УДК 004.3

АЛГОРИТМ КРИПТОГРАФІЧНОГО ЗАХИСТУ ТЕКСТОВИХ ДАНИХ НА ОСНОВІ ХЕШ-ФУНКЦІЙ

Касянчук М.М.[1)], Паздрій І.Р.[2)], Михальчук П.І.[3)], Слободян В.Р.[4)]
Тернопільський національний економічний університет
[1)]к.ф.-м.н., доцент; [2)] к.т.н., доцент; [3)] магістрант; [4)] студент

І. Постановка проблеми

На сучасному етапі, коли цифрові технології вдосконалюються з кожним днем, є актуальним завдання про цілісність і правдивість інформації [1], тому постійно виникають все нові і нові криптографічні методи захисту інформації [2]. Для сучасної криптографії характерне використання алгоритмів шифрування з відкритим ключем [3], що припускають використання обчислювальних засобів. Ще одним видом захисту даних, особливо текстових, є використання хеш-функцій.

Основною задачею, яка вирішується у даній роботі, є виявлення та дослідження усіх можливостей алгоритмів для побудови хеш-функцій. Для реалізації максимально оптимального алгоритму необхідно проаналізувати можливі середовища розробки та виявити найкращі засоби для здійснення шифрування. Також потрібно знайти позитивні сторони даного криптографічного методу і корисні якості, які властиві хеш-функціям.

ІІ. Мета роботи

Метою даної роботи є розробка алгоритмів криптографічного захисту текстової інформації на основі хеш-функцій.

ІІІ. Реалізація алгоритмів криптографічного захисту текстової інформації на основі хеш-функцій

Програма розроблена у середовищі Borland Delphi 7 на мові програмування Delphi і призначена для шифрування інформації з використанням хеш-функцій. Продукт міститиме у собі поле, куди можна ввести вхідні текстові та числові дані. Програма також надаватиме можливість для імпорту даних із завчасно створених файлів. Розроблений продукт дозволяє вибирати один із хеш-алгоритмів, за допомогою якого відбуватиметься перетворення вхідного значення зафіксованої довжини на вихідне значення меншої фіксованої довжини. Знаходиться у програмі інформаційне вікно, де відображається вихідне значення у числовому і текстовому форматі. Продукт дає можливість зберігати зашифровані дані в текстовому файлі. У програмі також є кнопки для початку шифрування, виведення інформації про автора, зберігання перетвореного файлу, довідка і для закінчення програми.

Область застосування розробленого продукту – це захист різних приватних даних користувачів, контроль цілісності даних при їх передачі або зберіганні, розробка програмних компонентів інформаційних систем для криптографічного захисту, а також аутентифікація джерела даних.

Розроблений продукт має виконувати ряд функцій, зокрема: контроль вхідної інформації; організація процедури введення даних для шифрування; генерування криптографічного ключа (ключів) із заданими параметрами (тобто розрахунок хеш-функції); організація процедури для шифрування даних; організація процедури для їх виведення.

Структурна схема включає три основних підсистеми: вводу, шифрування та виводу. Опрацювання введених файлів з розширенням .txt відбувається почергово.

Висновок

У даній роботі представлено, досліджено та програмно реалізовано алгоритми криптографічного захисту текстової інформації на основі хеш-функцій.

Список використаних джерел

1. Andrijchuk V. Modern Algorithms and Methods of the Person Biometric Identification / V.Andrijchuk, I.Kuritnyk, M.Kasyanchuk, M.Karpinski // Proceedings of the Third IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2005) – Sofia, Bulgaria. – 2005. – P.403–406.
2. Kasianchuk M. Rabin's modified method of encryption using various forms of system of residual classes / M.Kasianchuk, I.Yakymenko, I.Pazdriy, A.Melnyk, S.Ivasiev // Proceedings of XIV International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2017)", 21-25 February, 2017, Polyana-Svalyava. – P.222-224.
3. Касянчук М.М. Теорія алгоритмів RSA та Ель-Гамаля в розмежованій системі числення Радемахера – Крестенсона / М.М. Касянчук, І.З. Якименко, О.І. Волинський, І.Р. Пітух // Вісник Хмельницького національного університету. Технічні науки. – 2011. – № 3. – С. 265–273.