



Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Московский государственный технический университет  
имени Н. Э. Баумана  
(национальный исследовательский университет)»  
(МГТУ им. Н. Э. Баумана)

---

ФАКУЛЬТЕТ «Информатика и системы управления»

---

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

---

## ОТЧЕТ

по лабораторной работе №1  
по курсу «Защита информации»  
на тему: «Моделирование шифровальной машины «Энигма»»

Студент ИУ7-72Б  
(Группа)

Преподаватель

\_\_\_\_\_  
(Подпись, дата)

\_\_\_\_\_  
(Подпись, дата)

Е. О. Карпова  
(И. О. Фамилия)

И. С. Чиж  
(И. О. Фамилия)

2023 г.

# СОДЕРЖАНИЕ

<b>ВВЕДЕНИЕ</b>	<b>3</b>
<b>1 Аналитический раздел</b>	<b>4</b>
1.1 Роторы . . . . .	4
1.2 Рефлектор . . . . .	4
1.3 Коммутационная панель . . . . .	5
<b>2 Конструкторский раздел</b>	<b>6</b>
2.1 Описание использованных типов данных . . . . .	6
2.2 Разработка алгоритмов . . . . .	6
<b>3 Технологический раздел</b>	<b>8</b>
3.1 Реализация алгоритма шифрования . . . . .	8
3.2 Тестирование . . . . .	9
<b>ЗАКЛЮЧЕНИЕ</b>	<b>11</b>
<b>СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ</b>	<b>12</b>
<b>ПРИЛОЖЕНИЕ А Приложение А</b>	<b>13</b>

# ВВЕДЕНИЕ

Криптография — наука о методах обеспечения целостности данных, аутентификации, шифрования. По мере образования информационного общества, криптография становится одним из основных инструментов, обеспечивающих конфиденциальность, доверие, авторизацию, электронные платежи, корпоративную безопасность и бесчисленное множество других важных вещей [1]. «Энигма» является криптографической машиной, которая была создана в 1920-х для военных нужд [2].

Целью данной лабораторной работы является программная реализация аналога шифровальной машины «Энигма» на языке Си.

Для достижения поставленной цели необходимо выполнить следующие задачи.

- 1) изучить алгоритм работы шифровальной машины «Энигма»;
- 2) спроектировать алгоритм работы шифровальной машины «Энигма»;
- 3) реализовать алгоритм работы шифровальной машины «Энигма» на языке Си;
- 4) протестировать реализацию алгоритма работы шифровальной машины «Энигма».

# 1 Аналитический раздел

Машина под названием Enigma, разработанная немцем Артуром Шербиусом для обеспечения безопасности коммерческой информации работает, подавая электрический ток при нажатии любой клавиши. Механические части машины, двигаясь, случайным образом изменяют электрический контур каждый раз при нажатии клавиши, создавая разные буквы. Шифровальная машина «Энигма» состоит из роторов, рефлексора и коммутационной панели [2].

## 1.1 Роторы

Роторы реализуют полиалфавитный алгоритм шифрования, а их определённо выстроенная позиция представляет собой один из основных ключей шифрования. Для Энигмы было разработано восемь различных роторов, и каждый ротор выполнял чётко поставленную задачу в плане коммуникации. Выбор позиций роторов тоже имел значение, образуя свойство некоммутативности. Каждый ротор обладал 26 гранями, где каждая грань представляла собой нумерацию английского алфавита. Выбор одной определённой грани из 26 также представлял собой инициализацию ключа шифрования. Итого, если учитывать все факторы, то количество всевозможных ключей только на основе роторов будет равно  $\left(\frac{5!}{2!}\right) \cdot (26^3) = 1054560$  [3].

## 1.2 Рефлексор

Статичный механизм, позволяющий на одной машине реализовывать как шифрование, так и расшифрование. Представляет собой частный случай моноалфавитного шифра — парного шифра, особенностью которого является инволютивность шифрования. Парный шифр крайне примитивен в своей реализации — необходимо обеспечить связь «1 к 1» для открытого и закрытого символов. Тогда функции шифрования и расшифрования становятся тождественными, и любые 2 равные по сложности их композиции будут давать один и тот же результат.

