Санкт-Петербургский
государственный
университет
www.spbu.ru

Асимметричное шифрование изображений с разделением ключа

Выпускная квалификационная работа бакалавра

Направление 010300

Фундаментальная информатика и информационные технологии

Выполнил: студент гр. 13.Б13-ПУ

Хохлов Михаил Павлович

Научный руководитель: ассистент Ужегов Н.С

Санкт-Петербург

2018

Введение

“Кто владеет информацией - тот владеет миром.”

Nathan Mayer Rothschild

Цель работы

Разработать решение для групп людей, которые обеспокоены безопасностью общих данных, хранящихся в графическом виде.

Задачи

1. Найти способ шифрования изображений.
2. Изучить механизм защиты ключа шифрования.
3. Реализовать демонстрационное приложение на платформе Android.

Шифрования изображений

Алгоритм шифрования

1. Задаем n — количество чисел в ключе, по которому будем шифровать. ([k1,k2,k3,...kn])
2. Генерируем эти числа, которые будут принимать значения в диапазоне от 0 до 255, и заносим в массив key, размером n.
3. BMP-файл переводим в целочисленный массив srcPixels, каждый элемент которого содержит информацию о цвете соответствующего ему пикселя, т.е. этот массив будет длиной bitmap.height() * bitmap.width()

4. RGB компоненты i-го элемента массива srcPixels меняем следующим образом:

   R = (R + key[i % (key.length - 3)]) % 256

   G = (G + key[i % (key.length - 3) + 1]) % 256

   B = (B + key[i % (key.length - 3) + 2]) % 256

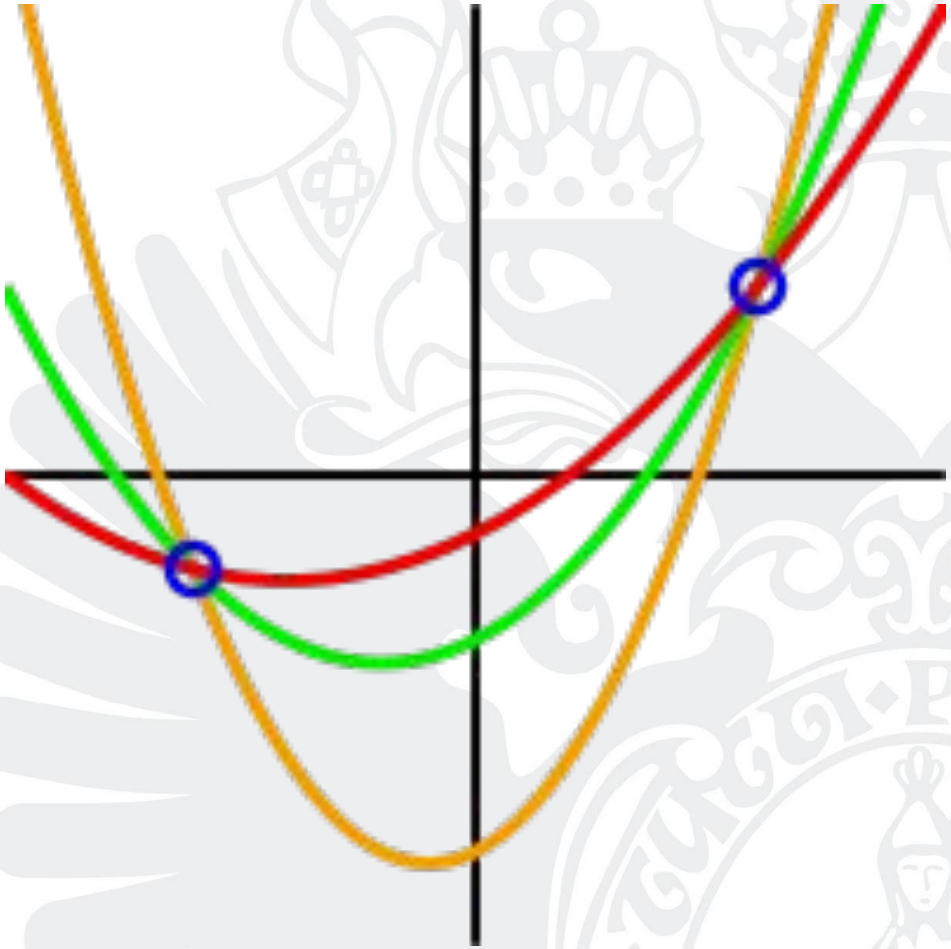
4. Из, уже измененного, массива srcPixels создаем новое изображение, которое и будет являться зашифрованным.
5. Генерируем QR-код, в котором записаны элементы массива key.

Secret Sharing

Одиннадцать ученых работают над секретным проектом. Они хотят запереть документы в шкафу, чтобы кабинет можно было открыть, если и только если присутствуют шесть или более ученых. Какое минимальное количество замков необходимо? Какое минимальное количество ключей для замков, должен носить каждый учёный?

Наша цель состоит в том, чтобы разделить данные D на n кусков D1, ...Dn таким образом, что:

- знание любого k или более Di частей, делает D легко вычислимым;
- знание любого k-1 или меньшего количества частей Di оставляет D полностью неопределенным (в том смысле, что все его возможные значения одинаково вероятны).



