УДК 004.021

ПРОЕКТИРОВАНИЕ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА СИСТЕМЫ ДЛЯ СКРЫТИЯ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ГИПЕРБОЛИЧЕСКИХ ФУНКЦИЙ

А.И. СМОЛЯК
(Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ)

Рассматривается проектирование графического интерфейса системы для скрытия информации с использованием гиперболических функций. Проведён анализ степени пригодности контейнера для модификации, моделирование атак и определение устойчивости к ним.

Введение. Необходимость в скрытии информации у человечества появилась очень давно. Вместе с появлением необходимости в скрытии информации, появилась и необходимость в взломе шифров. Так появилась криптология, наука о создании и взломе шифров.

Интерфейс программы должен обладать целым рядом свойств: естественность, согласованность, дружественность, простота, гибкость, эстетическая привлекательность.

Основная часть. Приложение «ExponentLog» представляет собой приложение для скрытия информации. В интерфейсе представлены 3 ключа шифрования, для каждого ключа есть 3 параметра, 2 функции на выбор: гиперболический косинус (1) и гиперболический синус (2).

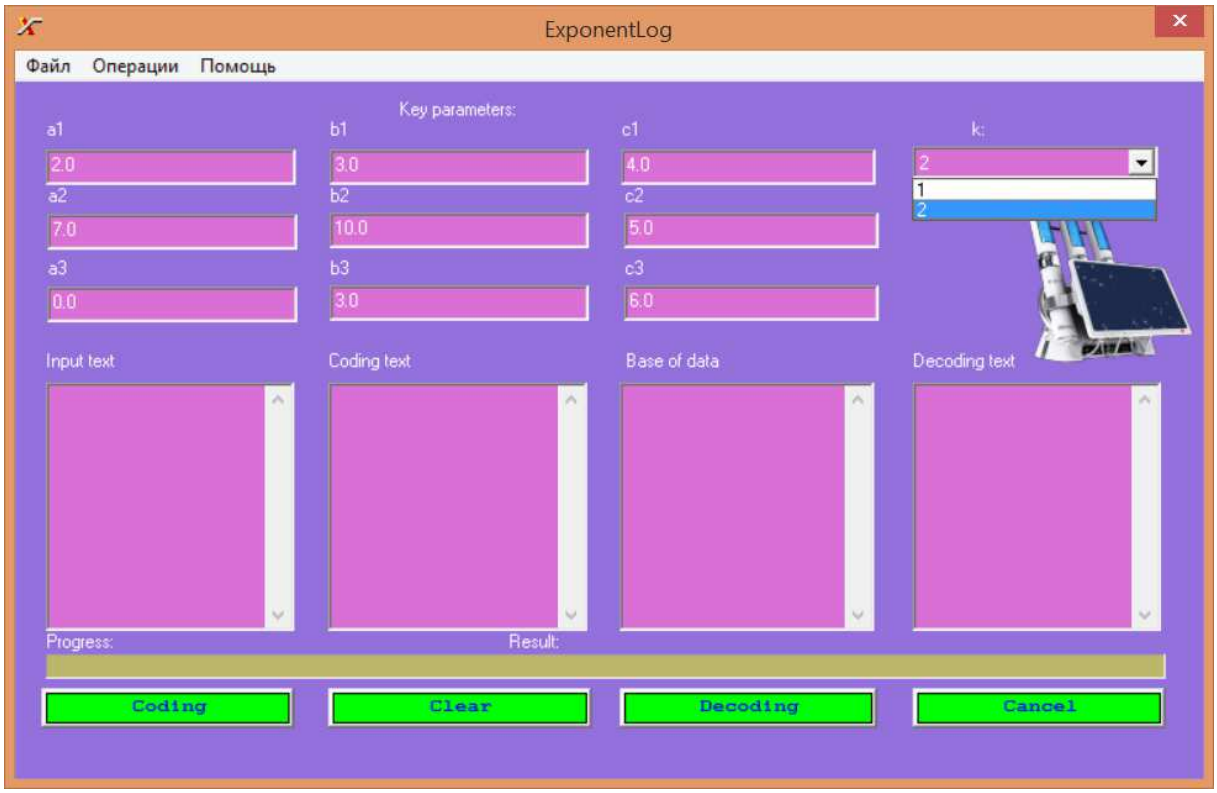

Рисунок 1. – Интерфейс программы

Для скрытия сообщения необходимо будет набрать текст для шифрования в поле Input text, выбрать 9 ключей шифрования и функцию k, нажать кнопку Coding. После нажатия произойдет заполнение строки состояния и текст будет зашифрован.