### 1.3 Коммутационная панель

Динамический механизм, представляет собой также парный шифр. Коммутаторы, можно их рассматривать как некие кабеля, вставляются в коммутационную панель, на которой изображены символы английского алфавита. Один коммутатор имеет два конца, каждый из которых вставляется в два отверстия коммутационной панели. Так, например, если коммутатор был вставлен в два отверстия  $(A, B)$ , то  $A$  и  $B$  становятся парными символами при шифровании. На одну шифровальную машину давалось десять коммутаторов, существовало 26 возможных отверстий в коммутационной панели (количество символов алфавита), один коммутатор одновременно связывал два символа такой панели.

Итого, учитывая все вышеописанные механизмы, а точнее роторы и коммутаторы, можно вычислить количество всех возможных ключей, которое будет равно  $[((5!)/(2!)) \cdot (26)] \cdot [(26!)/(6! \cdot 10! \cdot 210)] = 158962555217826360000$ .

## **2 Конструкторский раздел**

### **2.1 Описание использованных типов данных**

Для реализации алгоритма использованы:

- целое число для размерности алфавита;
- целое число для количества роторов;
- двумерный массив целых чисел для роторов;
- одномерный массив целых чисел для коммутационной панели;
- одномерный массив целых чисел для рефлектора.

### **2.2 Разработка алгоритмов**

На рисунке А.8 представлена схема реализации алгоритма шифрования машины «Энигма».

