Правительство Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ

О ПРАКТИЧЕСКОЙ РАБОТЕ № 1

по дисциплине «Криптографические методы защиты информации»

Подстановочные Шифры

|  |
| --- |
| Студент гр. 2  Д. О. Рубин  «15» мая 2021 г. |
| Руководитель  Заведующий кафедрой информационной безопасности киберфизических систем  канд. техн. наук, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_О.О. Евсютин  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г. |

Москва 2021

**СОДЕРЖАНИЕ**

[1 Задание на практическую работу 3](#_Toc62605616)

[2 Краткая теоретическая часть 4](#_Toc62605617)

[2.1 Описание шифров 4](#_Toc62605618)

[2.2 Методы криптоанализа шифров 4](#_Toc62605619)

[3 Примеры шифрования 5](#_Toc62605620)

[4 Программная реализация шифров 6](#_Toc62605621)

[5 Примеры криптоанализа 7](#_Toc62605622)

[7 Список использованных источников 9](#_Toc62605623)

# 1 Задание на практическую работу

Целью данной работы является приобретение навыков программной реализации и

криптоанализа применительно к простым подстановочным шифрам.

В рамках практической работы необходимо выполнить следующее:

1) написать программную реализацию следующих шифров:

- шифр простой замены:

- аффинный шифр;

- аффинный рекуррентный шифр;

2) изучить методы криптоанализа моноалфавитных подстановочных шифров с

использованием дополнительных источников;

3) провести криптоанализ данных шифров (с обязательным использованием

частотного метода криптоанализа);

# 2 Краткая теоретическая часть

## 2.1 Описание шифров

Шифр простой замены:

- Алфавит А мощностью m;

- Множество ключей – группа перестановок длины m;

- Открытый текст x = (x1, ... , xl), шифротекст y = (y1, ... , yl);

- Зашифрование открытого текста на ключе k: Ek(x) = (k(x1), ... , k(xl));

- Расшифрование шифротекста: Dk(y) = (k−1(y1), ... , k−1(yl)), k-1 – подстановка, обратная k;

Афинный шифр:

- Алфавит А мощностью m;

- Символы алфавита представляются элементами кольца классов вычетов Zm;

- Ключ – k = (α, β), α ∈ Zm∗, β ∈ Ζm;

- Открытый текст x = (x1, ... , xl), шифротекст y = (y1, ... , yl);

- Зашифрование yi = axi + b, i = 1 .. l;

- Расшифрование xi = (yi — b) \* a^-1;

Афинный рекуррентный шифр:

- Алфавит А мощностью m;

- Символы алфавита представляются элементами кольца классов вычетов Zm;

- Две ключевые пары k1 = (a1, b1), k2 = (a2,b2);

- Открытый текст x = (x1, ... , xl), шифротекст y = (y1, ... , yl);

- Ключевая пара для произвольного символа ki = (a\_(i-2) \* a\_(i-1), b\_(i-1) + b\_(i-2));

- Зашифрование yi = ai \* xi + bi, i = 1 .. l;

- Расшифрование xi = (yi — bi) \* ai^-1;

## 2.2 Методы криптоанализа шифров

Существует несколько видов криптоанализа моноалфавитных шифров:

- Атака грубой силы – перебор взломщиком всех возможных ключей

- Статистическая атака ( Частотный анализ ) – используются статистические характеристики исходного языка для криптоанализа шифра

- Атака по образцу

- Атака знания исходного текста

# 3 Примеры шифрования

Приведём примеры «ручного» шифрования для каждого из описанных шифров:

**3.1 Шифр простой замены**

В качестве алфавита возьмём обычный английский алфавит:

A = «abcdefghijklmnopqrstyuvwxyz», иные символы кодировать не будем. В качестве ключа возьмём K = «4 24 1 11 25 23 15 6 3 21 17 22 16 7 0 2 9 8 12 14 18 13 19 10 5 20», то есть «a» будем заменять на «e», «b» на «y» и т. д.

Пусть исходный текст S = «sentence to encrypt». Шифруем:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S: | s | e | n | t | e | n | c | e |  | t | o |  | e | n | c | r | y | p | t |
| K(S) | m | z | h | o | z | h | b | z |  | o | a |  | z | h | b | i | f | c | o |

Шифротекст Y = «mzhozhbz oa zhbifco».

