DOI: <https://doi.org/10.32839/2304-5809/2019-12-76-3>

УДК 377.169.3

Семенюк А.О., Чабан С.В.

Одеський національний політехнічний університет

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ, ЩО НАВЧАЄ ШИФРУВАННЮ З ЗАМІНОЮ

Анотація. Аналізуючи сучасний світ ми розуміємо, що в даний час існує потреба в автоматизованих навчальних системах, які використовуються в багатьох областях. Вони дозволяють автоматизувати працю викладача, зокрема видачі варіанта завдання, перевірки правильності його виконання студентом. Такі системи повинні мати найбільш широкі функціональні можливості та високу ефективність в навчальному процесі. В даній статті було розглянуто проблему розробки автоматизованих навчальних систем. Проводиться аналіз існуючих навчальних систем для виявлення недоліків та вивчення методів шифрування більш докладніше. Описується розробка підсистеми шифрування та підсистеми оцінювання на рівні логіки програми. Наводяться приклади та описання методів, які використовуються. Описується розробка інтерфейсу користувача на рівні представлення системи та розробка бази даних системи.

Ключові слова: шифрування, шифрування з заміною, автоматизована система, що навчає, шифр Цезаря, шифр Трітемуса, класифікація оцінок, навчання, система зі зворотнім зв'язком.

Semeniuk Anastasiia, Chaban Stanislav

Odessa National Polytechnic University

DEVELOPMENT OF AN AUTOMATED SYSTEM THAT TEACHES REPLACEMENT ENCRYPTION

Summary. Analyzing the modern world, we understand that at present there is a need for automated training systems that are used in many areas. Such systems allow you to automate the work of the teacher, in particular the issuance of a variant of the task and verification of the correctness of its implementation by the student. Given the human factor and fatigue, the teacher can make mistakes, and the system is not interested in any student. Currently, the use of training systems for the study of encryption methods is spreading, this is due to the fact that these methods are the basis of many information protection technologies. Automated systems have the widest functional capabilities and high efficiency in the educational process, where feedback is organized between the student and the educational system. This article discusses the problem of developing automated learning systems. The analysis of existing training systems is carried out to identify shortcomings and a more detailed study of encryption methods. The identification of previously unresolved parts of a common problem is manifested in the absence of built-in tools for testing knowledge about encryption-decryption methods, the implementation of several encryption methods, the lack of knowledge assessment and verification options. The aim of the article is to develop a system that teaches cryptography with replacement with a subsystem for assessing the quality of training. To develop the system, a three-level architecture was chosen: the presentation level, the program logic level and the data level. The presentation layer includes an interface. At the logical level of the program, the encryption subsystem, the evaluation subsystem, and the database interaction subsystem are presented. The data layer includes a database. The development of the encryption subsystem and the evaluation subsystem at the program logic level is described. Examples and description of the methods used are given. An algorithm for determining students' knowledge assessment is presented. It describes the development of the user interface at the level of system representation and the development of the database system. An experiment was conducted using the system and the results were presented.

Keywords: encryption, replacement encryption, training system, Caesar's code, Triteimius code, classification of ratings, training, feedback system.

Постановка проблеми. Автоматизовані навчальні системи (АНС) використовуються в багатьох областях, а саме під час вивчення правил дорожнього руху, іноземних мов, мови програмування тощо. Такі системи дозволяють автоматизувати працю викладача, зокрема видачі варіанта завдання, перевірки правильності його виконання студентом. З огляду на людські фактори і втому, викладач може допустити помилки, а система безкорисна до будь якого студента.

В даний час поширюється використання АНС для вивчення методів шифрування, що пов'язане з тим, що ці методи лежать в основі багатьох технологій захисту інформації. Шифруванням називається оборотний процес перетворення інформації з метою їх приховування від непривілейованих осіб.

Проаналізуємо існуючі АНС для вивчення методів шифрування більш докладніше.

Аналіз останніх досліджень та публікацій. На теперішній час існує доволі мало публікацій на тему автоматизованих систем, що навчають шифруванню. При цьому на ринку програмних продуктів за останнє десятиліття з'явилося досить велика кількість навчальних систем, в тому числі і автоматизованих навчальних систем, які охоплюють різні предметні області, і покликані вирішувати завдання навчання на різних етапах життя людини. Кожна АНС має чітко виражену структуру на основі групи елементів із зазначенням зв'язків між ними, яка надає уявлення о системі в цілому. Тому структура системи може бути охарактеризована за наявними в ній типам зв'язків. В кожній публікації АНС дає можливість перевіряти знання сутності

методів шифрування / дешифрування даних, але ні в одній з них немає вбудованих засобів для перевірки знання методів.

