Министерство науки и высшего образования Российской федерации Федеральное государственное бюджетное образовательное учреждение высшего образования

«Курский государственный университет»

Кафедра основы информационной безопасности

ЛАБОРАТОРНАЯ РАБОТА №5

По дисциплине: основы информационной безопасности

Выполнил студентка 2 курса, группы 213.2 факультета физики, математики, информатики

Очной формы обучения

Направление 02.03.03

Математическое обеспечение и администрирование информационных систем

Профиль: Проектирование информационных систем и баз данных

Файтельсон Антон Александрович

Проверил: к.т.н.,

и.о.заведующий кафедрой информационной безопасности Крыжевич Леонид Святославович

Курск, 2024 г.

**Задание 1. Без ключевое кодирование информации. Создание Qr-кодов**

Открыл в сети Интернет сайт Crypt-online, набрав в адресной строке браузера ссылку <http://crypt-online.ru/>. На панели «Преобразования» выбрал раздел «Утилиты» и категорию «Qr-код». В поле текст вписал свою фамилию, имя, отчество и нажал кнопку «Кодировать».

В результате получил изображение Qr-кода с закодированными данными.

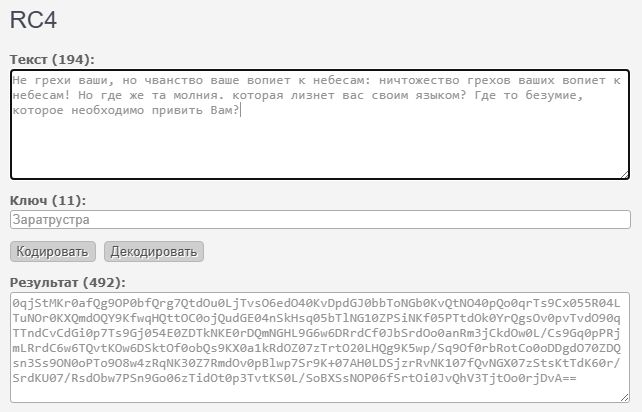


С помощью мобильного приложения на смартфоне считал с данного Qr-кода закодированную информацию.

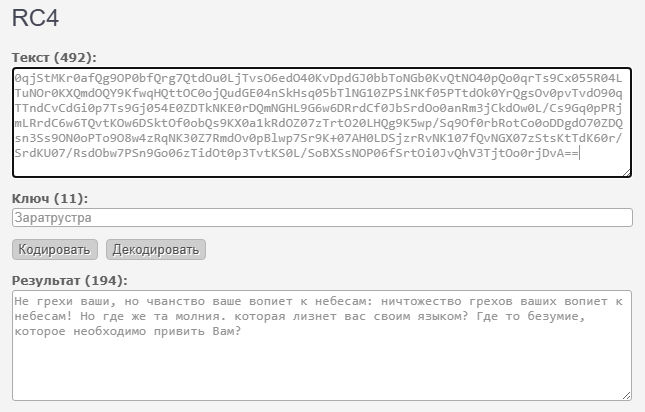
**Задание 2. Симметричное шифрование с помощью ресурса Crypt-online.**

На панели «Преобразование» выбрал раздел «Симметричные» и категорию «RC4». В поле «Текст» вписал секретную фразу, а в поле «Ключ» – секретный пароль и нажал кнопку «Кодировать».

В результате преобразования получил зашифрованное сообщение.



