УДК 025.7/9
© Ю. Наконечний[1], П. Гаранюк[1], Я. Совин[1], М. Стахів[1], 2012

ВИКОРИСТАННЯ НЕЙРОМЕРЕЖЕВИХ ТЕХНОЛОГІЙ ДЛЯ ЗАХИСТУ БЛАНКІВ ЦІННИХ ПАПЕРІВ

Проведений аналіз моделі для реалізації нейромережевої технології захисту бланків цінних паперів яка містить базові компоненти симетричної системи шифрування. Розглянуто режими функціонування алгоритмі шифрування у складі нейромережевої системи захисту.

The analysis of model for realization of neural networks technology of defence of forms of securities is conducted which contains the base components of the symmetric system of enciphering. The modes of functioning are considered algorithm of enciphering in composition the neural networks system of defencion.

1. ВСТУП

Системи передачі інформації (системи зв'язку) та системи криптографічного захисту (секретні систем) мають низку аналогій, що дозволяють певною мірою ототожнювати розглянуті системи. Зокрема, розглядаючи принцип впливу завад в каналі зв'язку на інформацію та дію алгоритму шифрування на повідомлення, можна стверджувати, за Шенноном, про шифртекст як аналог спотвореного сигналу. Проте, дані системи мають ряд розбіжностей, що полягають у складності процесу шифрування, природі ключа та спеціалізованому захисті характеристик інформації. Особливо розбіжності проявляються при побудові спеціалізованих систем – наприклад для захисту цінних паперів.

2. ПОСТАНОВКА ПРОБЛЕМА

Проаналізувати особливості реалізації алгоритмів шифрування у нейромережевій системі захисту цінних паперів, у різних режимах роботи і при варіації параметрів захисту.

3. СТРУКТУРНА СХЕМА СИСТЕМИ ЗАХИСТУ БЛАНКІВ ЦІННИХ ПАПЕРІВ НА ОСНОВІ НЕЙРОМЕРЕЖЕВИХ ТЕХНОЛОГІЙ

Розроблена схема системи включає в себе симетричну нейросистему, що реалізує нейромережевий алгоритм шифрування та програмний емулятор системи надійної передачі інформації .Система характеризується простотою використання внаслідок автоматичності процесів

[1] Національний університет «Львівська політехніка»

налаштування параметрів нейронної мережі та швидкодією за рахунок використання блокової структури нейромережевого декодера (рис.1).

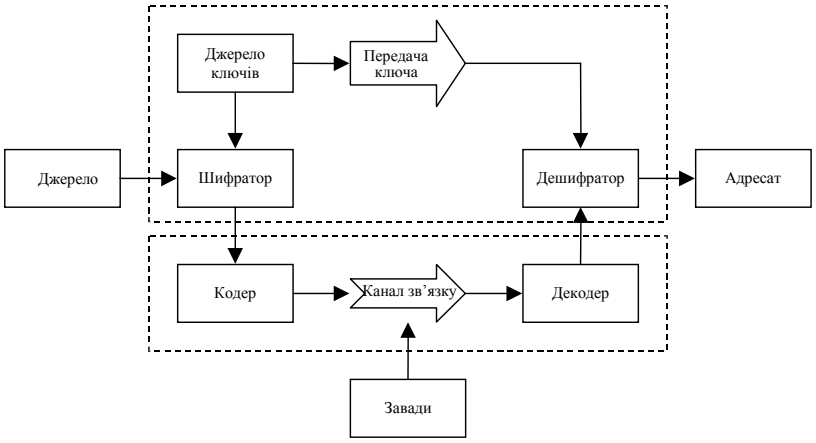

Рис. 1. Структурна схема системи комплексного захисту бланків цінних паперів

Вхідною інформацією (блок "Джерело", рис.1) служать файли даних, ефективна обробка яких забезпечується шляхом оперування побітовим машинним кодом. Внутрішні параметри програмних модулів (алгоритм кодування, генерація ключа та ін.) можуть вводитись в інтерактивному режимі або встановлюватись з попередньо створених бібліотек. Для експериментальних досліджень або подальшого гнучкого функціонування в програмних модулях була передбачена можливість зміни параметрів, таких як рівень завад в каналі зв'язку та довжина ключа.

Кожна компонента наведеної схеми містить елементи, що передбачають використання нейромережі та реалізують задачі підтримки інформаційних характеристик з наперед обумовленим ступенем захисту. В залежності від вибраної задачі (забезпечення цілісності, конфіденційності) в процесі роботи використовується відповідний модуль схеми і певна конфігурація кожної складової.

