МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»

Android приложение с блочным шифрованием «Кузнечик»

СТУДЕНТ: КУСТОВ И. А.
НАУЧНЫЙ РУКОВОДИТЕЛЬ: БОРОДИН А.А.

Цель проекта

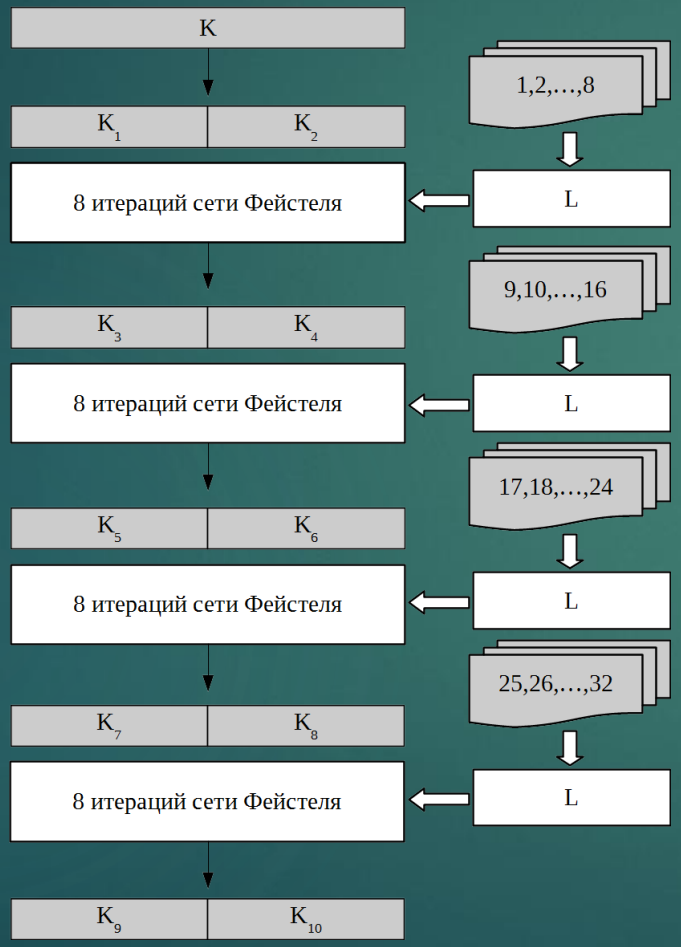
Создание мобильного приложения на платформе Android, реализация блочного шифра «Кузнечик» (ГОСТ Р 34.12-2015), скрытие зашифрованной информации в изображение посредством цифровой стеганографии.

Требования к проекту

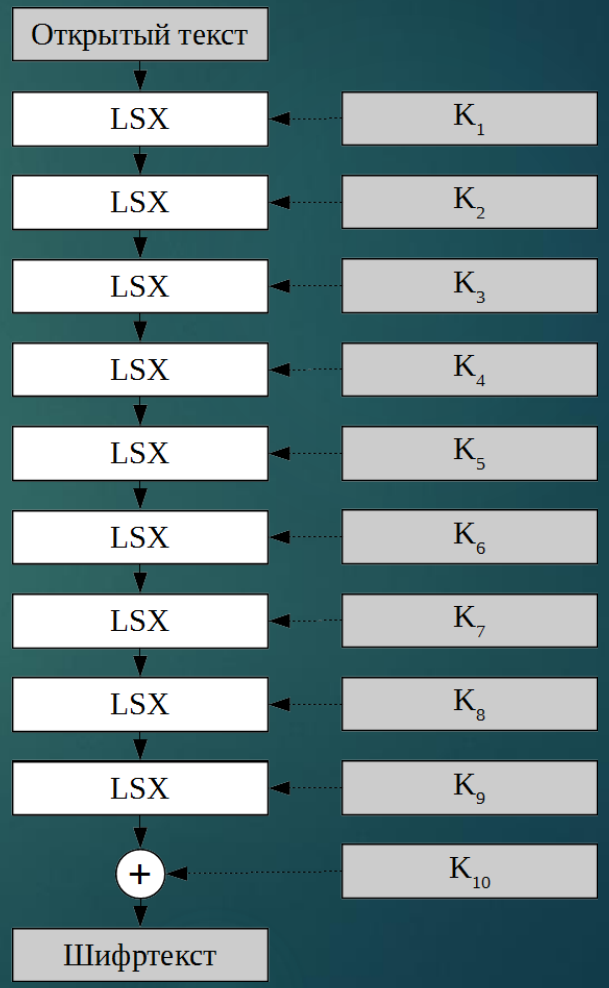
1. Мобильное приложение на платформе Android
2. Шифрование Кузнечиком и занесение данных в контейнер методом LSB
3. Дешифрование стеганоконтейнера и получение информации
4. Возможность изменения/удаления ключа для шифрования
5. Возможность сохранения стеганоконтейнера в формате PNG
6. Возможность копирования текстового результата шифрования/дешифрования в буфер