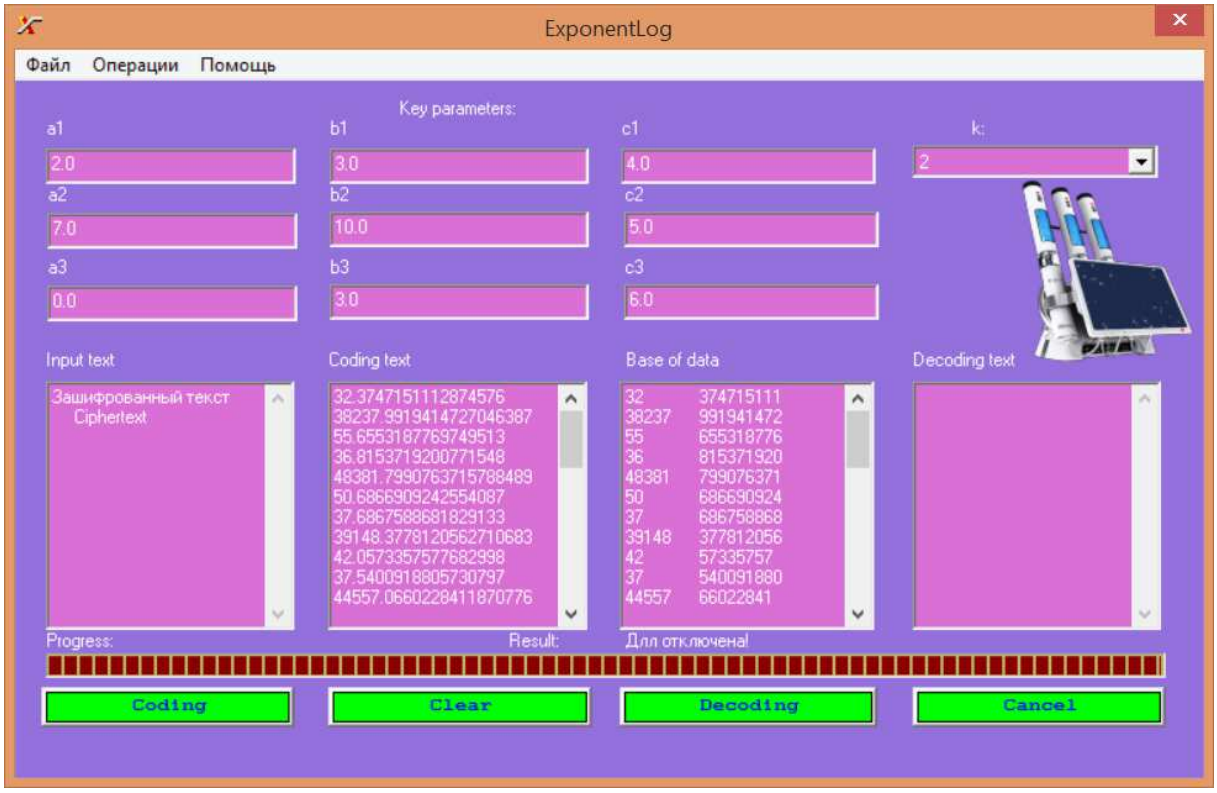

Рисунок 2. – Интерфейс шифрования

При нажатии кнопки Decoding происходит декодирование сообщения.

