УДК 519.72

ВОЗМОЖНЫЕ ВАРИАНТЫ ШИФРОВАНИЯ ТЕКСТОВЫХ ДАННЫХ, АНАЛИЗ И ВЫБОР ОПТИМАЛЬНОГО ТИПА ШИФРОВАНИЯ ТЕКСТОВЫХ ДАННЫХ ДЛЯ ДАЛЬНЕЙШЕЙ РЕАЛИЗАЦИИ

Е. ДЕНИСОВА
(***Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ***)

В статье рассматривается различные варианты шифрования текстовых данных. В ходе анализа был выбран оптимальный вариант шифрования текстовых данных. Проектирование приложения для шифрования и дешифрования текстовых данных модифицированным методом Владимира Сизова Проведены исследования по актуальности разработки данного приложения.

Введение. Люди издавна использовали шифрование − как способ защиты информации. Идея скрыть в тексте тайные значения и сообщения почти так же стара, как и само искусство письма. За века своего существования человечество придумало множество способов хранения тайны.

Основной раздел. Степень изученности методов шифрования достаточно высокая. Каждый год создается множество программ, литературы, посвящённым криптографическим системам. Криптографическая система − семейство преобразований шифра и совокупность ключей. Существуют Симметричные и Асимметричные криптосистемы.

Симметричные криптосистемы (с секретным ключом − SecretKeySystems) − данные криптосистемы построены на основе сохранения в тайне ключа шифрования. Процессы шифровки и расшифровки используют один и тот же ключ. Секретность ключа является постулатом.

Асимметричные криптосистемы (системы открытого шифрования − с открытым ключом PublicKeySystems) − смысл данных криптосистем состоит в том, что для шифровки и расшифровки используются разные преобразования. Одно из них − зашифрование − является абсолютно открытым для всех. Другое-же − расшифрование − остается секретным.

Рассмотрим возможные варианты шифрования текстовых данных:

1. Шифр XOR - это алгоритм шифрования данных с использованием исключительной дизъюнкции. Алгоритм шифрования заключается в «наложении» последовательности случайных чисел на текст, который необходимо зашифровать, Последовательность случайных чисел называется гамма-последовательность, и используется для шифрованный и расшифровки данных;
2. Шифр Цезаря - один из наиболее простых и широко известных алгоритмов шифрования текстовых данных. Алгоритм шифрования Цезаря заключается в замене каждого символа входящего сообщения на символ, который находится на некотором константном расстоянии с правой или левой стороны. Расстояние при этом называют - ключом;
3. Шифр Скитала - шифрование текста при помощи деревянного цилиндра и пергамента, также известен как шифр Древней Спарты. Для шифрования текст используется цилиндр фиксированного диаметра, на который наматывается узкая полоска пергамента. Сообщение записывают вдоль цилиндра, а затем разматывают, в итоге получается зашифрованное сообщение, которое можно расшифровать, применяя цилиндр того же диаметра. При этом диаметр цилиндра выступает в роли ключа шифрования;
4. Квадрат Полиция - метод шифрования текстовых данных с помощью замены символов. Для шифрования используется квадратная таблица, в которую вписаны все буквы шифруемого алфавита. Если букв больше, то можно их совмещать или добавлять ячейки с произвольными знаками.
5. Метод шифрования текста функцией косинуса Владимиром Сизовым предложен впервые в 2005 на международной конфененции Рускрипто. По координатной оси X расставляются компьютерные символы в любом порядке. Каждому символу соответствует свой порядковый номер от 1 до 256. По оси Y расставляем те же самые символы в любом (таком же или другом) порядке. Им также присваивают порядковые номера от 1 до 256. Функция, посимвольно переводит исходный текст в зашифрованный текст.

Исходя из вышеперечисленных вариантов можно сделать вывод, что каждый алгоритм имеет свои плюсы или минусы. Все вышеперечисленные алгоритмы были изучены и запрограммированы, но чтобы добиться надежного шифрования текстовых данных, необходимо привнести новизну в существующие алгоритмы. Таким образом был создан модифицированны метод шифрования Владимира Сизова. Метод был модифицирован произвольной периодической функцией с любым числом секретных ключей и апериодической неограниченной функцие типа обобщенного степенного ряда Фробениуса.

Актуальность разработки модифицированного метода шифрования В. Сизова текстовых данных заключается в возможности использовать для шифрования произвольные периодические и неограниченные непериодические функции.

Основу разрабатываемого приложения составляет возможность шифровать и дешифровать текстовые данные с помощью усовершенствованного метода шифрования В. Сизова. Аналогов подобного приложения найдено не было. Метод усовершенствовать также использованием апериодической неограниченной функцией сприменением более десятка секретных ключей для отдельного шифрования каждого второго, каждого третьего, каждого третьего символа отдельными ключами-это делает метод более защищенным от внешних атак злоумышленников.

Заключение. В ходе данного исследования и анализа были сделаны выводы о выборе оптимального шифрования текстовых данных и обоснование актуальности создания приложения для шифрования данных несколькими ключами с помощью апериодических функций и сложными периодически и функциями.

ЛИТЕРАТУРА

1. Сизов, В.П. Криптографические алгоритмы на остнове тригонометрических функций [Электронный ресурс]. – URL: https://www.ruscrypto.ru/accocuation/archive/rc2005.html. – Дата доступа: 22.09.2019.
2. Каминский, Л.П. Информационные технологии / Л.П. Каминский, В.А. Степанов // Тригонометрическая криптография. – Красноярск : Сибирский федеральный университет, 2005. – С. 38–41. – Дата доступа: 23.09.2018.