Теперь расшифруем. Находим перестановку обратную K: K^-1 = «14 2 15 8 0 24 7 13 17 16 23 3 18 21 19 6 12 10 20 22 25 9 11 5 1 4», то есть «e» заменяем на «a» и т. д.

Расшифровываем:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Y | m | z | h | o | z | h | b | z |  | o | a |  | z | h | b | i | f | c | o |
| K^-1(Y) | s | e | n | t | e | n | c | e |  | t | o |  | e | n | c | r | y | p | t |

Дешифрованный текст K^-1(Y) = «sentence to encrypt».

Пусть S = «never say never», K возьмём из предыдущего примера.

Шифруем:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S: | n | e | v | e | r |  | s | a | y |  | n | e | v | e | r |
| K(S) | h | z | n | z | i |  | m | e | f |  | h | z | n | z | i |

**3.2 Афинный шифр**

В качестве алфавита возьмём обычный английский алфавит:

A = «abcdefghijklmnopqrstyuvwxyz», иные символы кодировать не будем. В качестве ключа возьмём K = «7 2». S = «hello».

- `h` = 7; (7 \* 7 + 2) = 25 = `z` - `e` = 4; (7 \*4 + 2) = 4 = `e`

- `l` = 11; (7 \* 11 + 2) = 1 = `b`; - `o` = 14; (7 \* 14 + 2) = 22 = `w`

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S: | h | e | l | l | o |
| K(S) | z | e | b | b | w |

Для дешифровки необходимо найти обратное по модулю 26 к числу 7:

7^(-1) mod 26 = 15 mod 26;

Дешифруем:

- `z` = 25; (25 — 2) \* 15 = 7 = `h` - `e` = 4; (4 — 2) \* 15 = 4 = `e`

- `b` = 1; (1 — 2 ) \* 15 = 11 = `l`; - `w` = 22; (22 -2) \* 15 = `o`;

S = «hello»

**3.3 Афинный рекуррентный шифр**

В качестве алфавита возьмём обычный английский алфавит:

A = «abcdefghijklmnopqrstyuvwxyz», иные символы кодировать не будем. В качестве ключа возьмём K1= «7 2», K2 = «3 4», S = «hello».

- h = 7; (7 \* 7 + 2) = 25 = z; - e = 4; (4 \* 3 + 4) = 16 = q

- K3 = (7 \* 3, 2 + 4) = (21, 6); l = 11; (11 \* 21 + 6) = 3 = d

- K4 = (21 \* 3, 4 + 6) = (11, 10); l = 11; (11 \* 11 + 10) = b

- K5 = (23, 16); o = 14; (14 \* 23 + 16) = a;

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S: | h | e | l | l | o |
| K(S) | z | q | d | b | a |

Дешифруем:

- z = 25; 7 ^ -1 = 15; (25 — 2) \* 15 = 7 = h - q = 16; 3^-1 = 9; (16 — 4) \* 9 = 4 = e

- d = 3; 7 \* 3 ^ -1 = 5; (3 - 6) \* 5 = 11 = l - b = 1; 11^ - 1 = 19; (1 — 10 ) \* 19 = 11 = l;

- a = 0; 23 ^ -1 = 17; (0 — 16 ) \* 17 = 14 = o;

K^-1(Y) = «hello».

# 4 Программная реализация шифров

Реализация: [GitHub](https://github.com/Axer1001/CyberSecurity/tree/main/first_lab)

**4.1 Шифр простой замены**

Input:

S = « sentence to encrypt»

Mode: encrypt

K = « 4 24 1 11 25 23 15 6 3 21 17 22 16 7 0 2 9 8 12 14 18 13 19 10 5 20 »

Output:

«mzhozhbz oa zhbifco»

Input:

S = «mzhozhbz oa zhbifco»

Mode: decrypt

K = «4 24 1 11 25 23 15 6 3 21 17 22 16 7 0 2 9 8 12 14 18 13 19 10 5 20»

Output:

«sentence to encrypt»

**4.2 Афинный шифр**

Input:

S = «hello»

Mode: encrypt

K = «7 2»

Output:

«zebbw»

Input:

S = «zebbw»

Mode: decrypt

K = «7 2»

Output:

«hello»

**4.3 Афинный рекуррентный шифр**

Input:

S = «hello»

Mode: encrypt

K = «7 2 3 4»

Output:

«zqdba»

Input:

S = «zqdba»

Mode: decrypt

K = «7 2 3 4»

Output:

«hello»

# 5 Примеры криптоанализа

Проведём криптоанализ данных шифров методом частотного криптоанализа,

входные данные возьмём из примеров выше.