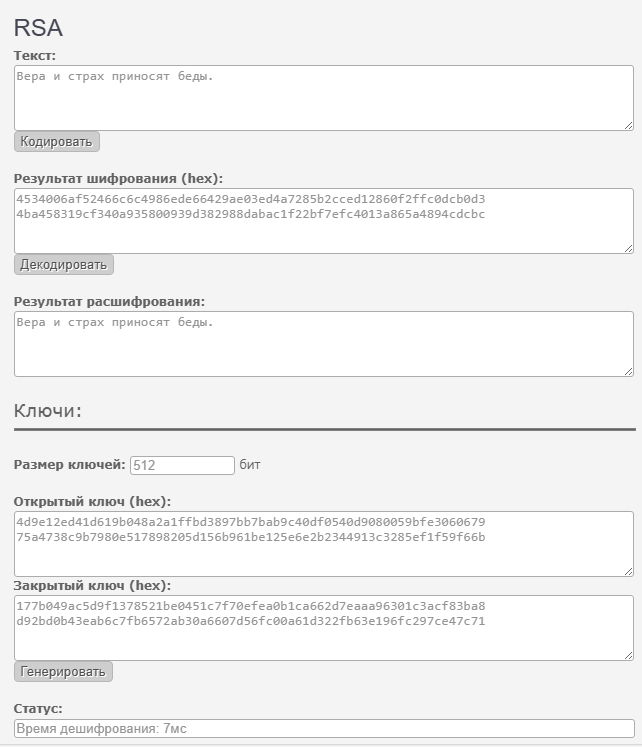
Далее, для проверки обратимости процесса шифрования, скопировал в буфер обмена зашифрованное сообщение, нажал на кнопку «Очистить». В поле текста ввел шифр, полученный до этого, а в строку ключа то же самое парольное слово. Нажал кнопу «Декодировать». Проверила, что в поле сгенерировалось исходное секретное сообщение.



**Задание 4. Ассиметричное шифрование с помощью ресурса Crypt-online.**

На панели «Преобразования» выбрал раздел «Ассиметричные» и категорию «RSA». Сгенерировал пару ключей: открытый и закрытый. Для этого воспользовалась кнопкой «Генерировать» в нижней части панели. В полях «Открытый ключ» и «Закрытый ключ» появились ключи шифрования.

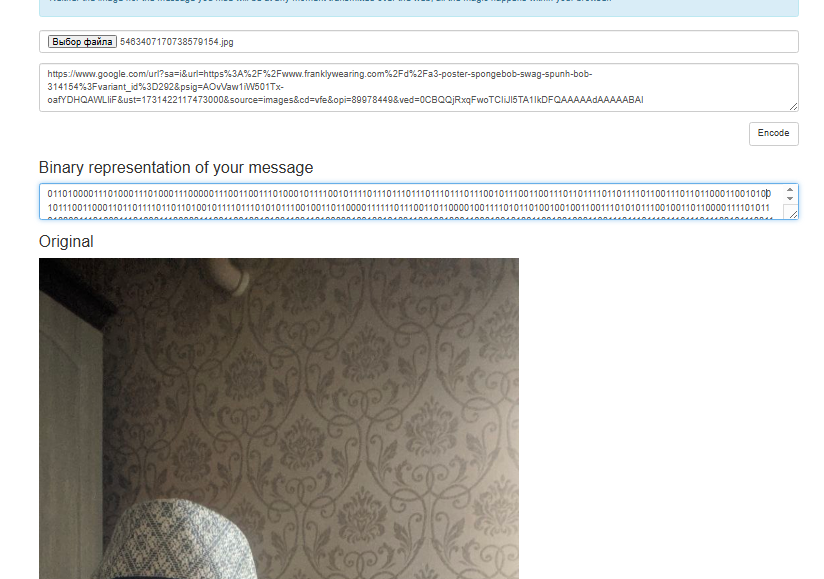
Написал своё секретное сообщение в поле «Текст», затем зашифровал и дешифровал его.

