Система передавання даних з інформаційним захистом та швидким декодуванням

ст. гр. 1КСУА15мн

Деревенько К. В.

Мета роботи полягає у підвищенні ефективності роботи системи передавання даних, в якій реалізовано виправлення двох помилок та інформаційний захист від несанкціонованого доступа.

Задачі, що вирішуються у роботі:

− розробка методу виправлення двох помилок на основі використання швидкого декодування в системі передавання;

− розробка методу захисту інформації з високою криптографічною стійкістю в системі передавання.

Об'єктом дослідження є процес передавання даних.

Предметом дослідження є метод декодування інформації та метод захисту інформації.

Методи дослідження: абстрактна алгебра, алгебраїчна теорія кодування

Практична цінність полягає у розробці методики, алгоритмів та програмних продуктів для передавання даних з виправленням 2-х помилок та високої криптографічної стійкості.

Новизною результатів дипломної роботи є низка результатів по підвищенню швидкості декодування інформації та криптографічної стійкості:

– вперше запропоновано метод виправлення двох помилок з високою швидкістю роботи в системі передавання, якій на відміну від існуючих характеризується високою швидкістю декодування за рахунок застосування при визначенню синдрому алгоритму перебору коренів розв`язку системи рівнянь;

– вдосконалено метод захисту інформації від несанкціонованого доступу, який на відміну від існуючих, має вищу ступінь протидії до криптоаналізу, за рахунок застосування багаторівневих підстановочно-перестановочних мереж

Впровадження результатів дисертаційної роботи. Результати проведених досліджень впроваджено на ТОВ «Спільна справа» (м. Вінниця, акт від 17.01.2017 р.).

Апробація результатів дослідження. Основні теоретичні положення й найвагоміші практичні результати виконаного дослідження було обговорено на:

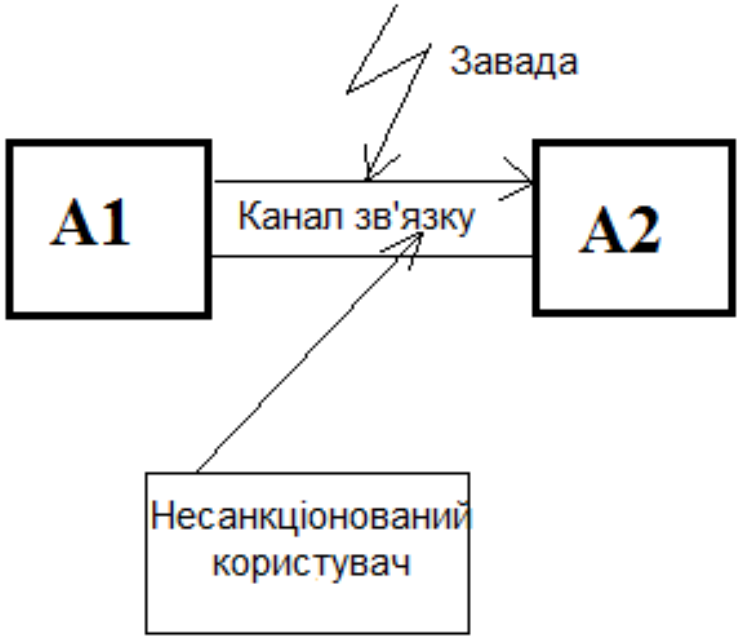
XLII регіональній науково-технічній конференції професорсько-викладацького складу, співробітників та студентів університету з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та області, XLIII регіональній науково-технічній конференції професорсько-викладацького складу, співробітників та студентів університету з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та області, XLIV регіональній науково-технічній конференції професорсько-викладацького складу, співробітників та студентів університету з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та області, XIII International Conference —Measurement and control in complex systems. MCCS- 2016, (Vinnitsia 3-6 October 2016).

Публікації. За результатами виконаних досліджень опубліковано 4 наукові праці: стаття [1], у виданні, яке включено до фахових видань ВАК, та 3 публікації [2, 3, 4] у вигляді тез доповідей.

Актуальність

Спотворення інформації призводить до помилок в роботі системи передавання даних і виникає внаслідок перешкод, які впливають на передані в системах дані. Найбільш часто спотворюються два інформаційних символи - виникають дві помилки. Несанкціонований доступ (НСД) учасників можливий унаслідок відкритості каналів зв'язку, на основі яких працює система передавання даних.

