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)

[ПРИЛОЖЕНИЕ А. Основные требования к оформлению отчета 10](#_Toc62605624)

[ПРИЛОЖЕНИЕ Б. Пример списка использованных источников 15](#_Toc62605625)

# 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

Особенности программной реализации и примеры работы программы.

# 5 Примеры криптоанализа

Примеры криптоанализа исследуемых шифров с помощью методов, описанных в подразделе 2.2.

**6 Выводы о проделанной работе**

Краткие выводы о проделанной работе: достоинства и недостатки исследуемых шифров, ограничения выбранных методов криптоанализа, наиболее эффективные сценарии криптоанализа.

# 7 Список использованных источников

Список библиографических ссылок, оформленных по ГОСТ (примеры приведены в приложении А).

# ПРИЛОЖЕНИЕ А. Основные требования к оформлению отчета

**А.1 Общие требования к оформлению отчета**

Шрифт: единый, рекомендуемый – Times New Roman,

Цвет: черный,

Размер: не менее 12 пт., одинаковый по всему отчету,

Выравнивание текста – по ширине,

Межстрочный интервал – полуторный (исключения: оформление титула, должностей в списке исполнителей, названий рисунков и таблиц),

Абзацный отступ – 1,25 см.,

Отступы и интервалы в тексте – 0 см.

Полужирный шрифт**:** применяют только для заголовков структурных элементов отчета,для заголовков разделов и подразделов основной части отчета.

Курсив:допускается для обозначения объектов и написания терминов. Курсив также может использоваться для *акцентирования внимания, выделения текста в отчете*, но при этом текст должен быть *того же кегля и гарнитуры*. Разрешается для написания определенных терминов, формул, теорем применять шрифты разной гарнитуры.

Размеры полей:левое – 3,0 см., правое – 1,5 см., верхнее и нижнее – 2,0 см.

Номера страниц– арабскими цифрами, *внизу по центру***.** Титульный листвключают в общую нумерацию страниц отчета. *Номер* страницы на титульном листе *не проставляют*. *Приложения* должны иметь общую с остальной частью отчета сквозную нумерацию страниц.

Оформление перечислений**:** перед каждым элементом перечисления следует ставить *тире* или, при необходимости ссылки в тексте отчета на один из элементов перечисления, вместо тире ставят *строчные буквы,*  начиная с буквы "а" (за исключением – е, з, й, о, ч, ъ, ы, ь), после которой ставится скобка. Простые перечисления отделяются запятой, сложные – точкой с запятой.

*НЕ*допускается использование *данных**знаков*:



При наличии конкретного числа перечислений допускается использовать *арабские*

*цифры* со скобками.

Перечисления приводятся с абзацного отступа – 1,25 пт., без отступов слева и выступов справа.

**А.2 Оформление иллюстраций**

К иллюстрациям относятся: чертежи, графики, схемы, диаграммы, фотоснимки.

Иллюстрации следует располагать в отчете *непосредственно после текста отчета*, где они упоминаются впервые, или на следующей странице (по возможности ближе к соответствующим частям текста отчета).

На все иллюстрации в отчете должны быть даны ссылки. При ссылке необходимо писать слово "рисунок" и его номер, например: "в соответствии с рисунком 2". *Не допускается*сокращение типа *Рис.5.*

Иллюстрации, за исключением иллюстраций, приведенных в приложениях, следует нумеровать арабскими цифрами сквозной нумерацией: Рисунок 1.

Допускается нумеровать иллюстрации в пределах раздела отчета. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой: Рисунок 1.1.

Если рисунок в отчете всего один, то он обозначатся: Рисунок 1.

Иллюстрации при необходимости могут иметь наименование и пояснительные данные (подрисуночный текст). Слово "Рисунок", его номер и через тире наименование помещают после пояснительных данных и располагают в центре под рисунком.

Пример оформления названия рисунка:

Рисунок 1.1 – Если наименование рисунка состоит из нескольких строк, то его записывают через один межстрочный интервал. Наименование рисунка приводят с прописной буквы без точки в конце. Перенос слов в наименовании рисунка не допускается

**А.3 Оформление таблиц**

Таблицу следует располагать непосредственно после текста, в котором она упоминается впервые, или на следующей странице.

На все таблицы в отчете должны быть ссылки. При ссылке следует печатать слово "таблица" с указанием ее номера***.*** *Не допускается сокращение – Табл*.5.

Допускается применять размер шрифта в таблице меньший, чем в тексте отчета.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Допускается нумеровать таблицы в пределах раздела при большом объеме отчета. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенных точкой: Таблица 2.3.

Наименование таблицы следует помещать над таблицей слева без абзацного отступа в одну строку с ее номером через тире, например,Таблица 1 – Наименование. Наименование таблицы приводят с прописной буквы без точки в конце. Если наименование таблицы занимает две строки и более, то его следует записывать через *один межстрочный интервал*.

Если таблица занимает больше двух страниц, то при переносе части таблицы на другую страницу пишут слова «Продолжение таблицы 1», пример оформления названия таблицы:

Таблица 1.1 – Наименование таблицы следует помещать над таблицей слева без абзацного отступа с прописной буквы в одну строку с ее номером через тире без точки в конце. Если наименование таблицы занимает две строки и более, то его следует записывать через один межстрочный интервал

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Продолжение таблицы 1.1

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**А.4 Оформление формул и уравнений**

Уравнения и формулы следует выделять из текста в отдельную строку. Выше и ниже каждой формулы или уравнения должно быть оставлено *не менее одной свободной строки*. Если уравнение не умещается в одну строку, оно должно быть перенесено после знака равенства (=) или после знаков плюс (+), минус (–), умножения (×), деления (:) или других математических знаков. На новой строке знак повторяется.

