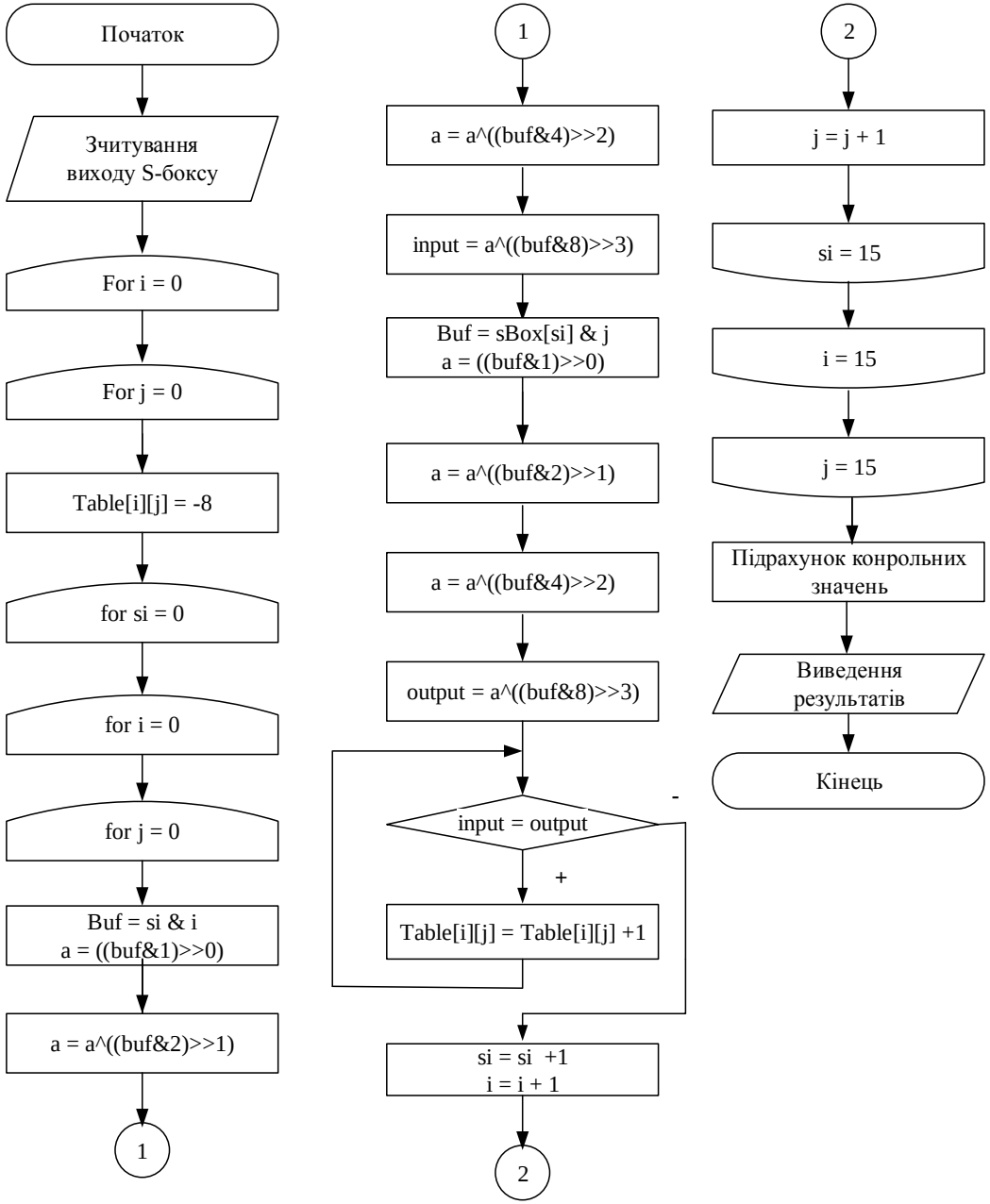


СХЕМА ПРОГРАМИ ШИФРУВАННЯ

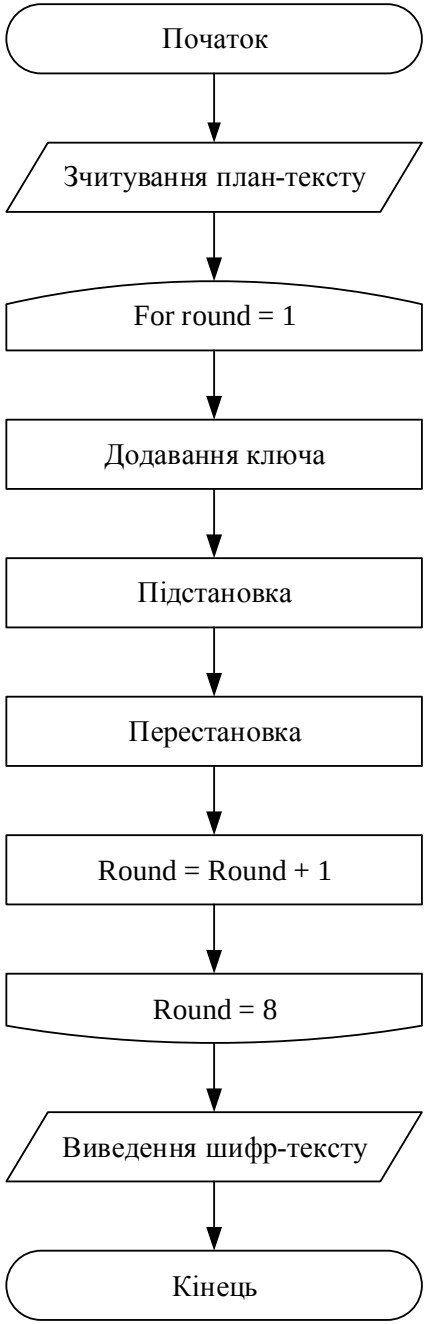


СХЕМА ЕТАПУ ПІДСТАНОВКИ

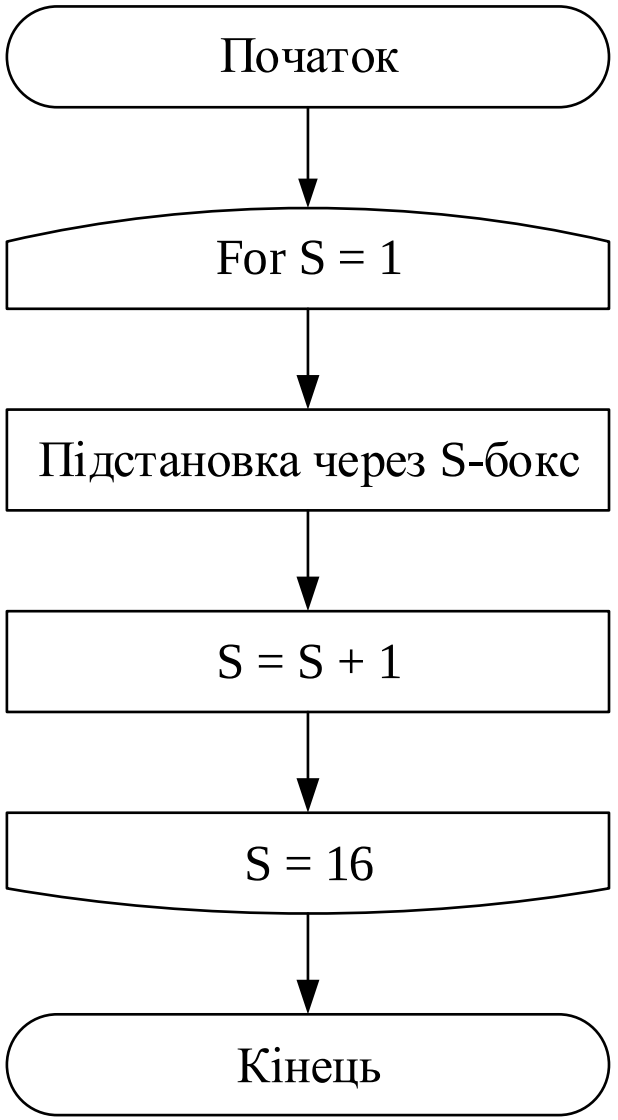
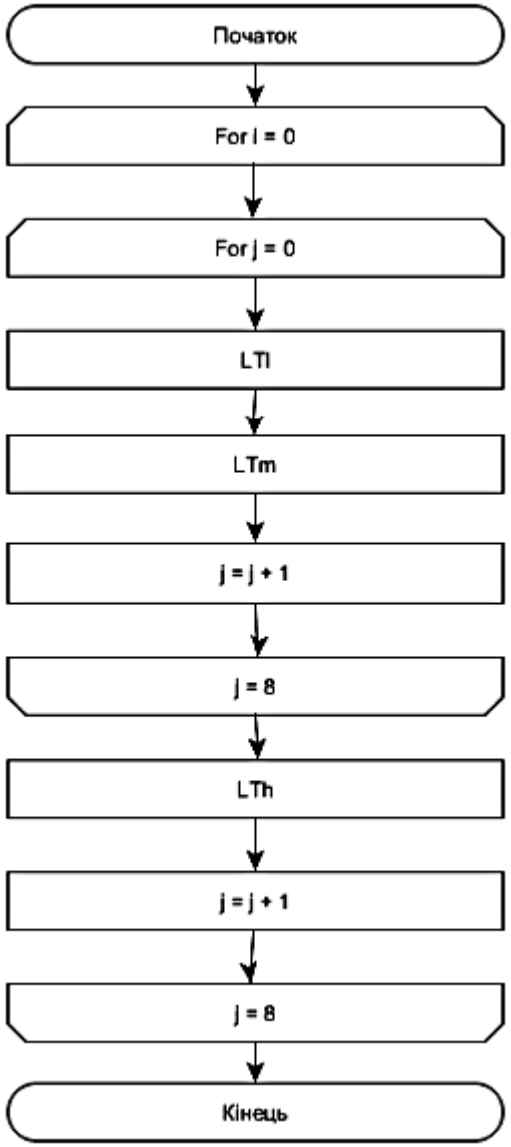


СХЕМА ЕТАПУ ПЕРЕСТАНОВКИ



ВИСНОВКИ

У даній роботі виконано дослідження з метою підвищення ефективності захисту інформації в комп’ютерних системах та мережах, шляхом підвищення їх криптографічної стійкості.

Запропоновано метод формування блоків підстановки, що базується на трьохкратному псевдовипадковому перемішуванні, який забезпечує в 1,32 рази вищу нелінійність, за рахунок рандомізації звязків між входом та виходом S-боксів.

Розроблено метод перестановки, що базується на використанні трьохрівневих гніздових підстановочно-перестановочних мереж, який забезпечує пыдвищення кількості активних S-боксів у 1,8 разів, за рахунок збільшення кількості рівнів перестановок.

Вперше розроблено метод шифрування, що вкористовує 16-бітні блоки підстановки, сформовані шляхом трьохкратного псевдовипадкового перемішування та використовує трьохрівневу підстановочно-перестановочну мережу, що забезпечує підвищену стійкість проти лінійного та диференційного криптоаналізу, за рахунок використання високонелінійного перетворення на етапі підстановки та методу перестанвоки, що забезпечує збільшення кількості активних S-боксів.

На основі розробленого методу шифрування сформовано алгоритмічне та програмне забезпечення, яке шифрує текст із швидкістю, вищою, ніж у аналогічних системах шифрування, що досягається за рахунок паралелізації обчислень, та забезпечити його високу стійкісь проти лінійного та диференційного криптоаналізу. Достовірність отриманих показників стійкості та продуктивності роботи підтверджена математичним розрахунками та спеціально розробленим програмним забезпеченням.

ДЯКУЮ ЗА УВАГУ!