розпізнавання образів, системи асоціативної пам'яті, компресія даних, оптимізаційні задачі, теорія керування, розробка нейрокомп'ютерів, наближення функцій з високою точністю, екстраполяція та прогнозування.

Розвиток теорії штучних нейронних мереж багато у чому пов'язаний із іменами У. Маккалока, Ф. Розенблатта, Б. Уідроу, М. Мінскі, Т. Кохонена, С. Мууроги, В. Вапніка, Д. Хопфілда, Дж. Хінтона та інших. Значний внесок був зроблений українськими вченими М. Амосовим, О. Івахненком, Є. Бодянським, Н. Айзенбергом, І. Айзенбергом Р. Ткаченком, Л. Тимченком, О. Михальовим, В. Литвиненком, Ф. Гече, П. Тимощуком, Ю. Романишином.

Однак, незважаючи на значні успіхи, досягнуті останнім часом у застосуванні нейромережних технологій, при використанні прикладних систем на основі штучних нейронних мереж необхідно вирішувати такі завдання, які існуючими системами на основі традиційних нейропарадигм розв'язуються з недостатньою точністю або швидкістю. Саме тому актуальним є вирішення задачі розробки і дослідження моделей узагальнених штучних нейронних елементів, які мають більш високі функціональні можливості, ніж звичайні нейронні елементи. Важливою науковою задачею є розроблення та обґрунтування ефективних методів навчання ШНМ, побудованих на основі узагальнених нейронних елементах.

Література

1. Хайкин С. Нейронные сети, полный курс. 2-е изд., перед. М. : Вильямс, 2008. 1103 с. ISBN 5-8459-0890-6

2. Whitely D., Starkweather T., Bogart C. Genetic Algorithms and Neural Networks: Optimizing Connections and Connectivity. *Parallel Computing.* 1990. Vol. 14.

3. Tang C., He Y., Yuan L. A Fault Diagnosis Method of Switch Current Based on Genetic Algorithm to Optimize the BP Neural Network : International Conference on Electric and Electronics. 2011. Vol. 99.

4. Jinru L., Yibing L., Keguo Y. Fault diagnosis of piston compressor based on Wavelet Neural Network and Genetic Algorithm : Proceedings of the 7th World Congress on Intelligent Control and Automation. 2008.

5. Wu W., Guozhi W., Yuanmin Z., Hongling W.Genetic Algorithm Optimizing Neural Network for Short-Term Load Forecasting : International Forum on Information Technology and Applications. 2009.

УДК 544.421.43:544.421.032.76:544.431.122.2:547.541:547.636.3

СТВОРЕННЯ ДОДАТКУ З ГРАФІЧНИМ ІНТЕРФЕЙСОМ «РЕАЛІЗАЦІЯ АЛГОРИТМУ ШИФРУВАННЯ RC5»

В. Г. Крижановський, А. І. Шевченко

Блочний шифр RC5 - алгоритм прямого шифрування, при якому береться блок даних заданого розміру (2w бітів) і з нього за допомогою залежного від ключа перетворення генерується блок шифрованого тексту такого самого розміру. Цей режим часто називають режимом ECB (режим електронної шифрувальної книги).

У класичному алгоритмі використовуються три примітивних операції їх інверсії:

- складання по модулю;
- побітовое виключення АБО (XOR);
- операції циклічного зсуву на змінне число біт.

Основним нововведенням є використання операції зсуву на змінне число біт, що не використалися в більш ранніх алгоритмах шифрування. Ці операції однаково швидко виконуються на більшості процесорів, але в той же час значно ускладнюють диференційний і лінійний криптоаналіз алгоритму.

Шифрування за алгоритмом RC5 складається з двох етапів. Процедура розширення ключа і безпосередньо шифрування.