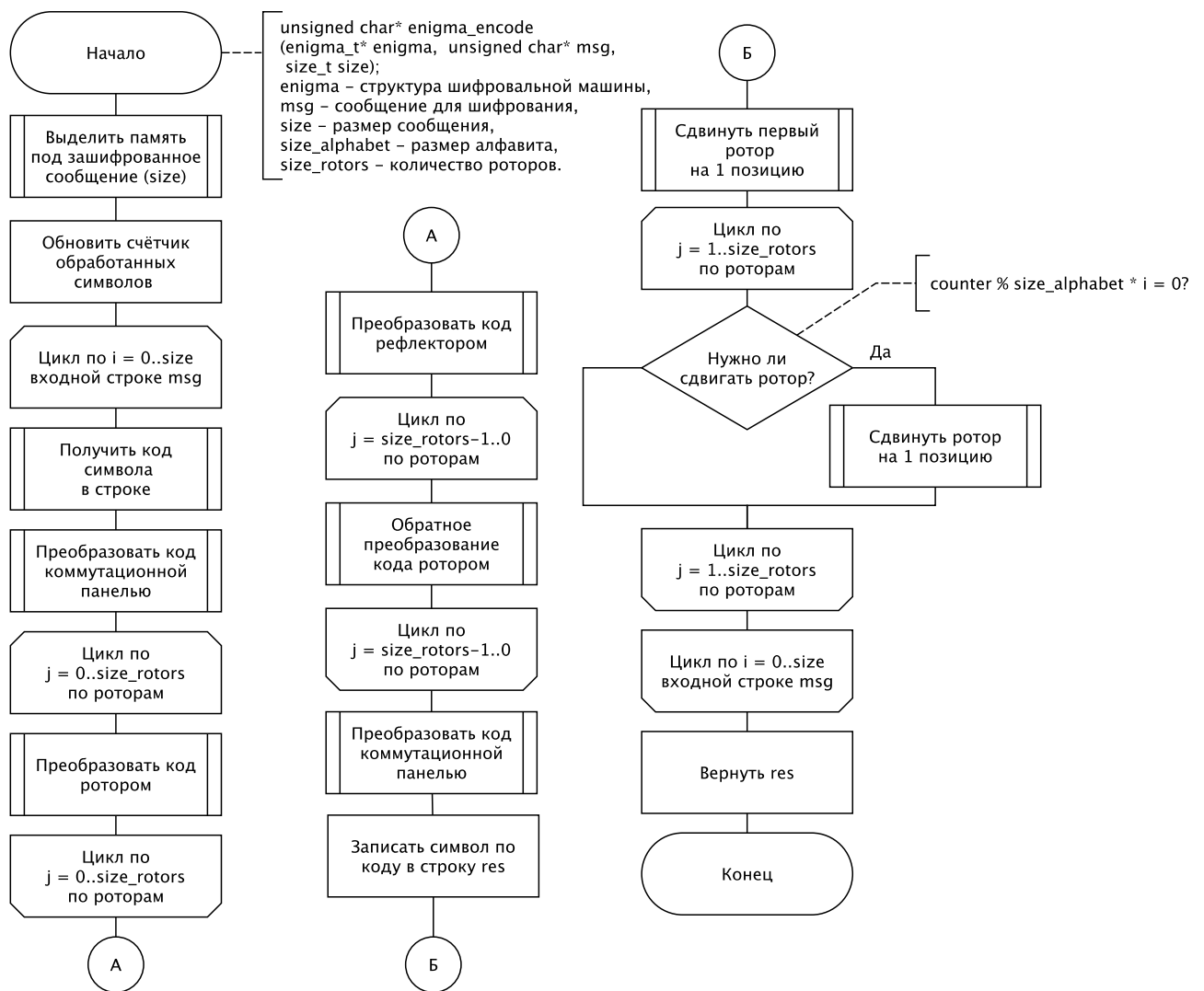


Рисунок 2.1 – Схема реализации алгоритма шифрования машины «Энигма»

## 3 Технологический раздел

### 3.1 Реализация алгоритма шифрования

В листингах 3.1 – 3.2 приведена реализация алгоритма шифрования машины «Энигма».

Листинг 3.1 – Реализация алгоритма шифрования (начало)

```
1 void shift_by_one(int* rotor, size_t size) {
2     int last = rotor[size - 1];
3
4     for (size_t i = size - 1; i >= 1; i--) {
5         rotor[i] = rotor[i - 1];
6     }
7
8     rotor[0] = last;
9 }
10
11 size_t get_index(const int* rotor, size_t size, int val) {
12     for (size_t i = 0; i < size; i++) {
13         if (rotor[i] == val) {
14             return i;
15         }
16     }
17
18     return -1;
19 }
20
21 unsigned char* encode_enigma(enigma_t* enigma, unsigned char* msg,
22     size_t size) {
23     unsigned char* res = calloc(size, sizeof(unsigned char));
24
25     enigma->counter = 1;
26     for (size_t i = 0; i < size; i++, enigma->counter++) {
27         int code = msg[i];
28
29         code = enigma->panel[code];
```



### Листинг 3.2 – Реализация алгоритма шифрования (продолжение 3.1)

```
1
2     for (size_t j = 0; j < enigma->size_rotors; j++) {
3         code = enigma->rotors[j][code];
4     }
5
6     code = enigma->reflector[code];
7
8     for (int j = enigma->size_rotors - 1; j >= 0; j--) {
9         code = get_index(enigma->rotors[j], enigma->size_alphabet
10            , code);
11     }
12
13     code = enigma->panel[code];
14
15     res[i] = code;
16
17     shift_by_one(enigma->rotors[0], enigma->size_alphabet);
18     for (size_t j = 1; j < enigma->size_rotors; j++) {
19         if (enigma->counter % (enigma->size_alphabet * j) == 0) {
20             shift_by_one(enigma->rotors[j], enigma->size_alphabet
21                );
22         }
23     }
24
25     return res;
26 }
```

## 3.2 Тестирование

Корректность алгоритма проверялось путем применения дешифрации на шифрованное сообщение.



Тестирование было проведено на файлах с типами:

- 1) текстовый (txt);
- 2) графический (jpg, png);

- 3) архив (zip);
- 4) исходного кода (с);
- 5) несуществующий (cumberbatch).

В таблице 3.1 представлены тестовые данные.

Таблица 3.1 – Тестовые данные

Номер теста	Тип файла	Содержимое файла
1	txt	зачем это все, если можно просто лечь на спину....7....
2	txt	why do all this if you can just lie on your back....7....
3	txt	Ø
4	zip	Файлы с тестов 1 и 5
5	jpg	
6	с	Файл исходного кода текущей л/р
7	cumberbatch	On Пон, 27 Мар 2023 10:48:02 +0300 Толпинская Наталья Борисовна wrote: Добрый день!Задание на Лаб 7 On Пон, 13 Мар 2023 10:02:34 +0300 Толпинская Наталья Борисовна wrote: Добрый день!Задание на первую часть 6 лаб раб. выполнять надо на занятии! Н.Б. Толпинская
8	png	

## ЗАКЛЮЧЕНИЕ

В результате выполнения данной лабораторной работы поставленная цель достигнута: реализован в виде программы на языке Си аналог шифровальной машины «Энигма».

В ходе выполнения лабораторной работы были выполнены все задачи.

- 1) изучен алгоритм работы шифровальной машины «Энигма»;
- 2) спроектирован алгоритм работы шифровальной машины «Энигма»;
- 3) реализован алгоритм работы шифровальной машины «Энигма» на языке Си;
- 4) протестирована реализация алгоритма работы шифровальной машины «Энигма».