Подготовительная фаза

Пусть нужно разделить секрет M между n сторонами таким образом, чтобы любые k участников могли бы восстановить секрет.

$$F(x) = \left(a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x + M\right) \mod p$$

Генерация долей секрета

Теперь вычисляем «тени» — значения построенного выше многочлена, в n различных точках, причём $x \neq 0$

$$
\begin{aligned}
k_1 &= F(1) = \left(a_{k-1} \cdot 1^{k-1} + a_{k-2} \cdot 1^{k-2} + \cdots + a_1 \cdot 1 + M\right) \mod p \\
k_2 &= F(2) = \left(a_{k-1} \cdot 2^{k-1} + a_{k-2} \cdot 2^{k-2} + \cdots + a_1 \cdot 2 + M\right) \mod p \\
&\cdots \\
k_i &= F(i) = \left(a_{k-1} \cdot i^{k-1} + a_{k-2} \cdot i^{k-2} + \cdots + a_1 \cdot i + M\right) \mod p \\
&\cdots \\
k_n &= F(n) = \left(a_{k-1} \cdot n^{k-1} + a_{k-2} \cdot n^{k-2} + \cdots + a_1 \cdot n + M\right) \mod p
\end{aligned}
$$

Восстановление секрета

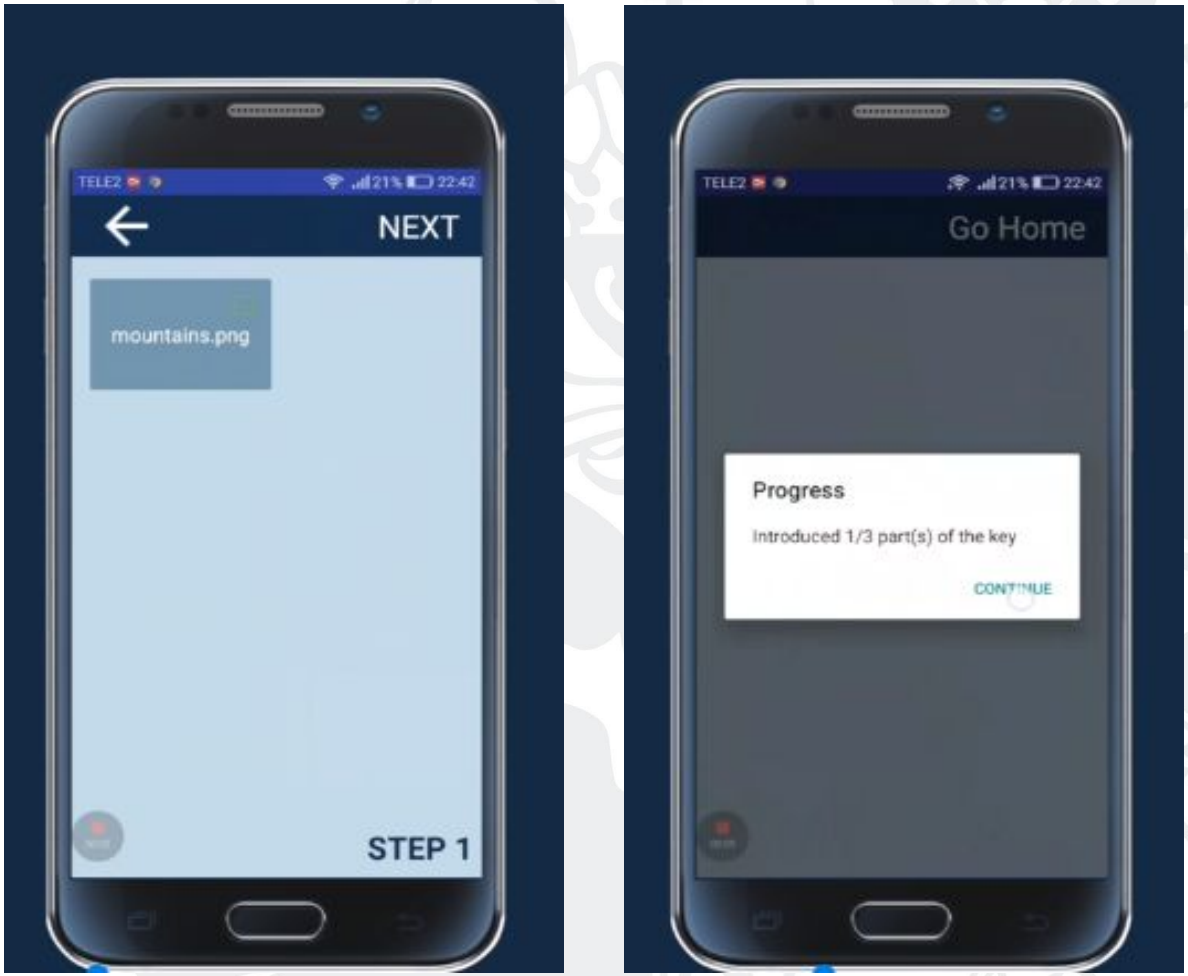
Теперь любые k участников, зная координаты k различных точек многочлена, смогут восстановить многочлен и все его коэффициенты, включая последний из них — разделяемый секрет.