4. АБСОЛЮТНО СТІЙКІ ТА СТІЙКІ В ОБЧИСЛЮВАЛЬНОМУ СЕНСІ ШИФРИ

Для більш детального пояснення можливостей функціонування запропонованого нейромережевого алгоритму шифрування в різних режимах, розглянемо особливості побудови шифрів підкласу симетричних: блокових та потокових. Типовим представником останнього підкласу є шифр Вернама, який відповідає умові абсолютної стійкості, але

відрізняється складністю реалізації, оскільки вимагає наявності надійного каналу зв'язку для обміну довгим ключем. Для всіх інших шифрів був введений критерій надійності в обчислювальному сенсі, який відображає кількісну оцінку необхідних часових ресурсів для розкриття шифру, при яких таємниця втрачає актуальність.

Найвідомішим шифром, надійним саме в обчислювальному сенсі, є шифр Фейстеля, що був реалізований в стандарті DES. Розглянемо принципи побудови та процеси шифрування і дешифрування зазначених вище шифрів.

Шифр одноразового блокноту (шифр Вернама) оперує інформацією в двійковому представленні, над якою проводяться бінарні операції. Причому, в словах однакової довжини додавання відбувається побітово, що відповідає властивостям потокового шифру.

Позначимо результати додавання слів x та y як $x \oplus y$. Тоді для суми повинні виконуватись наступні властивості, що обумовлюють можливість дешифрування тексту:

$x \oplus y = y \oplus x$;

$(x \oplus y) \oplus z = x \oplus (y \oplus z)$;

$x \oplus \varnothing = x$;

$x \oplus x = \varnothing$, причому $|x| = |y| = |\varnothing|$.

Перед шифруванням повідомлення записується у двійковій формі та перетворюється за допомогою ключа в шифртекст

$C = M \oplus K$, $|M| = |K|$.

Процес дешифрування, відповідно

$$C \oplus K = (M \oplus K) \oplus K = M \oplus (K \oplus K) = M \oplus \varnothing = M$$

В шифрі Фейстеля враховуються переваги і недоліки шифру одноразового блокноту. Він також оперує інформацією в двійковому представленні, блоки якої шифруються за допомогою ключа однакової з блоком сталої довжини. Для створення криптосистеми DES був обраний саме шифр Фейстеля в якості базового, оскільки він відповідав основним вимогам:

можливість та однозначність дешифрування:

$\forall K \;\; E_K(M') \neq E_K(M'')$, якщо $M' \neq M''$;

– ефективність, що визначається швидкодією;
– надійність в обчислювальному сенсі.

В результаті модифікації та покращень шифру Фейстеля був створений алгоритм DES, що включає в себе наступні кроки:

крок 1. Перестановка бітів вхідного повідомлення відповідно до спеціальних IP-перестановок;

крок 2. Повідомлення розбивається на блоки $|M_i| = 64$, $i = \overline{1, n}$;

крок 3. Формування ключів для циклів шляхом розбиття вихідного ключа

$K = (K_1, K_2, \ldots, K_{16})$; $|K_j| = 48$, $j = \overline{1,16}$.

крок 4. Блок повідомлення розділяється на праву R_0 та ліву L_0 частини над якими відбуваються перетворення

$L_j = R_{j-1}$ та $R_j = L_{j-1} \oplus f(R_{j-1}, K_j)$,

де f – функція перетворювача;

крок 5. $E_K(M) = R_{16}L_{16}$;

крок 6. Застосовуються IP-1 перестановки.

Дешифрування відбувається в зворотному порядку:

$$M = E_{K_{16}, K_{15}, \ldots, K_1}(C).$$

Зазначимо, що з 64 бітів ключа *K* алгоритм DES використовує лише 56, решта бітів використовуються для перевірки надійності передачі ключа з точки зору теорії інформації.

В практичних системах шифрування використовується лише один із наведених вище режимів, оскільки їх поєднання призводить до істотного збільшення необхідних ресурсів на виконання.

Розглянемо симетричний алгоритм шифрування, що містить залежні від ключа взаємообернені перетворення вихідного тексту. При достатньо великому розмірі повідомлення розбивається на блоки фіксованої довжини і кожен блок шифрується окремо та незалежно один від одного, тобто відбуваються перетворення

$$C_i = E_K(M_i),\ i = \overline{1, n},$$

$$M_i = D_K(C_i),\ i = \overline{1, n},$$

причому $|C_i| = |M_i| = N$,

де N – довжина блоку; n – кількість блоків.

Такий режим шифрування називається *режимом простої заміни* або електронної кодової книги (Electronic Code Book – ECB). При його використанні на практиці виникає ряд проблем:

при $|M_n| < N$ (рис. 2);

якщо $\forall i, j\ \ M_i = M_j$, то $C_i = C_j$.