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой они представлены в формуле. Значение каждого символа и числового коэффициента необходимо приводить с новой строки. Первую строку пояснения начинают со слова "где" без двоеточия с абзаца.

Формулы в отчете следует располагать *посередине строки* и обозначать порядковой нумерацией в пределах всего отчета арабскими цифрами в круглых скобках в крайнем правом положении на строке. Одну формулу обозначают (1).

Ссылки в отчете на порядковые номера формул приводятся в скобках в формуле (1).

Допускается нумерация формул в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой: (3.1)

Пример:

Для рядов данных *x, y* коэффициенты линейных зависимостей *a, b (y* = *a* + *bx)* рассчитываются, как решение системы уравнений (3.1):

|  |  |
| --- | --- |
| \begin{pmatrix}1&\bar{x}\\\bar{x}&\bar{x^2}\\\end{pmatrix}\begin{pmatrix}a\\b\\\end{pmatrix}=\begin{pmatrix}\bar{y}\\\overline{xy}\\\end{pmatrix}, | (3.1) |

где *x* – средние или максимальные значения температуры процессоров;

*y* – температуры на выходе бака;

, – среднее арифметическое значение элементов ряда.

**А.5 Оформление списка использованных источников**

Список должен содержать сведения об источниках, использованных при составлении отчета. Сведения об источниках приводятся в соответствии с требованиями ГОСТ 7.1, [ГОСТ 7.80](consultantplus://offline/ref=1664E79CF97BFD0858C3BB176F68BD1AE7E0C40EC8784F205FE14ABC80BBR0M), [ГОСТ 7.82](consultantplus://offline/ref=1664E79CF97BFD0858C3AD1B6D68BD1AEAEBC600CA2A18220EB444BBR9M) (пример приведен в Приложении Б).

Сведения об источниках следует располагать в порядке появления ссылок на источники в тексте отчета и нумеровать арабскими цифрами с точкой и печатать с абзацного отступа.

Список использованных источников должен включать библиографические записи на документы, использованные при составлении отчета, ссылки на которые оформляют арабскими цифрами в квадратных скобках [1], [3]–[10] в тексте отчета. На каждый источник в тексте отчета должна быть такая ссылка.

# ПРИЛОЖЕНИЕ Б. Пример списка использованных источников

1. DeRidder J.L. The immediate prospects for the application of ontologies in digital libraries// Knowledge Organization – 2007 . – Vol. 34, No. 4 . – P. 227 – 246 .

2. Прогноз научно-технологического развития Российской Федерации на период до 2030 года . – URL: http://government.ru/media/files/41d4b737638891da2184/pdf (дата обращения 15.11.2016).

3. U.S. National Library of Medicine. Fact sheet: UMLS Metathesaurus/National Institutes of Health, 2006 – 2013. – URL: http://www.nlm.nih.gov/pubs/factsheets/umlsmeta.html (дата обращения 2014-12-09).

4. U.S. National Library of Medicine. Fact sheet: Unfied Medical Language System/National Institutes of Health, 2006 – 2013. – URL: http://www.nlm.nih.gov/pubs/factsheets/umls.html (дата обращения 2009-12-09).

5. Антопольский А.Б., Белоозеров В.Н. Процедура формирования макротезауруса политематических информационных систем// Классификация и кодирование – 1976 . – N 1 (57). – С. 25 – 29 .

6. Белоозеров В.Н., Федосимов В.И. Место макротезауруса в лингвистическом обеспечении сети органов научно-технической информации// Проблемы информационных систем – 1986 . – N 1. – С. 6 – 10 .

7. Гуреев В.Н., Мазов Н.А. Использование библиометрии для оценки значимости журналов в научных библиотеках (обзор)// Научно-техническая информация. Сер. 1. – 2015 . – N 2. – С. 8 – 19 .

8. Земсков А.И., Шрайберг Я.Л. Электронные библиотеки: учебник для вузов. – М: Либерея, 2003 . – 351 с.

9. Костюк К.Н. Книга в новой медицинской среде. – М.: Директ-Медиа, 2015. – 430 с.

10. Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги [Электронный ресурс]. – URL: http://bookhamber.ru/stat\_2006.htm (дата обращения 12.03.2009).

11. Web of Science. – URL: http://apps.webofknowledge.com (дата обращения 15.11.2016).

12. Леготин Е.Ю. Организация метаданных в хранилище данных// Научный поиск. Технические науки: Материалы 3-й науч. конф. аспирантов и докторантов/отв. за вып. С.Д. Ваулин; Юж.-Урал. гос. ун-т. Т. 2. – Челябинск: Издательский центр ЮУрГУ , 2011 – С. 128 – 132 .

13. Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги [Электронный ресурс]. – 2006. – URL: http://bookhamber.ru/stat\_2006.htm (дата обращения 12.03.2009).

14. Приказ Минобразования РФ от 19 декабря 2013 г. N 1367 "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры". – URL: http://www. consultant.ru/document/cons\_doc\_LAW\_159671 (дата обращения 04.08.2016).

15. ГОСТ 7.0.96-2016 Система стандартов по информации, библиотечному и издательскому делу. Электронные библиотеки. Основные виды. Структура. Технология формирования. – М: Стандартинформ, 2016 . – 16 с.