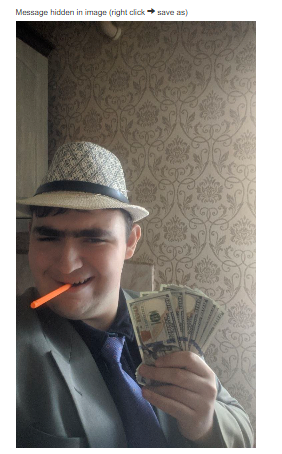
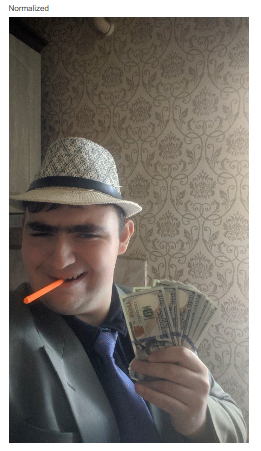


**Задание 6. Скрытие текстовой информации в растровых изображениях.**

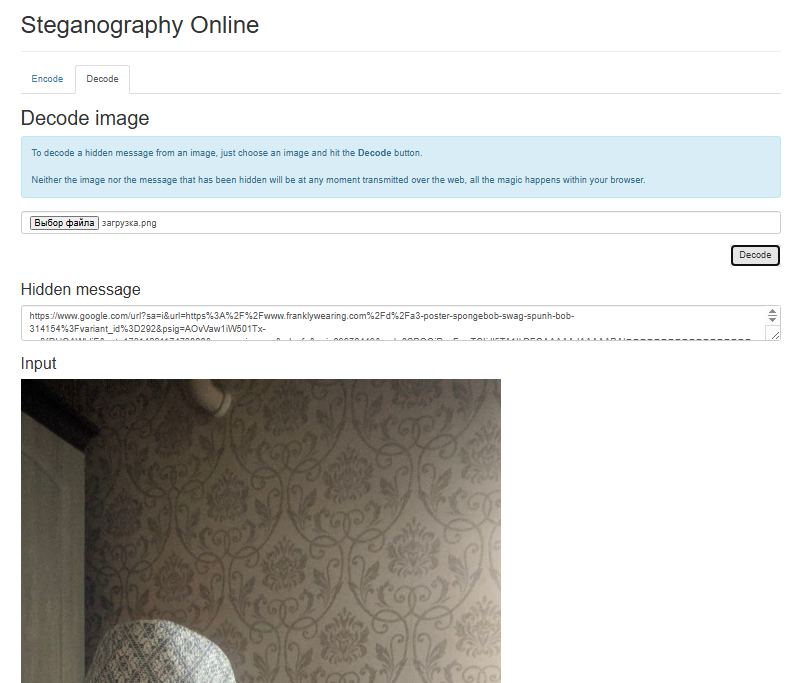
Открыл сайт «Steganography Online» («Онлайн стеганография») перейдя по ссылке <http://stylesuxx.github.io/steganography/>. В разделе «Encode» («Зашифровать») загрузил изображение, нажав кнопку «Обзор» («Выбрать файл»). В поле ниже ввел сообщение, которое необходимо внедрить в изображение. Нажал на кнопку «Encode» («Зашифровать»).

Появилось бинарное разложение текстового сообщения, которое внедрено в изображение. Загруженное изображение вначале нормализовано, а по следующему изображению распределены биты текста. Поэтому на компьютер скачал последнее из них.





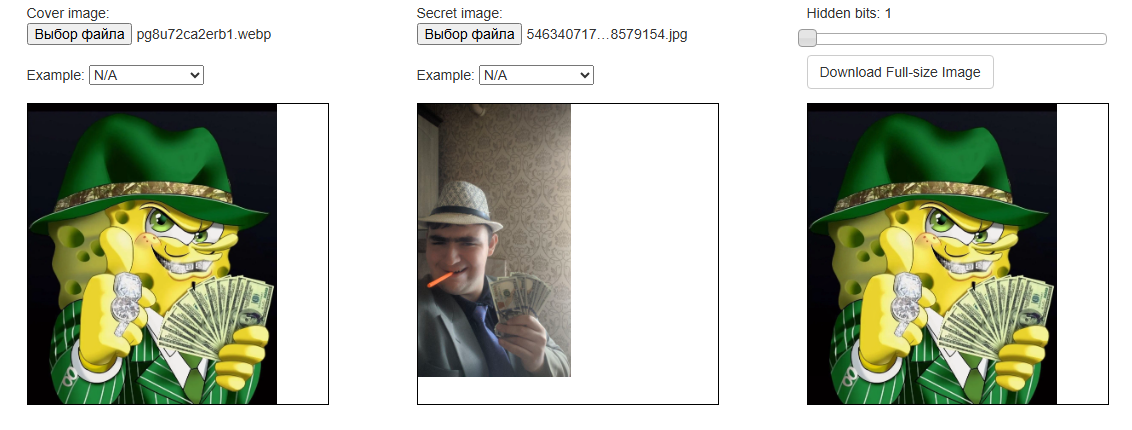
Перешел в раздел «Decode» («Расшифровать») и загрузил последнее скаченное изображение, нажав «Обзор» («Выбрать файл»). Нажал на кнопку «Decode» («Расшифровать»). В окне "Hidden message" («Скрытое сообщение») появилось скрытое сообщение.



