УДК 004.056

А.В. Цон
А.С. Васюра

Мікропроцесорна система передавання інформації з захистом від несанкціонованого доступу

Вінницький національний технічний університет

Анотація

В роботі розглянуто сучасні криптографічні методи захисту інформації. Було розроблено електрична структурна, електрична принципова та програмне забезпечення.

Ключові слова: *сучасні криптографічні методи, цілісність даних, шифрування та дешифрування.*

Abstract

Modern cryptographic methods of information security are considered in the work. Electrical structural, electrical, and software were developed.

Keywords: modern cryptographic methods, data integrity, encryption and decryption.

Вступ

Необхідність захисту інформації від несанкціонованого доступу в системах передачі інформації пояснюється тим, що постійно відбувається велика кількість спроб отримання конфіденційних даних в цих системах. Так на виробництві для управління різноманітних процесами користування даними, що вказують на певні режими процесу та застосовуються для регулювання певних параметрів. Спотворення, перехоплення цих даних, які виникнуть після незаконного втручання іншої особи приведуть до неправильного руху всього процесу та збитків на виробництві.

В іншому випадку під час передачі інформації в каналах зв’язку завдяки завадам виникає спотворення інформації, внаслідок чого виникає доступ некоректної інформації до виконавчих вузів виробничого процесу, що призводить до серйозних проблем. Надійним способами захисту від несанкціонованого доступу є перетворення інформації за математичними правилами, які обумовлюються алгоритмами шифрування. Способом захисту інформації від помилок є використання методів кодування з визначенням помилок.

Актуальність роботи. По цій причині розробка мікропроцесорної системи яка забезпечує одночасний захист інформації від помилок та несанкціонованого доступу є актуальною задачею.

Метою даної роботи є розробка підвищення ефективності захисту інформації від несанкціонованого доступу та від помилок в мікропроцесорних системах передавання інформації.

Для досягнення поставленої мети проаналізувати існуючі методи захисту інформації в мікропроцесорних системах, розробити алгоритм реалізації блочного шифру який має високу продуктивність реалізації мікропроцесорних систем.

Об’єктом досліджень процес обробки та перетворення даних для захисту інформації від несанкціонованого доступу та від помилок. Предмет дослідження методи шифрування та кодування для захисту інформації мікропроцесорних системах.

Методи дослідження – використана лінійна алгебра та теорія алгебраїчного кодування.

Результати дослідження

На сьогоднішній день величезний обсяг секретної інформації передається з допомогою звичайних ліній зв'язку. Комп'ютерні системи і мережі являються одними з самих вразливих компонентів сучасних організацій та банківських установ. Тому існує загальна потреба захищати таємну інформацію від несанкціонованого доступу в комп'ютерних системах та мережах.

Безпечному передаванню інформації в мережах перешкоджають наступні види загроз мережевої взаємодії:

- перехоплення даних з метою викрадення, модифікування чи переадресування;

- несанкціоноване відмивання даних від імені іншого користувача;
- заперечення користувачами автентичності даних і фактів відсилання-отримання інформації.

Здійснення повного та комплексного захисту інформації має відповідати трьом криптографічним вимогам: конфіденційність, автентичність та цілісність даних [1].

Конфіденційність даних – це статус, наданий даним, чим визначається необхідний ступінь їх захисту. Конфіденційні дані повинні бути відомі тільки допущеним (і тим, що пройшли перевірку) авторизованим суб'єктам системи.

Автентичність даних – це процес підтвердження інформації щодо особи або системи забезпечення, хеш-функції і асиметричні шифри.

Цілісність даних – це гарантованість того, що дані не були змінені, підмінені або знищені в результаті зловмисних дій або випадків.

Симетричні шифри поділяються на блочні та поточні шифри. Шифрування та дешифрування використовується однаковий ключ для шифру (рисунок 1).