Виділення невирішених раніше частин загальної проблеми проявляється у відсутності вбудованих засобів для перевірки знання методів шифрування-дешифрування, реалізації небагатьох методів для шифрування, відсутності оцінювання знань та варіантів для перевірки.

Мета дослідження – розробка системи, яка навчає шифруванню з заміною з підсистемою оцінювання якості навчання на базі трьохрівневої архітектури. Така архітектура забезпечить поширення програмного коду та реалізується у вигляді трьох рівнів: рівня представлення, рівня логіки програми та рівня даних.

Виклад основного матеріалу. Найбільш широкими функціональними можливостями і високою ефективністю в навчальному процесі мають АНС, де організований зворотний зв'язок між учнем і навчальною системою. Розглянемо узагальнений принцип функціонування такої АНС (рис. 1). Процес взаємодії учня з АНС може бути представлений у вигляді зовнішнього зворотного зв'язку, де АНС спрямована на підвищення рівня знань користувача, і тим самим зменшення кількості помилок їм зроблених. Ланкою прямого каналу регулювання тут виступає АНС, об'єктом регулювання – «Учень». Генерація впливів на учня з боку АНС відбувається відповідно до знань учня на основі накопиченого їм раніше досвіду і вхідним завданням, а також в залежності від прийнятих в програмному забезпеченні критеріїв достовірності оцінки знань учня. Залежно від характеру впливу з боку АНС учень приймає певне, достовірне з його точки зору, рішення, яке доводить, на його думку, факт засвоєння їм поданого матеріалу, і генерує його на вхід комп'ютера. Реакція учня на дії з боку АНС можна розглядати у вигляді деякої функції рівня кількості помилок в залежності від висунутої сукупності завдань, які має вирішити користувач. Вид цієї функції залежить від індивідуальних властивостей учня і програмного забезпечення.

Рис. 1. Узагальнена структурна схема замкнутої системи «АНС – учень»

Розглянемо декілька прикладів автоматизованих навчаючих систем.

Однією з існуючих систем, що навчають шифруванню, є система, розроблена у Вологодському Державному Педагогічному Інституті [1]. Вона дозволяє в інтерактивному режимі ввести тексти для шифрування або дешифрування в одне з двох вікон. Після натискання на кнопки «Шифрувати» або «Дешифрувати» у вільному вікні з'являється результат комп'ютерної обробки. Його можна звірити з результатом ручного шифрування.

Методи, які реалізуються системою: метод Цезаря (у тому числі з ключовим словом), афінна

кріптосистема, метод Полібія, метод смужок, система Віжинера, система Бофорта, система з автоключем (рис. 2). Є також можливість проводити частотний аналіз текстів. Також реалізовані наступні можливості: видача варіанта завдання з числа закладених в систему методів; виклик форм для комп'ютерної перевірки вміння шифрувати і розшифровувати шляхом використання відповідних криптографічних методів; оцінка правильності виконання завдання (рис. 3).

Рис. 2. Приклад діалогового вікна (метод Віжинера)

Рис. 3. Основне вікно системи, розробленої у Вологодському державному педагогічному інституті

Недолік розглянутої АНС в тому, що у програмі заздалегідь додані правильні відповіді; вона не має вбудованих засобів для перевірки знання методів шифрування-дешифрування; відсутній особистий кабінет для викладача та студента.

Ще одна АНС, що навчає шифруванню, розроблено у Волгоградському Державному Аграрному Університеті [2]. Ця система наочно відображає процеси перетворення тексту при шифруванні / дешифруванні і надає студенту можливість перегляду значень проміжних точок в межах перетворення. В сукупності з дружнім інтерфейсом (рис. 4), що забезпечує простоту і зручність використання, ця система сприяє кращому розумінню користувачем процесів перетворення інформації і дозволяє аналізувати роботу методів шифрування.

АНС, що розроблено у Волгоградському Державному Аграрному Університеті дозволяє в ін-

терактивному режимі ввести текст для шифрування в діалогове вікно. Після натискання на кнопки «Шифрувати» у вікні з'являється результат комп'ютерної обробки. Для перевірки правильності роботи програми натискається кнопка «Дешифрувати», після цього можна порівняти отриманий результат з початковим текстом. Далі користувач може проаналізувати метод шифрування, який реалізований у системі, а саме метод шифрування ГОСТ Р 28147-89.