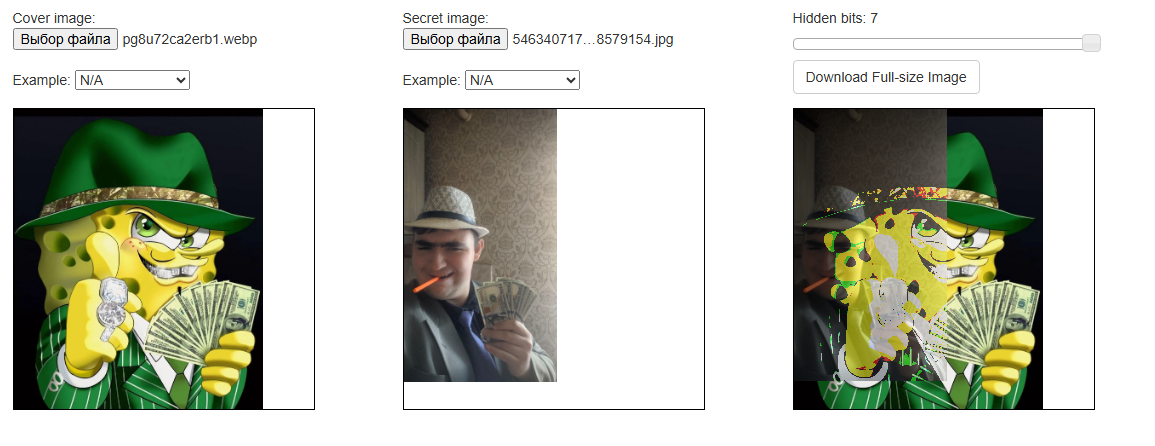
**Задание 8. Скрытие графической информации в растровых изображениях.**

Открыл сайт «Image Steganography» «Графическая стеганография».

В разделе «Hide image» («Скрыть изображение») присутствуют 3 окна: «Cover image» («Изображение-носитель»), «Secret image» («Скрываемое изображение») и «Finish image» («Окончательное изображение»). В первое окно загрузил изображение, которое станет носителем информации. Во второе окно - загрузил изображение, которое необходимо спрятать. После загрузки изображения результат внедрения появился в 3 окне автоматически.

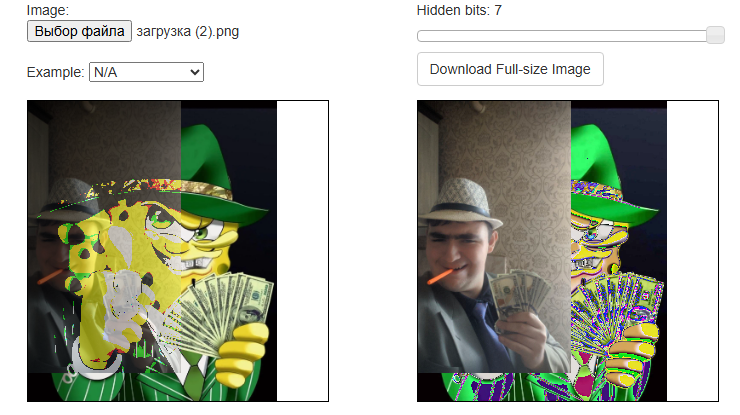


Бегунок «Hidden bits» («Внедряемые биты») открутил до такого правого положения, пока внедрение изображения не перестало быть заметным. После чего нажал кнопку «Download Full-size image» («Загрузить полноразмерное изображение»). Скачал увеличенную картинку на компьютер.