**5.1 Шифр простой замены**

S = «sentence to encrypt»

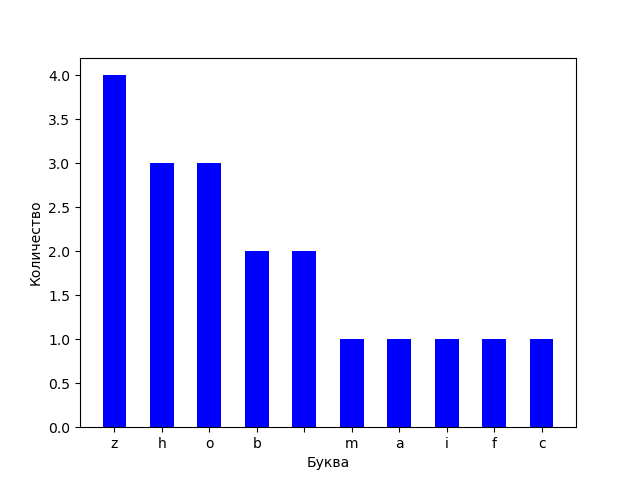
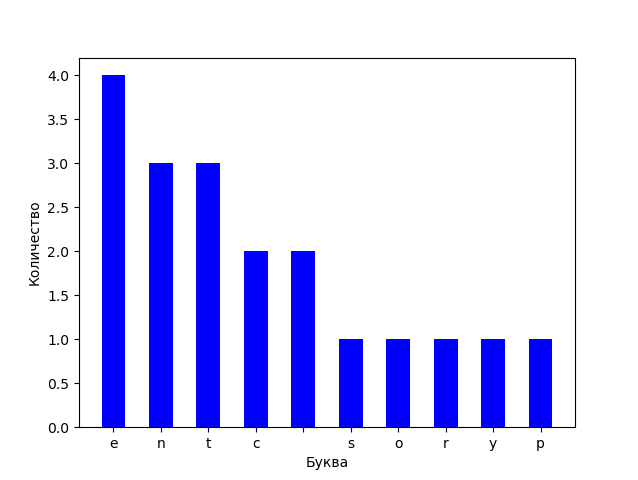


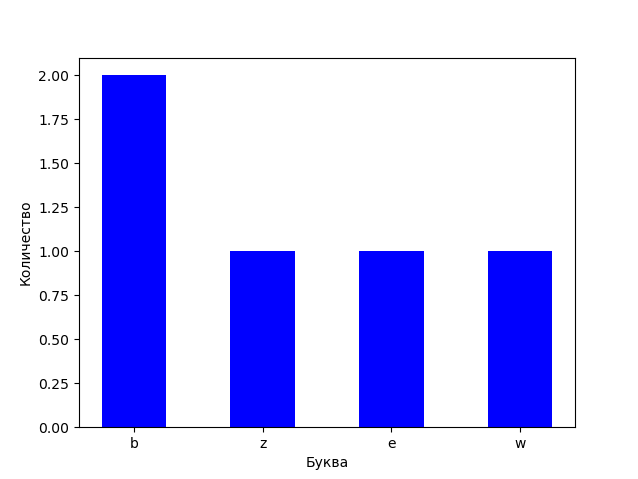
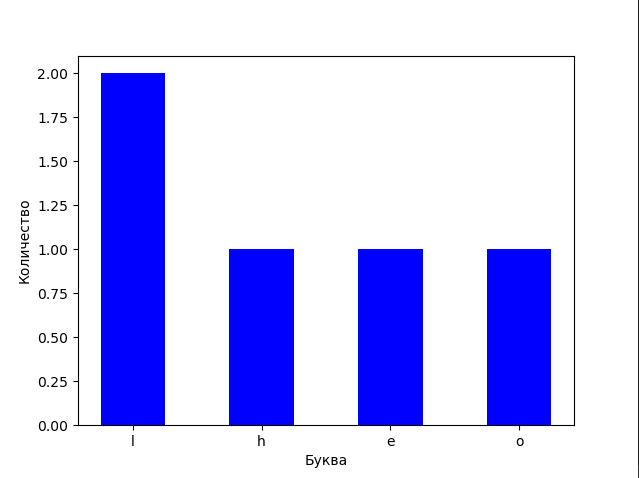
Рисунок 1.1 – исходный текст Рисунок 2.2 – шифротекст