Недолік розглянутої АНС в тому, що вона має небагато методів для шифрування, не має оцінки знання та варіантів для перевірки.

Для розробки АНС обрано трьохрівневу архітектуру: рівень представлення, рівень логіки програми, рівень даних (рис. 5).

Рівень представлення включає інтерфейс користувача. На рівні логіки програми представлено підсистему шифрування, підсистему оцінювання та підсистему взаємодії з базою даних. Рівень даних включає базу даних. Далі розглянуто аспекти реалізації перелічених компонентів АНС, яка навчає шифруванню з заміною.

Під час розробки підсистеми шифрування для АНС, що навчає шифруванню з заміною, використовуються методи симетричного шифрування Цезаря та Трітеміуса, а саме шифрування з простою заміною – клас методів шифрування, які зводяться до створення за певним алгоритмом таблиці шифрування, в якій для кожної букви відкритого тексту існує єдина зіставлена їй буква шифр-тексту [3; 4].

Шифр Цезаря – це вид шифру підстановки, в якому кожен символ у відкритому тексті замінюється символом, що знаходиться на деякому постійному числі позицій ліворуч або праворуч нього в алфавіті. Наприклад, в шифрі зі зрушенням вправо на 3, А була б замінена на Г, Б стане Д, і так далі (рис. 6).

Шифр Трітеміуса являє собою вдосконалений шифр Цезаря, тобто шифр підстановки. Кожен символ повідомлення зміщується на символ, який відстає від даного на деякий крок. Для шифра Трітеміуса крок зміщення робиться змінним, тобто залежним від будь-яких додаткових чинників. Наприклад, можна задати закон зміщення у вигляді лінійної функції (рівняння шифрування) позиції шифруємої літери. Сама функція повинна гарантувати цілочисельне значення. Прямая функція шифрування повинна мати зворотню функцію шифрування, теж цілочисельну.

Деякі варіанти обчислення кроку зміщення k : $k = Ar + B$ або $k = Ar^2 + Br + C$, де r – позиція букви в повідомленні, A, B, C – цілочисельні константи.

Рівнянням шифрування називається співвідношення, яке описує процес утворення зашифрованих даних з відкритих даних.

Рівняння шифрування для шифру Трітеміуса має наступний вигляд:

$$L = (m + k) \bmod N, \quad (1)$$

Рис. 4. Приклад діалогового вікна АНС, що навчає шифруванню, розробленої у Волгоградському державному аграрному університеті

Рис. 5. Структурна схема АНС

Рис. 6. Принцип роботи шифру Цезаря

де L – номер зашифрованої букви в алфавіті (таблиці Трітеміуса); m – номер позиції букви тексту в алфавіті, що шифрується; k – крок зсуву (функціональна залежність від позиції букви в повідомленні); N – число букв алфавіту (в таблиці Трітеміуса); $\bmod N$ – залишок від ділення на N .

Нехай у нас є якийсь алфавіт і якесь ключове слово, в даній роботі це «ТРИТЕМИУС». Складання таблиці відбувається наступним чином: вписуємо по черзі букви ключового слова, але якщо поточна буква вже потрапила в таблицю, другий раз її не вносимо. Далі по черзі дописуємо в таблицю букви алфавіту, пропускаючи ті, що були в ключовому слові. Для зручності алфавіт в таблиці створюємо більше, ніж початковий алфавіт, додаючи будь-які знаки, такі як «_», «.», «» тощо. У системі ми використовуємо російський алфавіт, де 33 літери, а в таблиці – 36.

Для побудови шифру Трітеміуса виконуємо наступне:

- а) задаємо ключове слово і заповнюємо алфавіт ключа;
- б) обчислюємо зсув k ;
- в) знаходимо код зашифрованою літери, користуючись рівнянням (1);
- г) за кодом L відновлюємо чергову букву криптограми;
- д) повторюємо пункти а-в до закінчення тексту шифрограми.

Для дешифровки використовуємо формулу $m = (L - k) \bmod N$. У разі, якщо при дешифровці різниця $L - k$ стає негативною, додаємо до неї N доти, поки вона не стане позитивною. Після цього вже беремо залишок від ділення.