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Точилкин М. В.* Шифрование Энигмой как один из исторических этапов развития криптографии // Студенческая наука: современные реалии. — 2017. — С. 24—26.
2. *Шолин И. М., Чубырь Н. О.* АЛГОРИТМ ПЕРЕНОСНОЙ ШИФРОВАЛЬНОЙ МАШИНЫ ЭНИГМА. // Форум молодых ученых. — 2018.
3. Программная реализация шифровальной машины «Энигма» на языке Си [Электронный ресурс]. — Режим доступа: <https://habr.com/ru/articles/721790/> (дата обращения: 28.09.2023).

# ПРИЛОЖЕНИЕ А

## Приложение А

Примеры работы реализации алгоритма шифрования машиной Enigma.

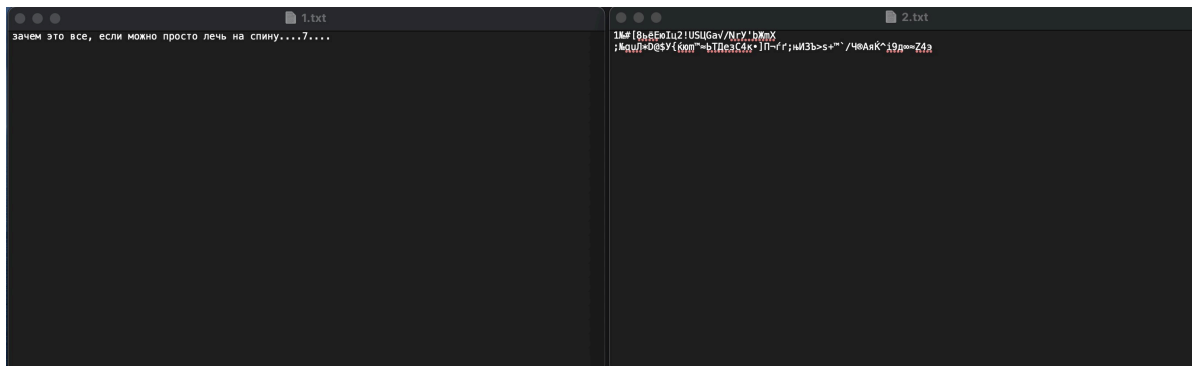


Рисунок А.1 – txt файл на русском

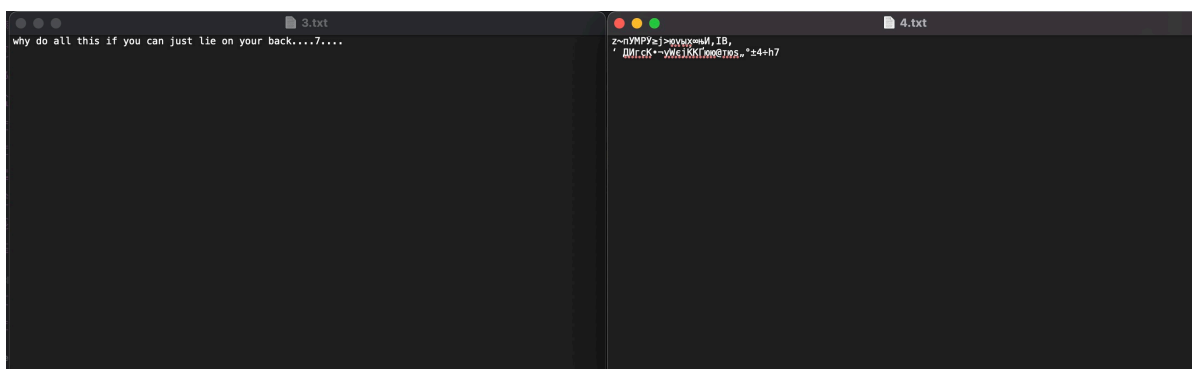


Рисунок А.2 – txt файл на английском

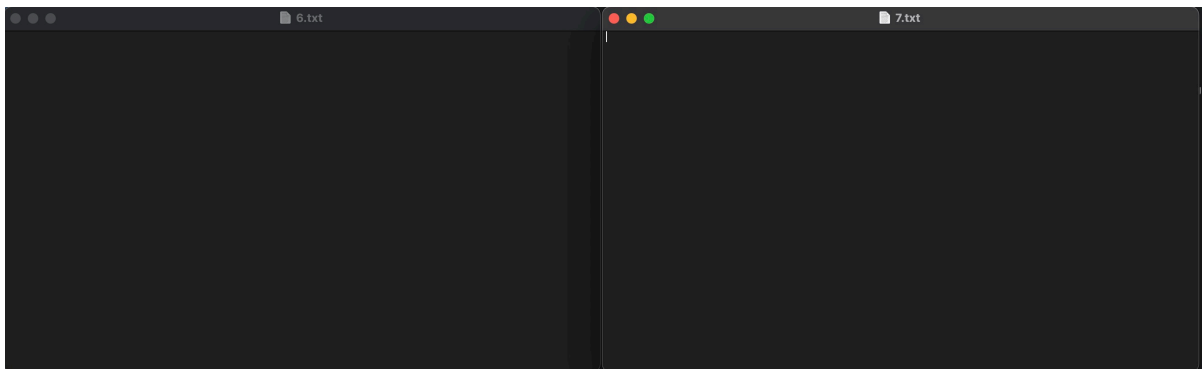


Рисунок А.3 – Пустой файл