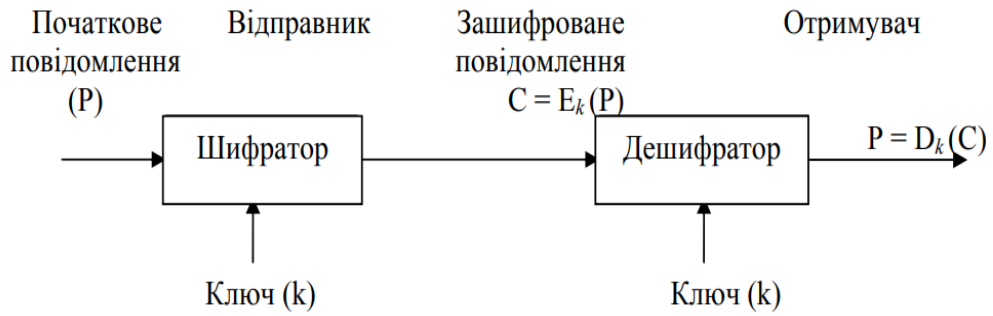


Рисунок 1 - Шифрування-дешифрування з закритим ключем

За наявності ключа шифрований текст перетворюється системою шифрування у відкритий текст. Тому доступ до ключа шифрування повинен бути обмежений [2].

Процес шифрування описується виразом:

$$C = E_k(P), \quad (1)$$

де P – відкритий текст,
k – ключ шифрування,
C – шифрований текст.

Процес дешифрування описується виразом:

$$P = D_k(C), \quad (2)$$

Цей тип шифрування має велику кількість представників. Найвідоміші з них – DES [3], AES [4], RC6 [5], MARS [6], Twofish [7], Serpent [8], LOKI 91[9], ГОСТ 28147-89 [10]. Криптографічні властивості цих шифрів наведено в [12-19]. В системах шифрування з відкритим ключем (асиметричні шифри) на відміну від симетричних шифрів використовуються два ключа – відкритий (публічний) та закритий (секретний) (рисунок 1.1). Ці ключи математично пов`язані між собою. Шифрований текст отримується з відкритого тексту відкритим ключем шифрування k_1. Відкритий текст отримується з шифрованого тексту закритим ключем дешифрування k_2. Ця система визначається трьома алгоритмами: генерація ключів, шифрування та розшифрування. Алгоритм генерації відкритий. Алгоритми шифрування Ek_1 та розшифрування Dk_2 такі, що для будь-якого відкритого тексту m виконується рівність $Dk_2(Ek1(m))=m$.

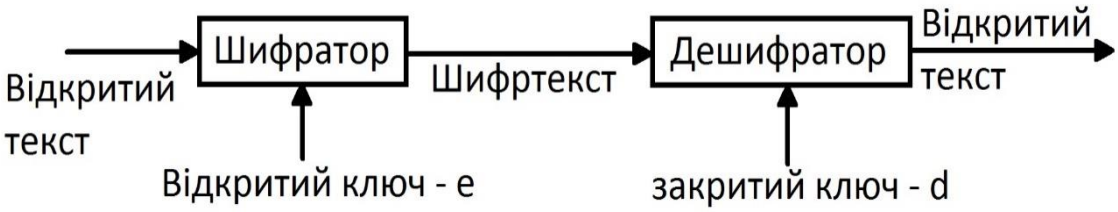


Рисунок 2 - Система шифрування-дешифрування з відкритим ключем

Хеш-функцією *H* називається математичною, або інша функція, що перетворює дані *M* довільною довжини в дані h фіксованої довжини.

$$h = H(M), \tag{3}$$

Хеш-алгоритми використовуються для визначення цілісність даних. Закриті канали отримають повідомлення обчислювання хеш і порівнюється з хешем повідомлення. Якщо не модифікувалися повідомлення, то вони однакові. Хеш-функції можуть використовуватися для автентифікації даних.

Як було визначено Шенноном, для ефективного забезпечення закритості повідомлення шифри повинні використовувати два основних та головних принципи – перемішування (confusion) та «розсіювання» (diffusion).

Переміщення – це сукупність операцій, які відкритим текстом та шифр текстом усувають зв`язок. Усунення зв`язку між шифртекстом та відкритим текстом виконується шляхом знищення між ними статистичних закономірностей та надлишковості.