Навчальна система, що розробляється, на рівні представлення включає інтерфейс корис-

тувача, який перед усім дає можливість вибору профілю для входу, такого як «Студент» і «Преподаватель» (рис. 7).

Діалогове вікно системи (рис. 8), що реалізує закладені методи шифрування з заміною, а саме, метод Цезаря та метод Трітеміуса, містить два основних поля, таких як «Исходный текст» і «Шифрованный текст», також містить кнопку «Задание», яка виводить варіант початкового тексту. Кнопка «Проверить» змушує систему саму зашифрувати початковий текст і звірити з введеним користувачем, підрахувати кількість помилок і поставити оцінку (рис. 9). Кнопка «Назад» повертає у попереднє діалогове вікно. Для методу Трітеміуса є додаткове поле для введення кроку зміщення.

Дана система дозволяє перевірити знання сутності методів шифрування даних. Система у профілі «Преподаватель» доповнена функціями авторизація студента, класифікація оцінок студента: високий, середній та низький, згідно яким формується завдання.

Профіль «Преподаватель» має можливість додавати до бази даних (БД) списки груп студентів, також система заповнює цей список оцінками, які заробили студенти.

У профілі «Студент» студент може авторизуватись і зайти до свого особистого кабінету, де він може переглянути всі свої оцінки та середній бал.

Для створення даної системи була обрана об'єктно-орієнтована мова програмування C# [7].

Навчальна система, що розробляється, на рівні представлення включає підсистему оцінювання. Після виводу підсистемою взаємодії з базою даних варіанту початкового тексту, користувач вводить зашифрований текст. Після натискання користувачем на кнопку «Проверить» підсистема оцінювання сама шифрує початковий текст і звіряє з введеним користувачем текстом. Ведеться підрахунок невідповідностей. Далі підсистема оцінювання ставить користувачу оцінку виходячи з кількості помилок.

Для визначення оцінки студента в підсистемі оцінювання реалізований алгоритм з рис. 10.

Рис. 7. Вікно системи з варіантами можливих профілів

Рис. 8. Приклад діалогового вікна для шифрування методом Трітеміуса

Рис. 9. Приклад вікна оцінювання знань студента

Рис. 10. Алгоритм визначення оцінки студента

Згідно цьому алгоритму для кожного методу шифрування спочатку підраховується кількість помилок, скоєних користувачем. Від кількості помилок залежить оцінка.

Оцінювання проходить за принципом перевірки диктантів в старшій школі. Від кількості зроблених студентом помилок залежить оцінка, яку підсистема оцінювання виставляє за 12-ти бальною шкалою. За безпомилкову відповідь ставиться максимальну оцінку 12. Якщо ж студент допустив 15 і більше помилок система ставить мінімальну оцінку 1. Критерії оцінки і визначення відповідності якості навчання до оцінки відповіді наведені в таблиці 1.

Розроблена система дозволяє автоматизувати працю викладача, зокрема видачі варіанта завдання, перевірки правильності його виконання студентом.

Був реалізований експеримент. Є група в 12 чоловік, в середньому на перевірку завдання одного студента викладач витрачає близько однієї години, так як обсяг одного завдання достатньо великий, тому на групу йде приблизно 12 годин. На перевірку завдання система витрачає близько 5 секунд з процесором Intel Core i3-5010U, 2.10 GHz CPU, пам'ять 4 GB, операційна система Windows 10, 64 бітова. З огляду на людські фактори і втому, викладач може допустити помилки, а система безкорисна до будь якого студента. Таким чином, викладач економить в середньому 11,5 годин, так як за півгодини він проходить по аудиторії і записує оцінки виставлені системою.

Навчальна система, що розробляється, на рівні представлення включає підсистему взаємодії з базою даних. Сама БД включає таблиці «Студенти», «Варіанти текстів» та «Логін для вчителів». При початку навчання студент вписує свої данні, обирає метод для шифрування, після чого підсистема рандомно надає учню варіант тексту та зберігає введену ним інформацію. По завершенню навчання підсистема зберігає оцінку студента, його ім'я та викладача. Якщо в системі реєструється або заходить до особистого кабінету викладач, то підсистема зберігає або знаходить указані логіни та паролі.

Схема бази даних системи представлена на рис. 11.