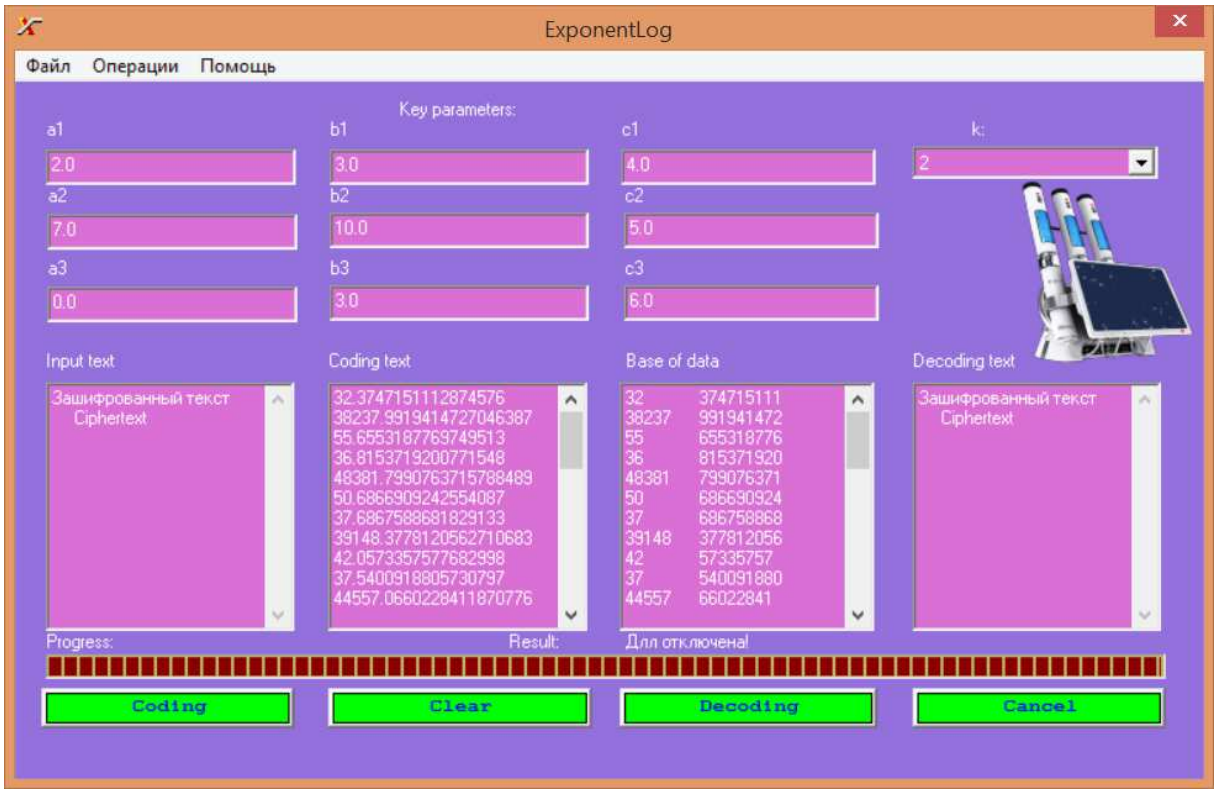

Рисунок 3. – Интерфейс дешифрования

Однако, если изменить хотя бы 1 из 9 ключей, то дешифрованное сообщение будет изменено.