Розсіювання змінює по всьому шифртексту шляхом розповсюдження надлишковість відкритого тексту. Найпростіший спосіб створити розсіювання є виконання транспозиції (перестановки). Елементарний перестановочний шифр лише переставляє букви відкритого тексту. Сучасні шифри для виконання розсіювання ще використовують операції розміщення частин повідомлення по всьому повідомленню.

Розсіювання в сучасних комп`ютерних системах доцільніше виконати бітовими перестановками, але ці операції не підтримуються сучасними процесорами

В таблиці 1 наведені сучасні блочні шифри та типи архітектури, які їм відповідають.

Таблиця 1 – Типи архітектури обчислення шифрів

Назва шифру	Тип архітектури (метод формування розсіювання)
CAST-256	Feistel network
Deal	Feistel network
DFC	Feistel network
Frog	SPN
LOKI	Feistel network
Mars	Feistel network
RC6	Feistel network
Rijndael	SPN
Safer K-64	SPN
Serpent	SPN
Twofish	Feistel network

Як зазначено вище одним з поширених методів формування «розсіювання» в блочних шифрах є класична мережа Фейстеля (рисунок 3).

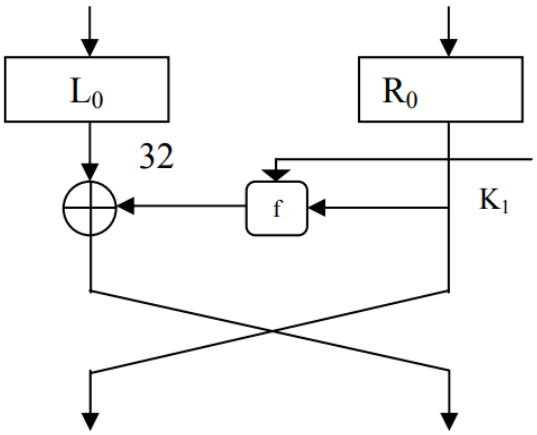


Рисунок 3 - Мережа Фейстеля

Даним методом користувалися майже всі блоки першого покоління. Початок розсіювання відбувається зміною місцями лівих та правих частини. Блок шифрування складається з двох частин: правих та лівих, які перетворюється певною кількістю ітерацій(раундів).

На кожному раунді з лівої частини і частини ключа k за допомогою функції шифрування f створюється елемент даних, що підсумовується за модулем 2 з правою частиною (R): $R` = R + f(L, k)$. Після цього ліва і права частини міняються місцями. Операція заміни місцями лівої L та правої частини R в одному раунді відповідає добутку на двомірну квадратну матрицю (4):

$$LR \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = RL, \qquad (4)$$

Перевагою цього методу є ефективність та компактність реалізації в апаратному та програмному варіантах. Причиною є зворотність перетворення і різниця лише в порядку застосування функції шифрування в раунді процедури зашифрування та розшифрування.

Зворотне ідентичність послідовності раундових функцій та використання одної функції шифрування є причиною різниці процедур шифрування лише в порядку використання ключових елементів.

Для підвищення ступеня розсіювання, та для збільшення об`єму перетворення інформації за одиницю часу використовується узагальнена або розширена мережа Фейстеля (рисунок 5). Ця мережа складається з чотирьох гілок.