Перешел в раздел «Unhide image» («Показать изображение»). Нажал кнопку «Обзор» («Выберите файл») и загрузил графический файл, полученный на предыдущем этапе.

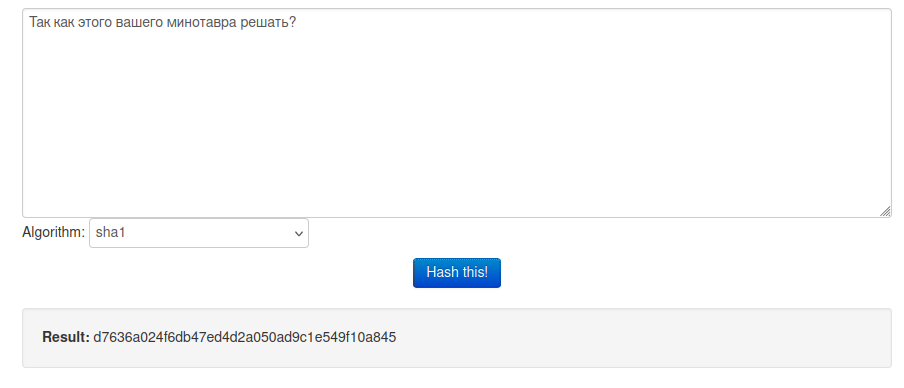
На последнем шаге установил бегунок «Hidden bits» («Внедряемые биты») на уровень, заданный при внедрении, чтобы внедряемое изображение приняло естественный вид.

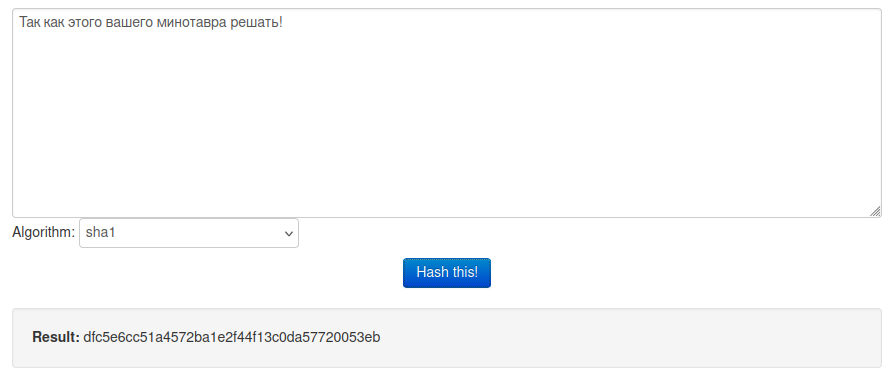


**Задание 10. Хэширование сообщений.**

Открыл сайт «https://www.tools4noobs.com». В открывшемся сайте выбрал категорию «Online hash calculator».

В появившемся окне ввел текст для создания хеш-кода. В качестве алгоритма выбрал sha1. Получил результат. Полученное сообщение является хэш-кодом для проверки оригинальности введенного текста. Скопировал его в отдельный файл.





Если добавить в текст некоторую информацию или изменить исходное сообщение, то изменяется и хэш-код. При этом стоит отметить, что даже при изменении одного символ измениться не один символ хэш-кода, а весь хэш-код в целиком (т.е. каждый символ хэш-кода не совпадет с первичным). Скопировал полученный хэш-код после внесений изменений в текст, в тот же файл, что и первый и сравнил их.