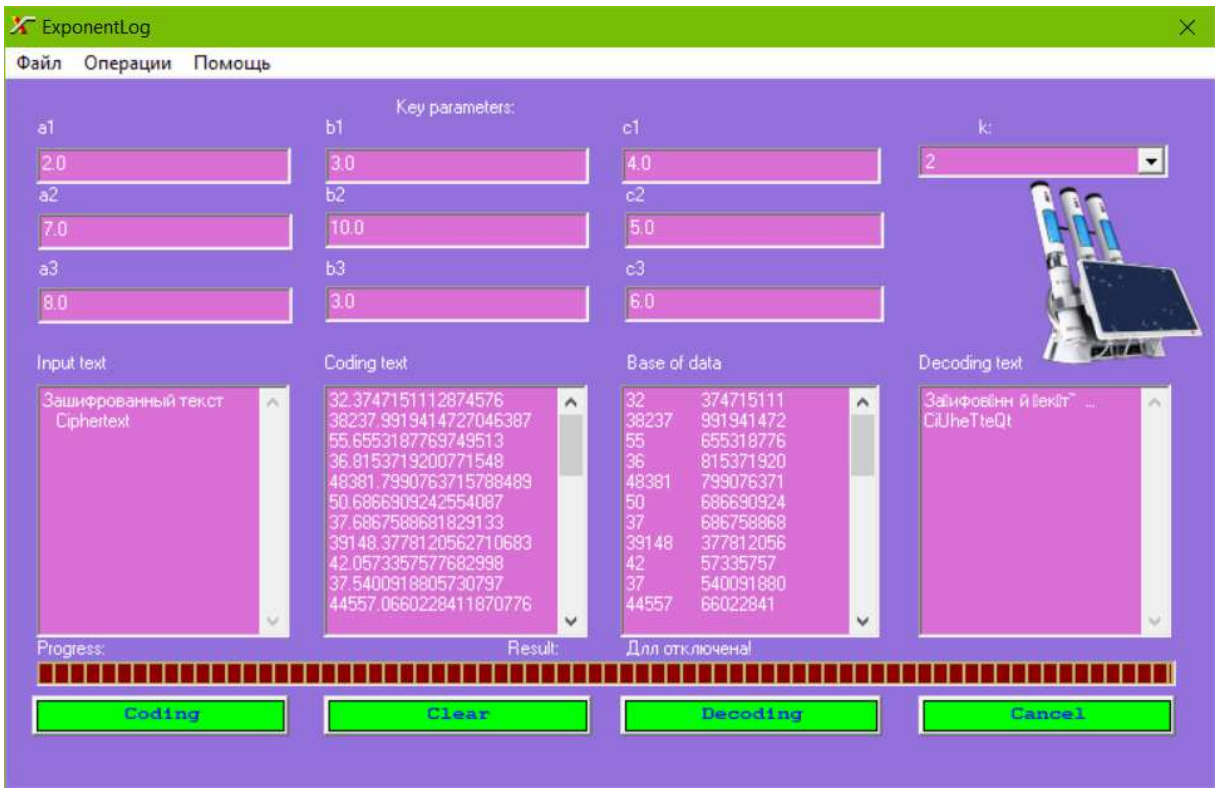

Рисунок 4. – Ошибка в дешифрованном тексте при изменении параметров ключа

Неимоверно большая чувствительность шифра относительно малых 10^{-10} -10^{-12} изменений параметров ключа $(Left, raight, a), (left, raight, n)$, обеспечивает большую размерность пространства распределения ключей. Если бы суперкомпьютер криптоаналитика подбирал ключи к фиксированному шифру нелинейными функциями со скоростью $10^9 \frac{1}{сек}$, то понадобилось бы время взлома, превосходящее время существования Земли (более 5 млрд. лет). Такая большая размерность обеспечивается применением чисел двойной точности (double) для аргументов и нелинейных функций. Действительно, в единичный диапазон изменения параметра одного ключа можно разместить 10^{16} различных шифров. Криптостойкость шифрования нелинейными функциями обеспечивается двумя вескими причинами: большая размерность пространства ключей, большой набор нелинейных функций с «плавающей» областью определения – отрезком, позволяющей с одной стороны увеличить пространство ключей, а с другой стороны повысить криптостойкость шифрования.

В данном приложении применялись 2 класса нелинейных функций: гиперболический синус и гиперболический косинус. Применяемые алгоритмы в программе можно использовать для хранения в базе данных паролей длиной до нескольких сотен – тысяч символов. Добавление алгоритмов рандомизации к шифрованию нелинейными функциями делает применяемые алгоритмы неуязвимыми для криптоаналитика.

Заключение. В данной статье рассмотрен способ построения графического интерфейса системы скрытия информации на основе нелинейных функций, проведён анализ криптостойкости шифрования нелинейными функциями.

ЛИТЕРАТУРА

1. Матюшик, В.Н. Методы и средства стеганографии для защиты графических образов / В.Н. Матюшик. – Минск : Белорус. гос. ун-т информатики и радиоэлектроники.
2. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : Солон-Пресс, 2002.
3. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006.