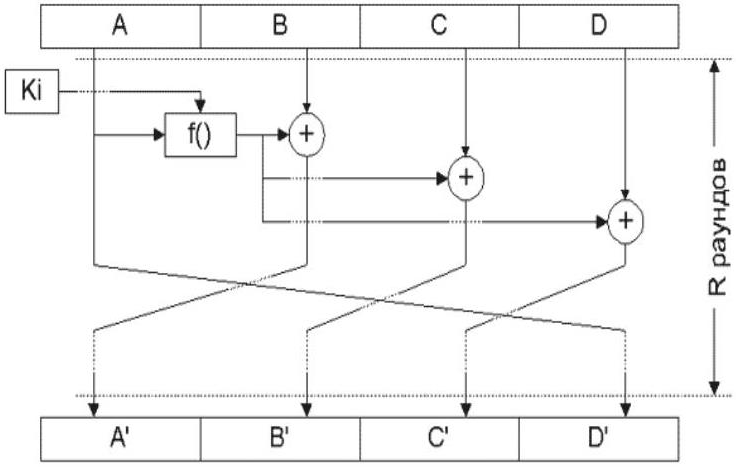


Рисунок 5 - Узагальнена мережа Фейстеля

Ці методи дозволили отримувати відкритий текст з шифрованого тексту без знання ключа шифрування. В мікроелектроніці збільшилися можливості електронних пристроїв. Швидкодія та об`єм пам`яті збільшилися на декілька порядків. Це привело до пропорційного збільшення можливостей екстенсивних методів крипт аналізу, таких як повний перебір можливих даних.

Підстановочно-перестановочна мережа створює розсіювання за допомогою перестановки бітів перед входом в наступний раунд.

Підстановочно-перестановочна мережа наведена на рисунок 6.

Доля мережі, що називається S-бокс створює перемішування вхідних бітів.

Підстановочно-перестановочна мережа складається з певною кількості раундів. Кожний раунд має три кроки. Перед входом в перший раунд план текст ділиться на блоки.

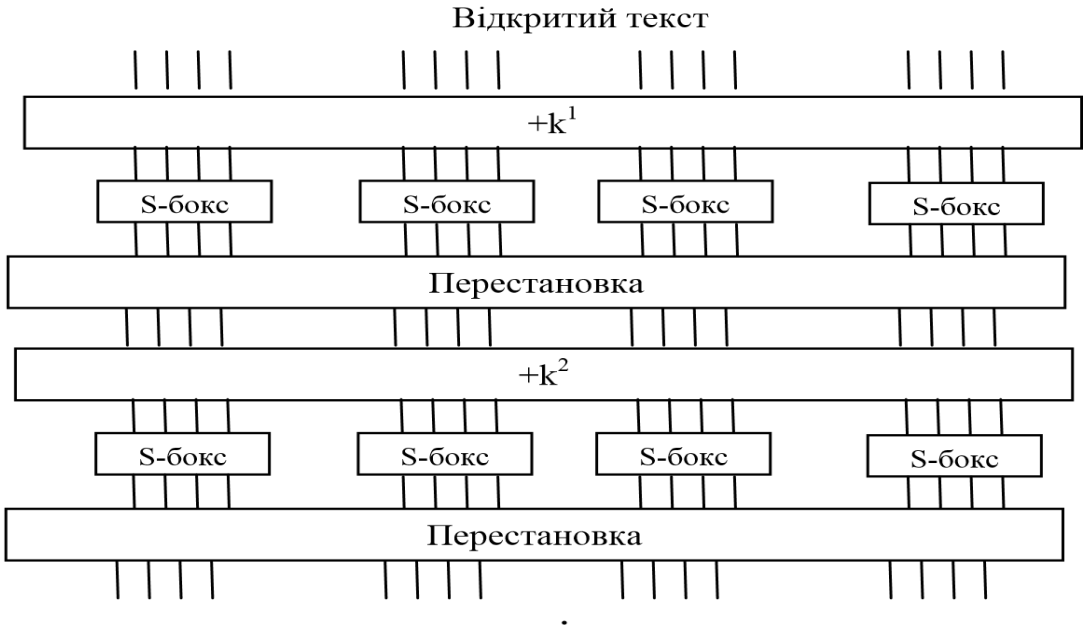
Перший крок вхідні біти додаються за модулем 2 з підключами цього раунду.

Другий крок бітів перетворюється S-боксами.

Третій крок перетворені біти одного S-боксу переставляються місцями з бітами інших блоків S-блоків.

Перестановка не потрібна через те, що вона не додає криптографічної стійкості.

Розшифрування відбувається зворотним чином. Крок перестановки виконує операцію зміни однієї послідовності біт на іншу. Стійкість підстановочно-перестановочна мережа залежить від S-боксів та виду перестановок.