Сучасні методи виправлення двох помилок і методи захисту від несанкціонованого доступу, які використовуються в системах передавання інформації, характеризуються рядом недоліків. Найкритичніші з них - низька швидкість роботи системи, яка призводить до зниження ефективності роботи системи передавання даних. Мета - підвищення ефективності роботи системи, в якій реалізовано виправлення двох помилок та інформаційний захист від несанкціонованого доступу.



Система передавання даних

Приведення системи рівнянь в кінцевому полі до квадратичного рівняння :

$$x_1 + z_1 x + \frac{Z_2}{Z_1} + Z_1^2 = 0 \qquad (1)$$

Преведення рівняння (1) до виду:

$$x^2 + x + \beta = 0 \qquad (2)$$

Довжина коду Хемінга

$$n = 2^m - 1, \qquad (3)$$

де m-кількість перевірочних символів, n-довжина кодового слова

Перевірочна матриця H кода Хеммінга при m = 4 і n = 15:

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \quad (4)$$

Скорочене позначення матриці (4):

$$H = [1, 2, 3 \ldots i \ldots 14, 15], \quad (5)$$

де і відповідний 4-бітний вектор

Матриця H' для виправлення 2 помилок:

$$H' = \begin{bmatrix} 1 & 2 & 3 & \ldots & 15 \\ f(1) & f(2) & f(3) & \ldots & f(15) \end{bmatrix}. \quad (6)$$

Значення і-го стобця матриці H’:

$$H_i = \begin{pmatrix} i \\ f(i) \end{pmatrix} \quad (7)$$

Синдром кода :

$$S = H_i + H_j = \begin{pmatrix} i & + & j \\ f(i) & + & f(j) \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \quad (8)$$

Нехай y-кодове слово, тоді декодування здійснимо на основі (8)

$$S = Hy^T = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \quad (9)$$

Якщо помилки відбулись на позиціях і, j кодового слова, то повинна виконуватись система:

$$\left.\begin{array}{ccccc} i & + & j & = & z_1 \\ f(i) & + & f(j) & = & z_2 \end{array}\right\} \quad (10)$$

Після заміни система (10) прийме наступний вигляд:

$$\left.\begin{array}{rcl} i + j & = & z_1 \\ i^3 + j^3 & = & z_2 \end{array}\right\} \qquad (11)$$

4 варіанта рішення системи (11):

Варіант 1. Якщо $z_1 = z_2 = 0$ - помилки відсутні.

Варіант 2. Якщо $z_1 \neq 0$ и $z_2 = z_1^3$ - відбулась помилка на на позиції $i = z_1$.

Варіант 3.Якщо $z_1 \neq 0$ и $z_2 \neq z_1^3$ - відбулись помилки на на позиціях i, j.

Варіант 4. Якщо $z_1 = 0$ та $z_2 \neq 0$ - відбулись три помилки.

Елементи поля Галуа і відповідні їм результати піднесені до кубу

1	2	3	4	5
0	0000	0	0	0
1	0001	1	1	1
2	0010	x	X	x^3
3	0011	x^4	1+x	x^{12}
4	0100	x^2	x^2	x^6
5	0101	x^8	$1+x^2$	x^9
6	0110	x^5	x^2+x	1
7	0111	x^{10}	x^2+x+1	1
8	1000	x^3	x^3	x^9
9	1001	x^{14}	x^3+1	x^{12}
10	1010	x^9	x^3+x	x^{12}
11	1011	x^7	x^3+x+1	x^6
12	1100	x^6	x^3+x^2	x^3
13	1101	x^{13}	x^3+x^2+1	x^9
14	1110	x^{11}	x^3+x^2+x	x^3
15	1111	x^{12}	x^3+x^2+x+1	x^6

Кількість активних S-боксів для кодів з максимальною довжиною:

$$N = (m_2 + 1)(m_1 + 1), \tag{12}$$

m_2 – довжина слова $КМД_к$, m_1 – довжина слова $КМД_в$ $КМД(2m, m, m+1)$

$$\begin{bmatrix} y_0 \\ \cdot \\ \cdot \\ \cdot \\ y_{m-1} \end{bmatrix} = \begin{bmatrix} c_{0,0} \dots c_{0,m-1} \\ \\ c_{ij} \\ \\ c_{m-1,0} \dots c_{m-1,m-1} \end{bmatrix} * \begin{bmatrix} x_0 \\ \cdot \\ \cdot \\ x_j \\ x_{m-1} \end{bmatrix}, \tag{13}$$

де x_j результуюче значення S-бокса. $x_i \in GF(2^n)$; y_j - результуюче значення дякого рівня гніздової SPN, $y_i \in GF(2^n)$; коефіцієнти матриці c_{ij} КМД – перетворення $c_{ij} \in GF(2^n)$.