Заметим, что поскольку шифр моноалфавитный по частоте встречаемости буквы в шифротексте можно однозначно определить что это за буква, например:

– `z` встречается в шифротексте 4 раза, а в исходном тексте 4 раза встречается буква `e`, значит `z` кодирует `e` и т.д.

**5.2 Афинный шифр**

S = «hello»

 Рисунок 2.1 – исходный текст Рисунок 2.2 – шифротекст

Аналогично прошлому примеру, буква однозначно определяется по частоте встречаемости:

- `l` – 2 < – > `b` = 2 и т.д.

**5.3 Афинный рекуррентный шифр**

S = «hello»

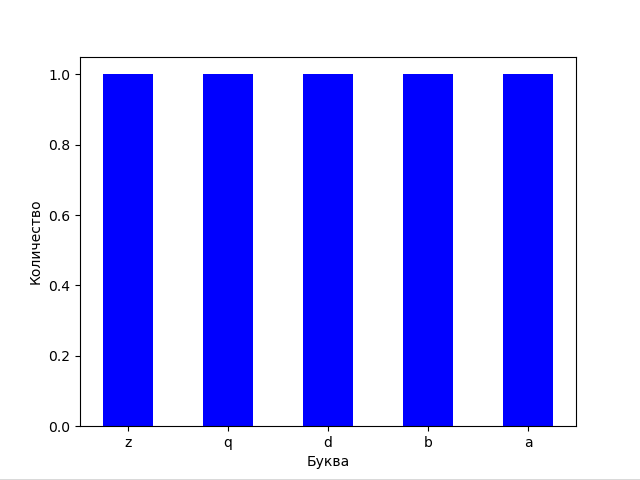
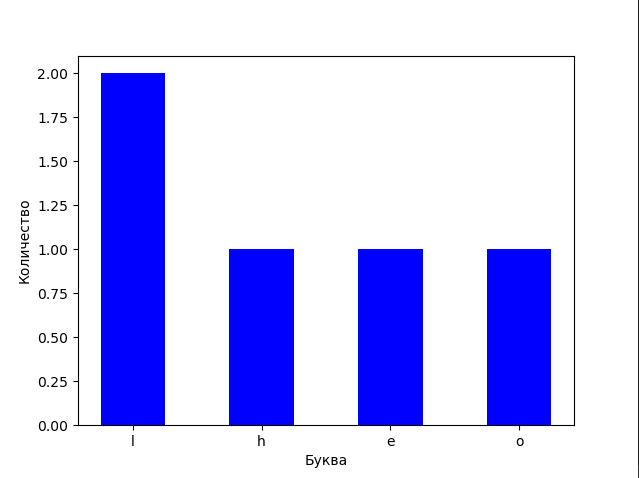


Рисунок 3.1 – исходный текст Рисунок 3.2 – шифротекст

Заметно, что здесь метод частотного криптоанализа уже не сработает, потому что частота встречаемости букв разная.

В этом и состоит преимущество афинного рекуррентного шифра перед афинным и шифром простой замены, и поэтому для афинного рекуррентного шифра применяются другие виды криптоанализа.

**6 Выводы о проделанной работе**

В ходе выполнения данной работы были изучены несколько простых подстановочных шифров, получены навыки программной реализации этих шифров и их криптоанализа. Были изучены несколько методов криптоанализа, в том числе метод частотного криптоанализа, которому уязвимы простые подстановочные шифры. Был изучен Афинный рекуррентный шифр, устойчивый к методу частотного криптоанализа.

# 7 Список использованных источников

1. НОУ Интуит [Электронный ресурс] –

https://intuit.ru/studies/courses/552/408/lecture/9355