6 - Підстановочно-перестановочна мережа

Якщо початкова послідовність біт (вектор) – $X = \{0,1\}^n$, а кінцева – $Y = \{0,1\}^n$, (n – кількість бітів в перетворенні), то згідно лінійної алгебри, операція перестановки виконує множення на певну матрицю χ з елементами
0 та 1:

$$Y = {}_{\chi}X, \qquad (5)$$

Висновки

В даній роботі розглянуто мікропроцесорну систему передавання інформації з захистом від несанкціонованого доступу та випадкових помилок, досліджено методи шифрування та кодування для захисту інформації мікропроцесорних системах.

Проведено аналіз існуючих методів захисту інформації в мікропроцесорних системах, та аналіз блочного шифру з підстановки S-боксів нелінійних перетворень та перестановки лінійних перетворень. Розроблено алгоритм реалізації блочного шифру який має високу продуктивність реалізації мікропроцесорних систем. Запропонована розробка забезпечує підвищення ефективності

захисту інформації від несанкціонованого доступу та від помилок в мікропроцесорних системах передавання інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. – М.: Триумф, 2002. – 816 с.
2. Лужецький В. А. Блоковий симетричний шифр на основі арифметичних операцій за модулем 2^N / В. В. Сокирук, В. А. Лужецький // Современные методы кодирования в электронных системах (СМКЭС-2004): Ткачук С. В.,Ткач В. В. Обґрунтування принципу дії проточного датчика витрат молока ємнісного типу. Механізація та електрифікація сільського господарства: загальнодержавний зб.. ННЦ «ІМЕСГ». Глеваха, 2016. Вип. 3 (102). С. 113–119.
3. Зима В. М. Безопасность глобальных сетевых технологий / В. М Зима., А. А. Молдовян, Н. А. Молдовян – СПб.: БХВ-Петербург, 2010. – 320 с.
4. National Bureau of Standart (NBS). Data Encryption Standart (DES) // Federal Information Processing Standards Publication 46-2. – December 1993.
5. National Bureau of Standart (NBS). Data Encryption Standart (DES) // Federal Information Processing Standards Publication 46-2. – December 1993.
6. The RC6 block cipher / [R. Rivest, J. Robshshaw, R. Sidney, and Y. Yin] // NIST AES proposal. – August 1998.
7. Burwick C. et al. MARS: a candidate cipher for AES // /NIST AES proposal. – June 1998.
8. Twofish: A 128-Bit Block Cipher / [B. Schneier, J. Kelsey, D. Whiting, C. Hall, N. Ferguson] // NIST AES proposal. – June 1998. – Режим доступу http://www. Schneider. Com/paper-twofish-paper. Pdf.
9. Biham E. Serpent: A New Block Cipher Proposal / E. Biham, R.Anderson, L. Knudsen // Proceeding in Fast Software Encryption (FSE 98): Lecture Notes in Computer Science. – Springer-Verlag. – Vol 1372. – P. 222 – 238.
10. Brown L. LOKI: A cryptographic primitive for authentication and secrecy applications / L. Brown, J. Pieprzyk, J. Sebery // Advances in Cryptology – AUSCRYPT `90. Lecture Notes in Computer Science. – Springer-Verlag. – Vol 453. – P. 229 – 236.

Цон Антон Валерійович – студент групи ІЯП-19м кафедри метрології та промислової автоматики факультету автоматики та комп'ютерних систем управління, Вінницький національний технічний університет, Вінниця, tson9788@gmail.com.

Васюра Анатолій Степанович— професор, кафедри метрології та промислової автоматики, Вінницький національний технічний університет, м. Вінниця.

Tson Anton - student of the IAP-19m group of the Department of Metrology and Industrial Automation, Faculty of Automation and Computer Control Systems, Vinnitsa National Technical University, Vinnitsa, tson9788@gmail.com.

Vasyura Anatoly S. - Professor, Departments of Metrology and Industrial Automation, Vinnitsa National Technical University, Vinnitsa.