Імовірність диференціальної характеристики раунда визначається виразом

$$P = p_s^n, \tag{14}$$

Імовірність лінійної характеристики раунда визначається виразом

$$Q = q_s^n, \qquad (15)$$

Варіанти гніздових SPN-мереж з S-боксами розміром 16 x 16 і відповідні показники ефективності реалізації

Номер варіанта	Тип КМД нижнього рівня	Тип КМД верхнього рівня	Коефіцієнт ефективності
1	2	3	4
1	(2, 1, 2)	(16, 8, 9)	11,7
2	(4, 2, 3)	(8, 4, 5)	18,3
3	(8, 4, 5)	(4, 2, 3)	20,6
4	(16, 8, 9)	(2, 1, 2)	11

Схема програми декодування

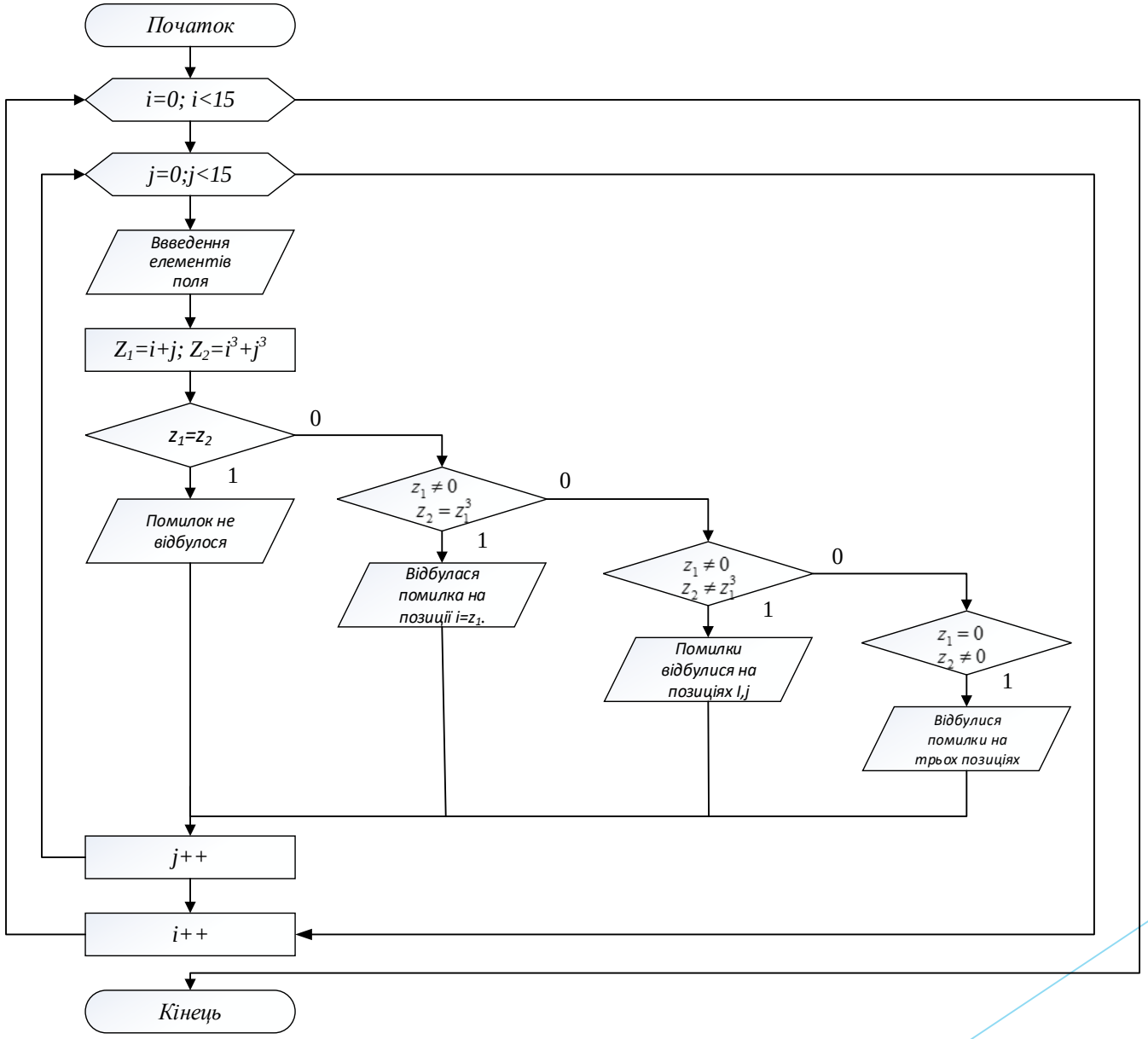
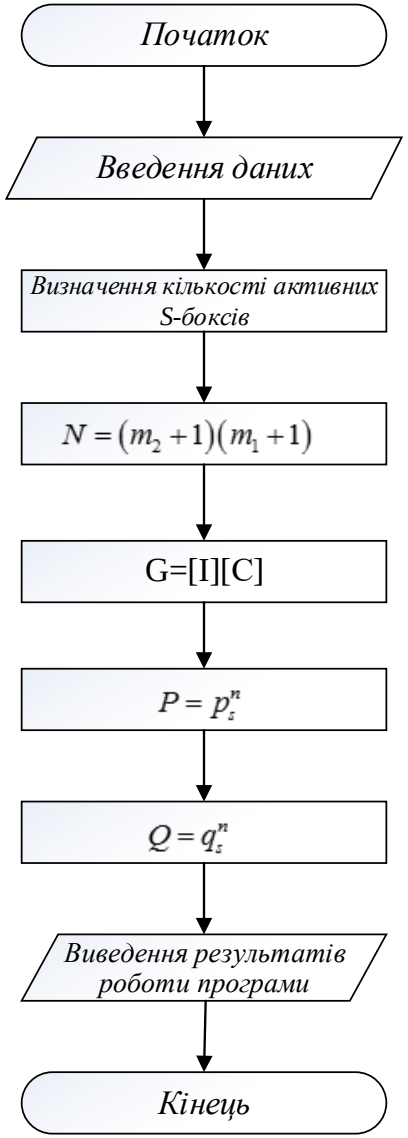
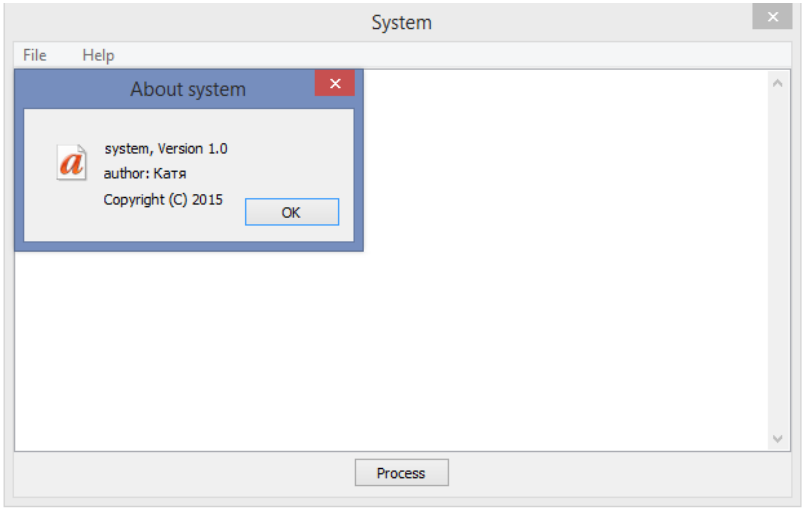
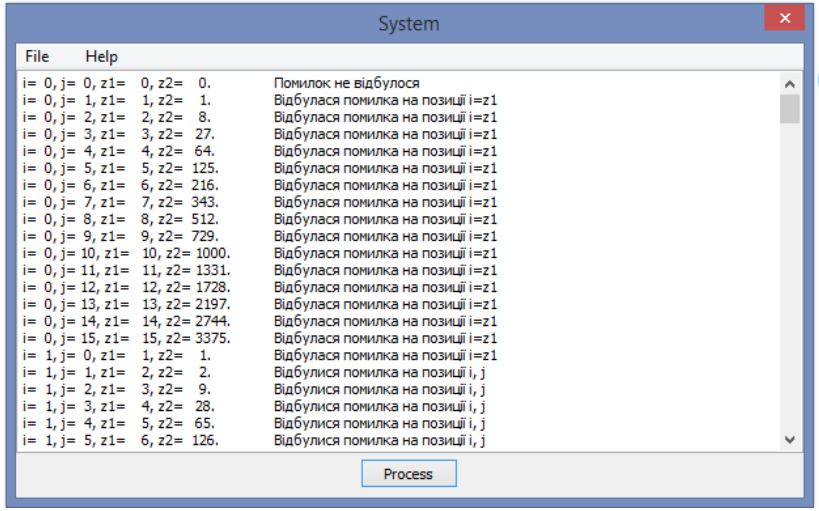
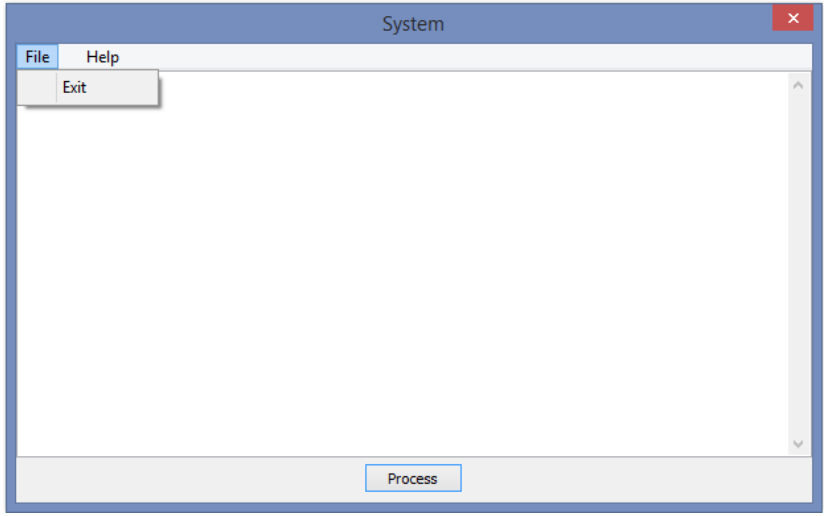