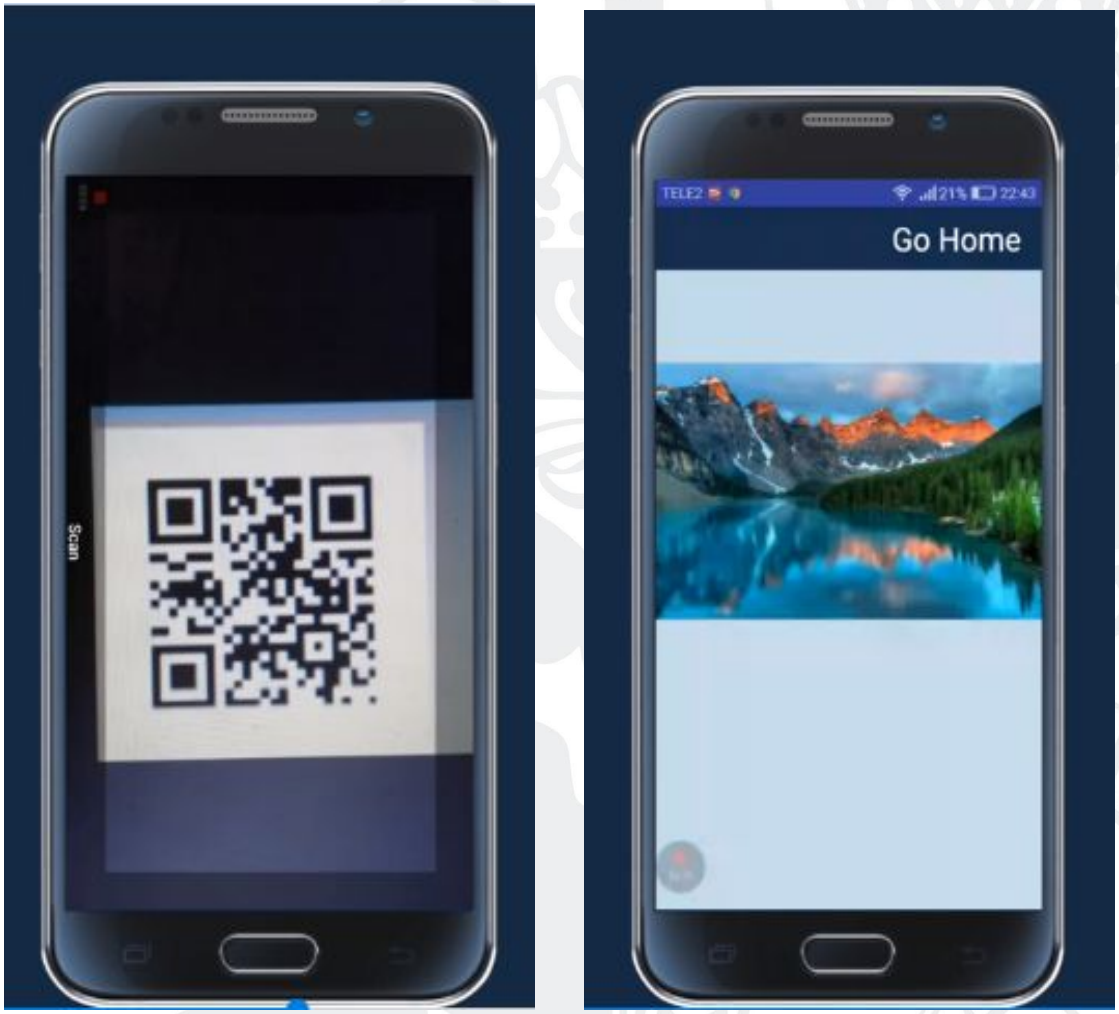
Android приложение


15:33
NEXT
mountains.png
STEP 1


15:33
NEXT
Min: 3
Max: 3
2
2
3
3
4
4
STEP 2


15:33
Go Home
STEP 3
TELE2
21%
22:42
Home
ENCRYPT
DECRYPT


TELE2
21%
22:42
NEXT
mountains.png
STEP 1
TELE2
21%
22:42
Go Home
Progress
Introduced 1/3 part(s) of the key
CONTINUE


scan
TELE2
21%
22:43
Go Home

Заключение

Все поставленные цели и задачи были выполнены:

1. Был разработан способ шифрования изображений
2. Была изучена и применена схема разделения секрета Шамира
3. Было разработано приложение на платформу Android, выполняющее шифрование и дешифрование изображение с разделение секрета.

Дальнейшее направление исследования

- **На данный момент, целью является создания сервиса для хранения изображений, в котором все элементы будут храниться в зашифрованном виде.**
- **Расшифровать данные изображения можно будет только в том случае, если к сервису в данный момент времени подключено определенное количество пользователей, которым предоставлен доступ.**
- **Причем, при подключении меньшего количества людей, изображения невозможно будет расшифровать.**

Благодарю за внимание!