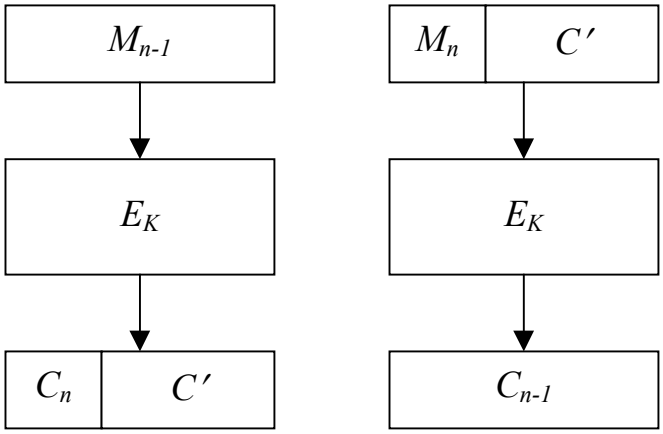

Рис. 2. Ілюстрація проблеми шифрування останнього блоку в ECB

Для усунення зазначених недоліків, були розроблені наступні способи використання криптологічних перетворень (зчеплення блоків), які роблять залежним блок шифртексту від попередніх блоків відкритого і зашифрованого тексту :

$$C_i = F\left(M_1, M_2, \ldots, M_i, C_1, C_2, \ldots, C_{i-1}\right), \; i = \overline{1,n},$$

де F – рандомізуюча функція, для якої виконується умова

$$F\left(M_1, M_2, \ldots, M_i, C_1, C_2, \ldots, C_{i-1}\right) \neq$$
$$\forall i, j \;\; F\left(M_1, M_2, \ldots, M_j, C_1, C_2, \ldots, C_{j-1}\right).$$

В залежності від способу та порядку використання операцій розрізняють два основні режими шифрування: блоковий та потоковий.

Блоковий режим

Повідомлення, яке було розбите на блоки, спочатку модифікується шляхом накладання на нього за допомогою бінарної операції значення рандомізуючої функції, після чого отримане значення перетворюється згідно E_K. Тобто, процес шифрування (рис. 3) та розшифрування в блоковому режимі можна представити як

$$C_i = E_K\left(M_i \oplus F\left(M_1, M_2, \ldots, M_i, C_1, C_2, \ldots, C_{i-1}\right)\right),$$
$$i = \overline{1,n},$$

$$M_i = D_K\left(C_i \oplus F\left(M_1, M_2, \ldots, M_i, C_1, C_2, \ldots, C_{i-1}\right)\right),$$
$$i = \overline{1,n}.$$

Необхідно зазначити, що в якості бінарної операції будемо використовувати операцію додавання за модулем 2, оскільки вона представляється найбільш простою для обчислень та технічної реалізації.

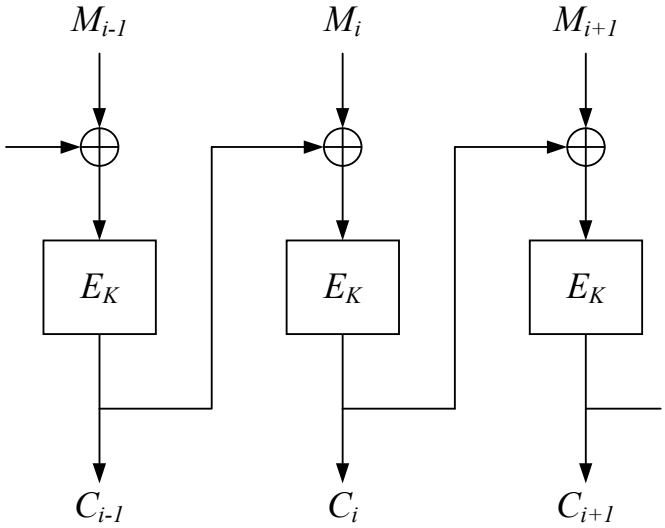

Рис. 3. Процес блокового шифрування

В залежності від алгоритму шифрування розмір блоку при цьому режимі може бути в діапазоні 64÷1024 біт, причому збільшення розміру блоку спричиняє збільшення швидкодії алгоритму. До недоліків блочного режиму можна віднести появу штучної часової затримки, що обумовлюється необхідністю заповнення блоку перед початком шифрування. Така властивість може негативно відображатись на якості обробки мультимедійних даних, при передачі яких використовується режим реального часу.