Перша таблиця призначена для зберігання варіантів текстів. Друга таблиця призначена

Таблиця 1

Критерії оцінювання якості навчання

Шкала оцінювання	Визначення якості навчання
1 бал	15 та більше помилок
2 бала	14 помилок
3 бала	12-13 помилок
4 бала	10-11 помилок
5 балів	8-9 помилок
6 балів	6-7 помилок
7 балів	5 помилок
8 балів	4 помилки
9 балів	3 помилки
10 балів	2 помилки
11 балів	1 помилка
12 балів	Немає помилок

Рис. 11. Схема бази даних системи

для зберігання логінів і паролів від профілів викладачів. Третя таблиця призначена для зберігання Ф.І.П. студентів, групи, фамілія викладача, метод шифрування/дешифрування.

Висновки. В даний час в процес навчання активно впроваджуються програмні технології на базі персональних комп'ютерів, що застосовуються для передачі учневі навчального матеріалу і контролю ступеня його засвоєння.

Дана робота присвячена розробці системи, яка навчає шифруванню з заміною з підсистемою оцінювання якості навчання на базі трьохрівневої архітектури. Така архітектура забезпе-

чує поширення програмного коду та реалізується у вигляді трьох рівнів: рівня логіки програми та рівня даних.

Рівень представлення включає інтуїтивно зрозумілий інтерфейс користувача. Рівень даних включає базу даних з трьох таблиць. Одна таблиця призначена для зберігання варіантів завдань, друга – для зберігання інформації, що корисна викладачеві, третя зберігає дані про студентів.

На рівні логіки програми реалізовано підсистему шифрування методами Цезаря і Трітеміуса для навчання шифруванню. Також реалізовано

підсистему оцінювання з розробленими критеріями оцінювання студента та підсистему взаємодії з базою даних, що реалізує підключення до бази даних з варіантами текстів для шифрування.

У подальшій розробці системи буде додана класифікація оцінок, отриманих одним студентом. Вона передбачає рівень складності завдання, що видає система. Якщо студент буде отримувати погані оцінки, то система буде надавати йому легший варіант, у разі підвищення середнього балу – система надаватиме складніший варіант.

Список літератури:

1. Ефимов С.С., Ефимова О.С. Методы шифрования и дешифрования данных в системе автоматизированного контроля знаний по разделу «Криптография» курса «Информационная Безопасность». *Омский научный вестник*. 2003. № 2(23). С. 124–129.
2. Яковлев С.Л. Интеллектуальная обучающая система алгоритмов шифрования данных. *Национальная ассоциация ученых*. 2016. № 3–1 (19). С. 34–37.
3. Мао В. Современная криптография: Теория и практика. Вильямс, 2005. 768 с.
4. Алферов А.П., Zubov A.Yu., Кузьмин А.С., Черемушкин А.В. Основы Криптографии. Москва, 2002. 480 с.
5. Уэйт М., Прага С., Мартин Д. Язык С. Руководство для начинающих. Москва, 1995. 521 с.
6. Menezes A., P. van Oorschot, Vanstone S. Handbook of Applied Cryptography. CRC Press, 1997.
7. Schneier B. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth). – John Wiley & Sons, Inc, 1996.
8. Простейшая кластеризация изображений методом k-средних (k-means) / Хабр. 2013. URL: <https://habr.com/ru/post/165087/> (дата звернення: 27.11.2019).

References:

1. Efimov, S.S., & Efimova, O.S. Methods of encryption and decryption of data in an automated knowledge control system for the "Cryptography" section of the "Information Security" course. *Omsk Scientific Herald*. 2003. Vol. 2, no. 23, pp. 124–129.
2. Yakovlev, S.L. Intelligent training system of data encryption algorithms. *National Association of Scientists*. 2016. Vol. 3-1, no. 19, pp. 34–37.
3. Mao, V. Modern cryptography: Theory and practice. Moscow, 2005. 768 p.
4. Alferov, A.P., Zubov, A.Yu., Kuzmin, A.S., & Cheremushkin, A.V. Fundamentals of Cryptography. Moscow, 2002. 480 p.
5. Waite, M., Prague, S., & Martin, D. Language C. Beginner's Guide. Moscow, 1995. 521 p.
6. Menezes, A., P. van Oorschot, & Vanstone, S. Handbook of Applied Cryptography. CRC Press, Inc, 1997.
7. Schneier, B. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth). John Wiley & Sons, Inc, 1996.
8. The simplest clustering of images using the k-means method (k-means). Habr. 2013. URL: <https://habr.com/ru/post/165087/>