Блочный шифр «Кузнечик»

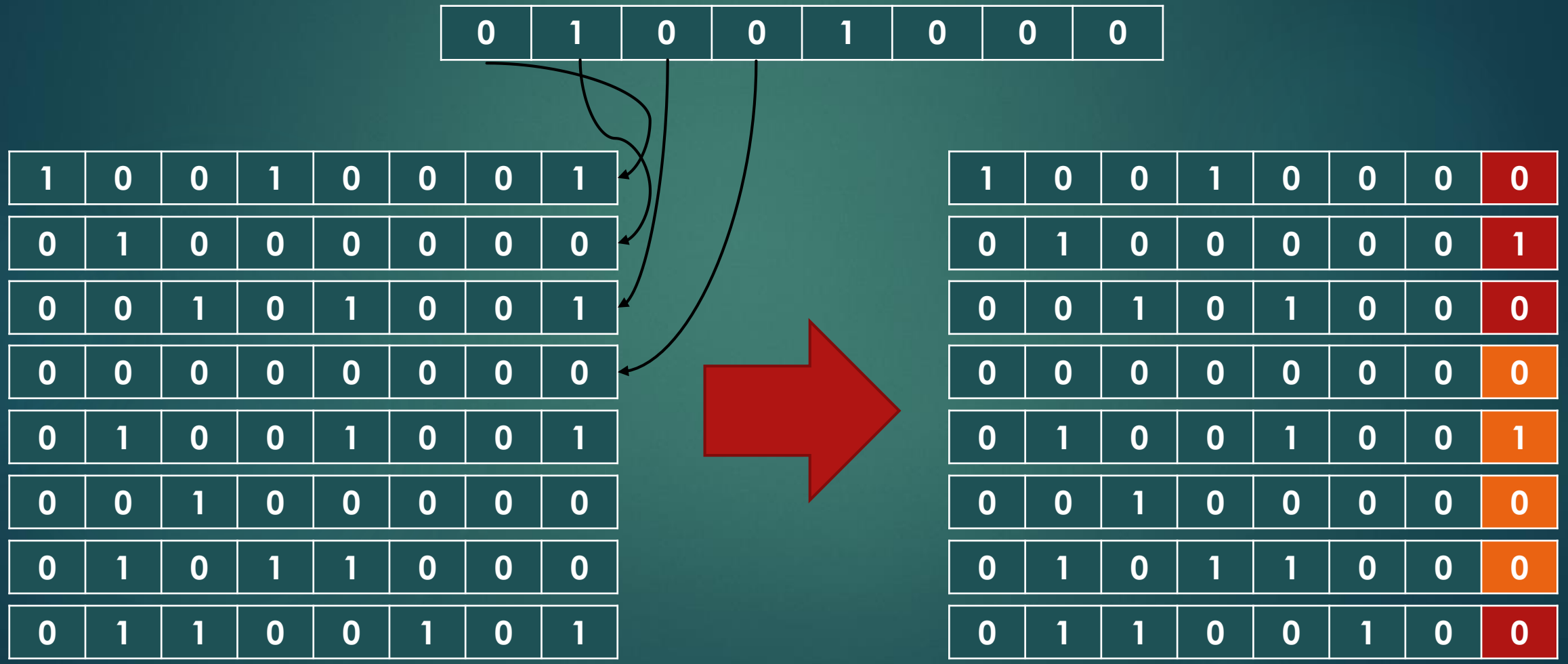
Генерация раундовых ключей



Алгоритм шифрования



Стеногрофирование методом LSB



Работа с мобильным приложением

Диалоговое окно ввода ключа

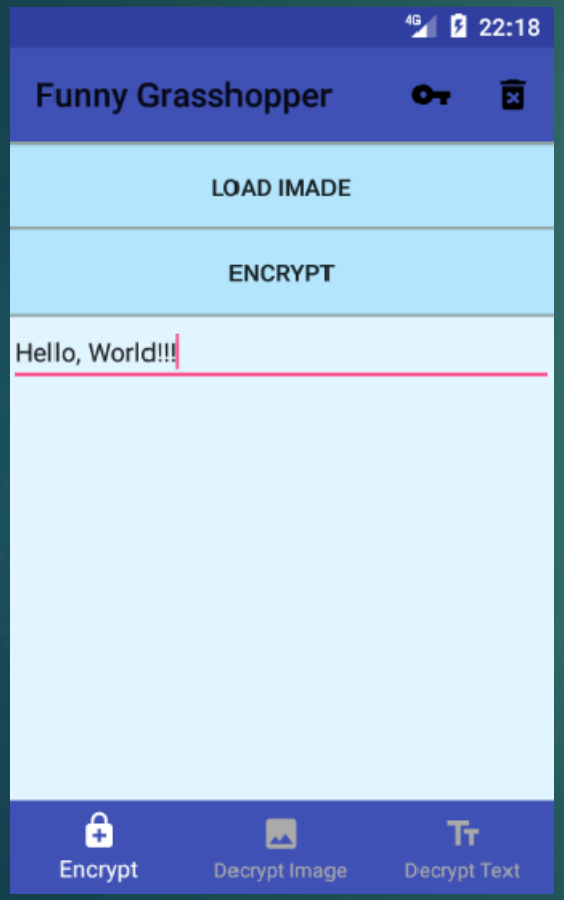
Удаления ключа

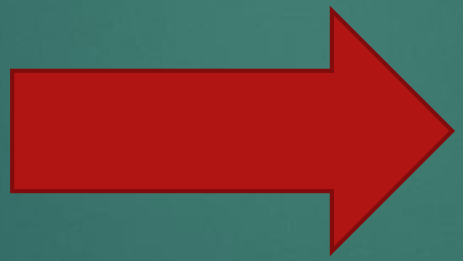
Фрагмент дешифрования текста

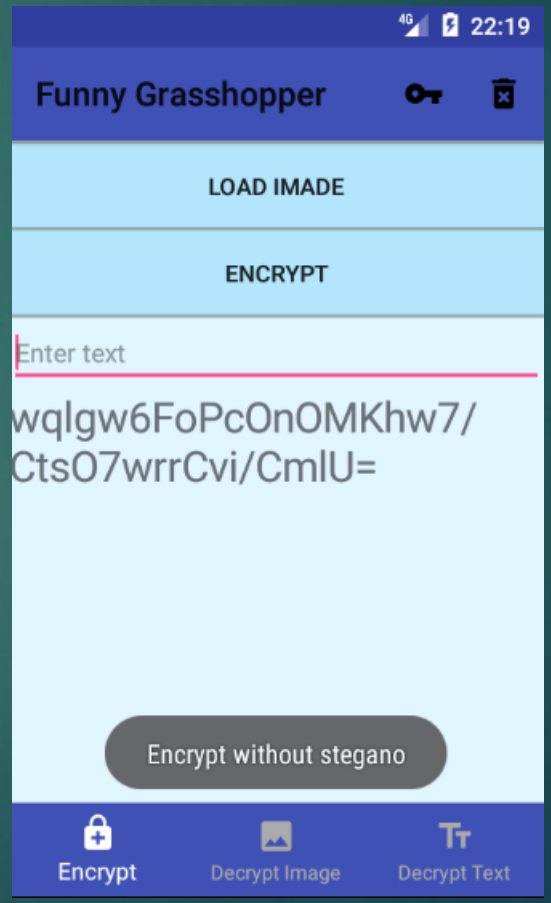
Фрагмент шифрования