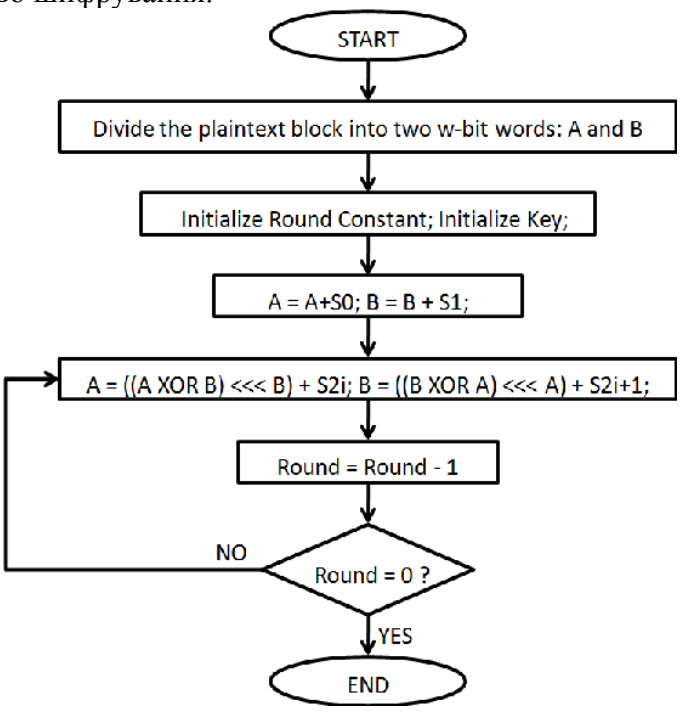

Рис. 1. Алгоритм реалізації шифру RC5

Програма працює з алгоритмом RC5 32/100/128:

– 32 – розмір слова в бітах;

– 100 – кількість раундів (повторів по циклу);

– 28 – розмір ключа в байтах.

Заданий текст для шифрування: «RC5 is a symmetric-key block cipher. Designed by Ronald Rivest in 1994.»