Потоковий режим

Блок вихідного тексту модифікується шляхом накладання на нього результату криптографічного перетворення E_K значення рандомізуючої функції, а саме

$$C_i = M_i \oplus E_K\left(F\left(M_1, M_2, \ldots, M_i, C_1, C_2, \ldots, C_{i-1}\right)\right), \quad i = \overline{1,n},$$
$$M_i = C_i \oplus D_K\left(F\left(M_1, M_2, \ldots, M_i, C_1, C_2, \ldots, C_{i-1}\right)\right), \quad i = \overline{1,n}.$$

Актуальність застосування режиму потокового шифрування набула важливого значення з появою мультимедійних засобів та мереж з високою пропускною здатністю. В сучасних інформаційних системах застосовуються інноваційні технології, які вимагають передачі великих об'ємів даних в режимі реального часу. До таких технологій можна віднести: факсимільний, відео та мовний зв'язок; голосова та відео пошта; системи відеоконференцій.

Оскільки при передачі оцифрованої звукової, графічної та відео інформації окрім вимоги швидкодії висувається вимога забезпечення конфіденційності, виникає проблема шифрування великих обсягів даних, що розв'язується з застосуванням потокового режиму шифрування.

Отже, для застосування блокового режиму необхідна наявність стійкого та взаємооберненого криптографічного перетворення, на відміну від режиму потокового шифрування, до якого висувається вимога тільки про його стійкість. Основні параметри симетричних алгоритмів з блоковим режимом шифрування наведено у таблиці 1.

Таблиця 1

Базові параметри симетричних алгоритмів шифрування

Назва алгоритму	Довжина блоку, біт	Розмір ключа, біт	Кількість циклів	Потужність множини ключів	Основні операції *
DES	64	56÷256	16	$7{,}2\times10^{16}\div1{,}2\times10^{77}$	SB, TR, ⊕
FEAL	64	64	≥4	$1{,}8\times10^{19}$	AD(8), RO, ⊕
		128		$3{,}4\times10^{38}$	
IDEA	64	128	8	$3{,}4\times10^{38}$	ML(16)+1, AD(16), ⊕
ГОСТ-28147-89	64	256	32	$1{,}2\times10^{77}$	AD(32), ⊕, TR, RO
RC5	32, 64, 128	≤2040	≤255	$1{,}3\times10^{61}$	AD(x), RO, ⊕
Blowfish	64	≤448	16	$7{,}2\times10^{34}$	AD(32), SB, ⊕
Skipjack	64	80	32	$1{,}2\times10^{25}$	-/-
Safer	64	40	≤10	$1{,}1\times10^{12}$	-/-
		64		$1{,}8\times10^{19}$	
		128		$3{,}4\times10^{38}$	

* SB – підстановка, TR – перестановка, ⊕ – додавання за модулем 2, AD(x) –додавання за модулем 2^x, RO – циклічний зсув, ML(x) –

множення за модулем 2^x , “-/-“ – дані відсутні, алгоритм в процесі тестування.

5. ВИСНОВКИ

Проведені дослідження показали, що алгоритм та отримані результати дозволяють виконувати оптимізацію структури захищеної нейромережі при її удосконаленні або додаванні нових компонентів.

1. Вербіцький О.В. Вступ до криптології.- Львів: В-во наук.-техн. літ-ри, 1998.- 247с. 2. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах.- К.: Корнейчук, 2000.- 152с. 3. Grzywak A. Bezpieczenstwo systemow komputerowych.- Gliwice: Wydawnictwo pracowni komputerowej jacka skalmierkiego, 2000.- 326p. 4. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C.- New York: 2d ed., John Wiley&Sons Inc., 1996.- 675p. 5. Грицик В.В., Томашевський О.М. Нейромережевий підхід до забезпечення захисту інформації з високими показниками завадостійкості при передачі // Доповіді Національної академії України.- 2003.- №3.- С.62-68. 6. Hrytsyk V.V., Aizenberg N.N., Tkachenko R.O. and other. The neural and neural-like networks: synthesis, realization, application and future // Інформаційні технології і системи.- 1998.- №1/2.- С.15-55. 7. Ткаченко Р.О. Неітераційне навчання штучних нейронних мереж прямого поширення // Технічні вісті.- 1999.- №1(8), 2(9).- С.41-42. 8. Томашевський О.М. Нейромережева криптосистема з таємним ключем // Інформаційні технології і системи.- 1999.- Т.2, №1.- С.143-150. 9. Томашевський О. Захист середовища передачі даних в оперативному поліграфічному комплексі // Комп'ютерні технології друкарства.- 2000.- №5.- С.368-375.