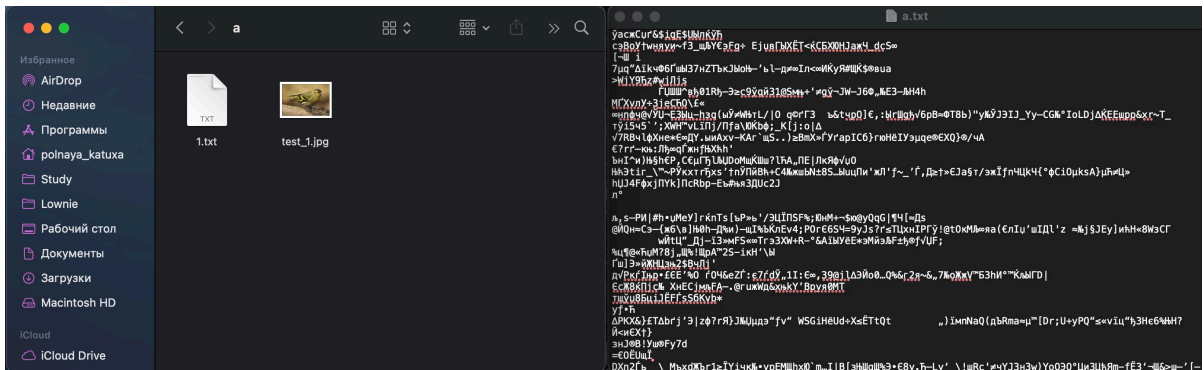


Рисунок А.4 – zip архив с двумя файлами

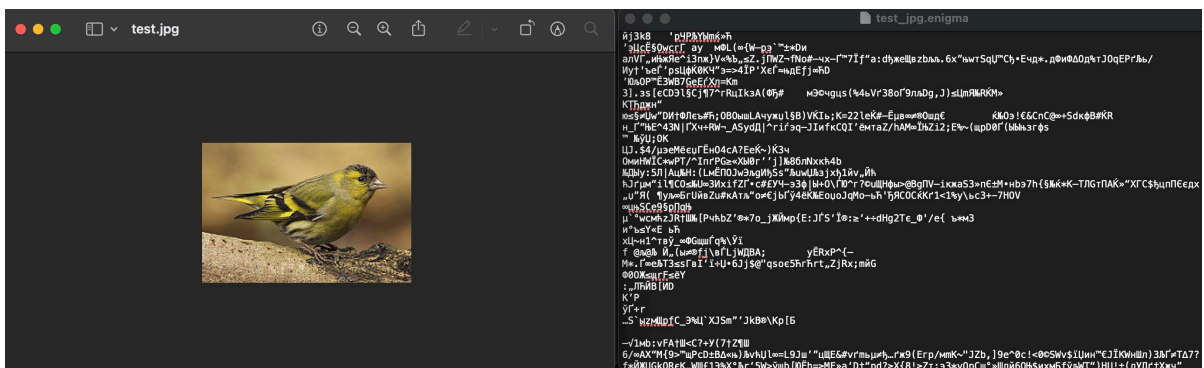


Рисунок А.5 – jpg изображение

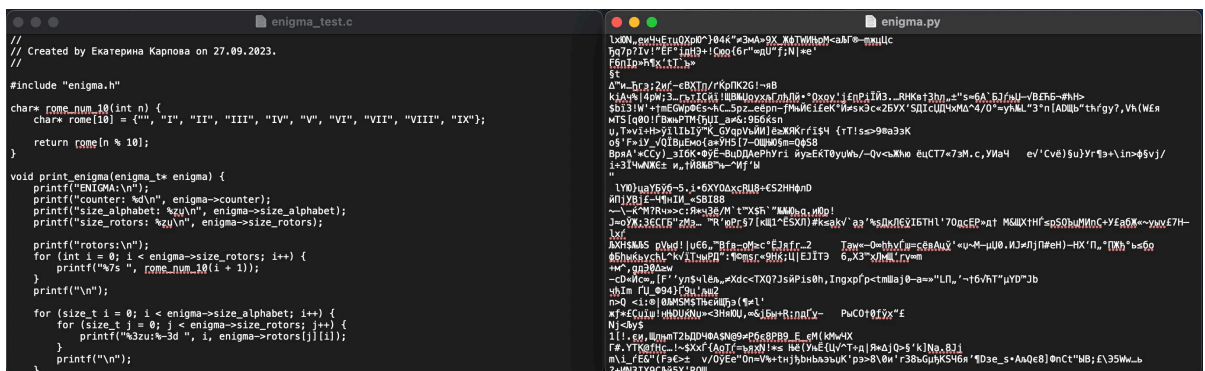


Рисунок А.6 – Файл исходного кода на языке С

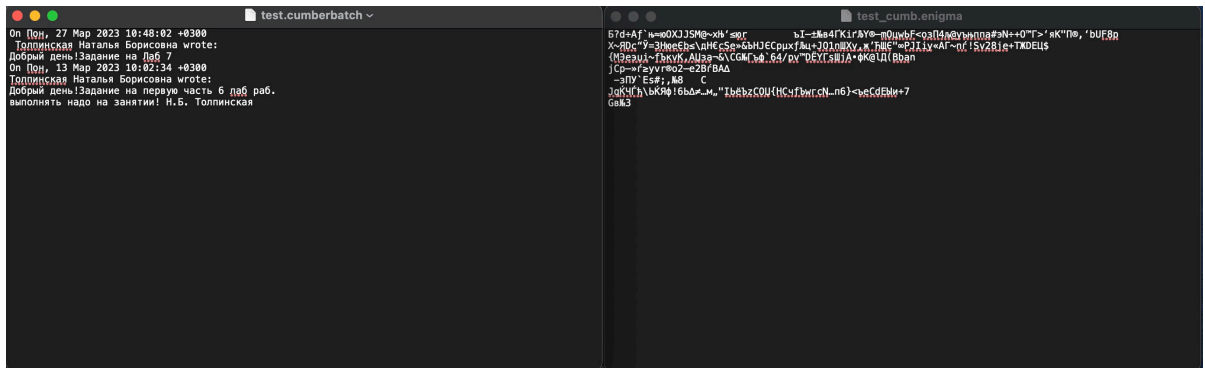


Рисунок А.7 – Файл с выдуманным расширением

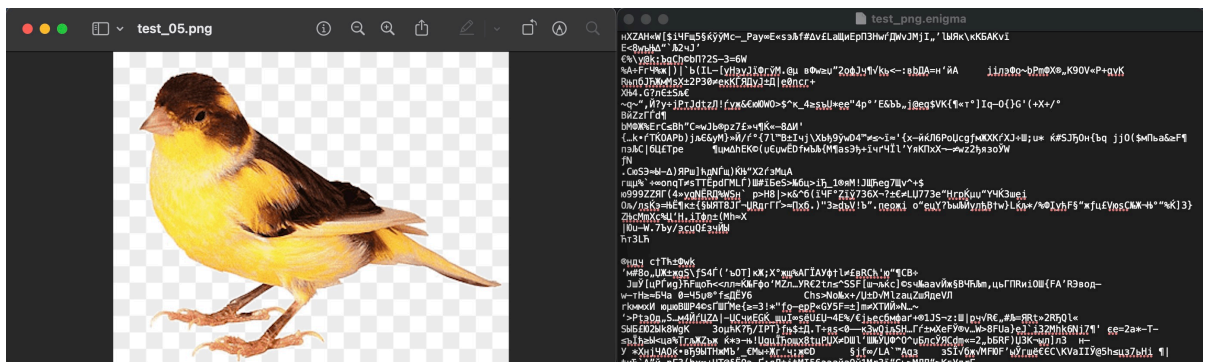


Рисунок А.8 – png изображение