Схема програми шифрування




System
File
Help
About system
system, Version 1.0
author: Катя
Copyright (C) 2015
OK
Process


System
File
Help
i= 0, j= 0, z1= 0, z2= 0. Помилок не відбулося
i= 0, j= 1, z1= 1, z2= 1. Відбулася помилка на позиції i=z1
i= 0, j= 2, z1= 2, z2= 8. Відбулася помилка на позиції i=z1
i= 0, j= 3, z1= 3, z2= 27. Відбулася помилка на позиції i=z1
i= 0, j= 4, z1= 4, z2= 64. Відбулася помилка на позиції i=z1
i= 0, j= 5, z1= 5, z2= 125. Відбулася помилка на позиції i=z1
i= 0, j= 6, z1= 6, z2= 216. Відбулася помилка на позиції i=z1
i= 0, j= 7, z1= 7, z2= 343. Відбулася помилка на позиції i=z1
i= 0, j= 8, z1= 8, z2= 512. Відбулася помилка на позиції i=z1
i= 0, j= 9, z1= 9, z2= 729. Відбулася помилка на позиції i=z1
i= 0, j= 10, z1= 10, z2= 1000. Відбулася помилка на позиції i=z1
i= 0, j= 11, z1= 11, z2= 1331. Відбулася помилка на позиції i=z1
i= 0, j= 12, z1= 12, z2= 1728. Відбулася помилка на позиції i=z1
i= 0, j= 13, z1= 13, z2= 2197. Відбулася помилка на позиції i=z1
i= 0, j= 14, z1= 14, z2= 2744. Відбулася помилка на позиції i=z1
i= 0, j= 15, z1= 15, z2= 3375. Відбулася помилка на позиції i=z1
i= 1, j= 0, z1= 1, z2= 1. Відбулася помилка на позиції i=z1
i= 1, j= 1, z1= 2, z2= 2. Відбулися помилка на позиції i, j
i= 1, j= 2, z1= 3, z2= 9. Відбулися помилка на позиції i, j
i= 1, j= 3, z1= 4, z2= 28. Відбулися помилка на позиції i, j
i= 1, j= 4, z1= 5, z2= 65. Відбулися помилка на позиції i, j
i= 1, j= 5, z1= 6, z2= 126. Відбулися помилка на позиції i, j
Process


System
File
Help
Exit
Process

ДЯКУЮ ЗА УВАГУ!