Фрагмент дешифрования изображения

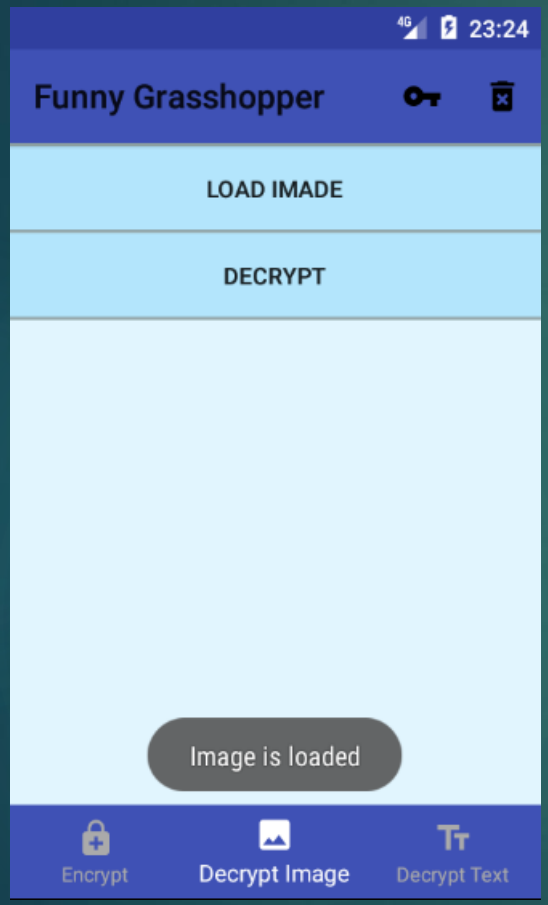
Работа с мобильным приложением: Encrypt

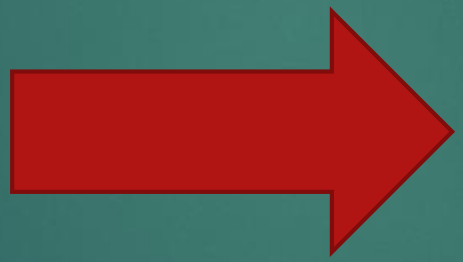


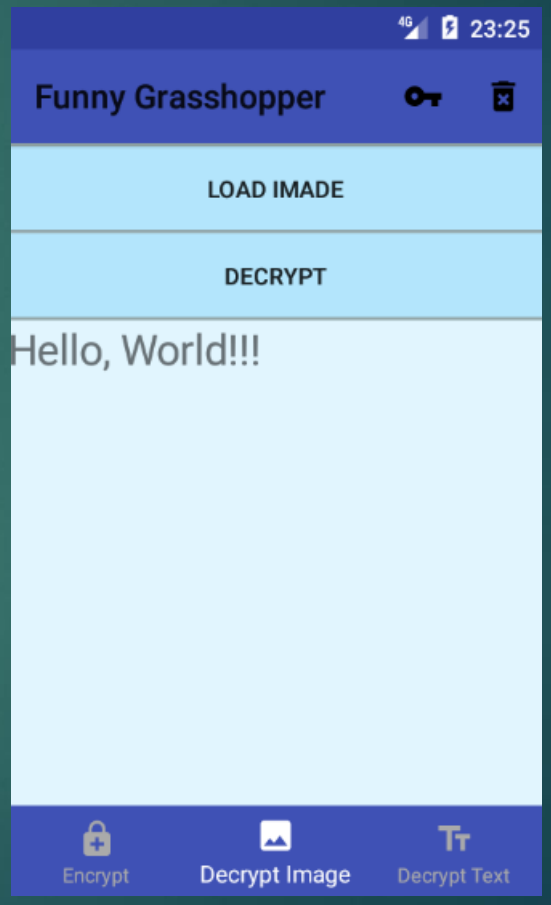




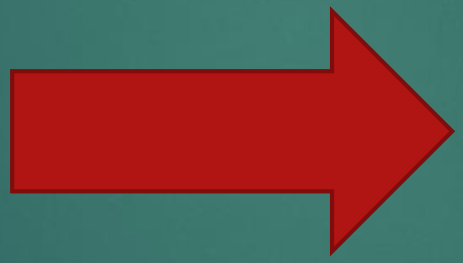
Работа с мобильным приложением: Decrypt Image

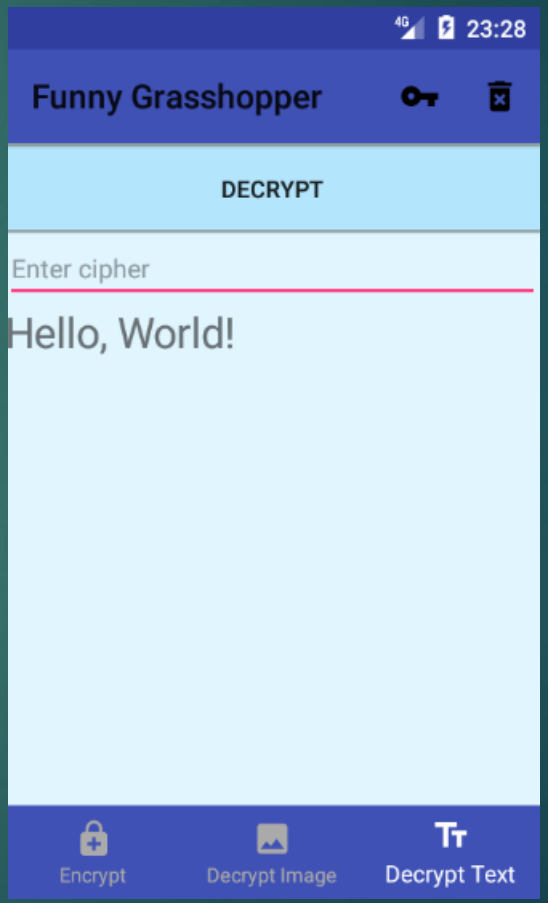






Работа с мобильным приложением: Decrypt Text





Заключение

Было реализовано мобильное приложение для шифрования текстовой информации. Таким образом, приложение предоставляет возможность хранить текст в изображениях, обмениваться ими с другими пользователями, либо шифровать непосредственно в текст. В следующих версиях может быть реализовано:

- Выбор языка платформы и ввода данных
- Переход на стеганографирование в формат JPEG

Спасибо за внимание!