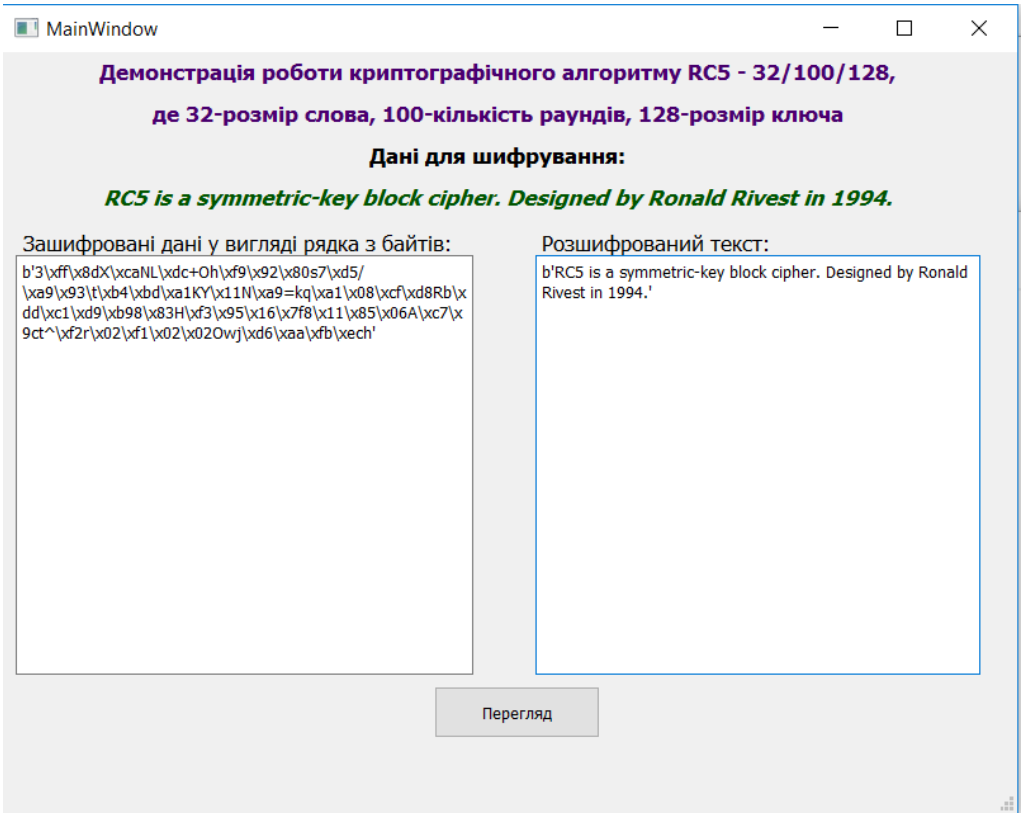

Рис. 2. Виведення зашифрованого та розшифрованого текстів у байтовій формі

Висновки: Працюючи над роботою, було досліджено принцип роботи алгоритму, його характеристики, спосіб шифрування та дешифрування даних, його криптостійкість і, як наслідок, доцільність практичного використання.

У ході роботи було створено програмний продукт з графічною оболонкою, який реалізовує заданий алгоритм шифрування з розміром слова в 32 біти, 100 раундами та 128-байтовим ключем.

Література

1. Методи криптографії. 2017. URL : https://www.dkws.org.ua/article.php?id=80
2. Алгоритм шифрування RC5. 2013. URL : https://studbooks.net/1590228/informatika/algoritm_shifrovaniya
3. RC5. 2015. URL : https://ru.wikipedia.org/wiki/RC5

УДК 004.56.53

АВТОМАТИЗАЦІЯ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ МЕРЕЖЕВИХ ПРОГРАМ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ЛЮДИНИ

Т. О. Лукашук

Контроль доступу на основі мережевих програм розпізнавання обличчя людини відноситься до біометричних методів контролю доступу, над якими сьогодні працюють передові організації світу, такі як: Amazon, Google, IBM і т. д. Біометричні методи розпізнавання людини доволі давно використовуються правоохоронними органами, для ідентифікації людей. Ідея для створення методів аутентифікації та авторизації на основі біометричних даних людини на сьогоднішній день має доволі велике поширення, наприклад в багатьох смартфонах на сьогоднішній день використовуються оптичні сканери відбитку пальця для авторизації користувачів, також використовуються методи розпізнавання обличчя, за допомогою його геометрії, які наприклад в останній моделі iPhone X, називаються FaceID. Біометричні системи авторизації – це зручно, швидко та надійно. Про надійність цих систем, говорить те, що їх використовують в Пентагоні. До недавніх пір головним фактором, який заважав цим системам розвиватись – це була їхня ціна, але з розвитком технологій на сьогоднішній день ситуація змінилась.

Біометричні системи аутентифікації:

Біометрична система аутентифікації – це система аутентифікації, яка використовує для підтвердження особистостей їхні біометричні данні. Процес доказу і перевірки належності заявленого користувачем імені, через представлення користувачем свого біометричного зразку, шляхом перероблення цього зразка відповідно до заранння визначеного протоколу.

Біометричні системи аутентифікації поділяються на 2 види: Статичні методи та Динамічні методи.

Статичні методи основані на фізіологічних характеристиках людини, які присутні від народження до смерті, які знаходяться при людині на протязі всього життя, і які не можуть бути втрачені, вкрадені або скопійовані. Наприклад: аутентифікація по відбитку пальця, геометрії руки, геометрії лиця, термограмі лиця.

Динамічні методи біометричної аутентифікації та ідентифікації основані на поведінкових характеристиках людей, тобто основані на характерних для підсвідомих рухів в процесі відтворення або повторення якої-небудь звичайної дії. Наприклад: Аутентифікація по голосу чи почерку.

Біометричні системи аутентифікації повинні відповідати 5 параметрам:

1) Всезагальність: Даний признак повинен бути присутній у всіх людей без виключення.