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 № 4

по дисциплине «Криптографические методы защиты информации»

Современные симметричные шифры

|  |
| --- |
| Студент гр. \_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_ В. С. Новиков  «\_\_\_» \_\_\_\_\_\_\_\_\_ 2025 г. |
| Руководитель  Заведующий кафедрой информационной безопасности киберфизических систем  канд. техн. наук, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_О.О. Евсютин  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2025 г. |

Москва 2025

**СОДЕРЖАНИЕ**

[1 Задание на практическую работу 3](#_Toc155608317)

[2 Название раздела 4](#_Toc155608318)

[2.1 Название подраздела 4](#_Toc155608319)

[X Выводы о проделанной работе 5](#_Toc155608320)

[X Список использованных источников 6](#_Toc155608321)

[ПРИЛОЖЕНИЕ А. Основные требования к оформлению отчета 7](#_Toc155608322)

[ПРИЛОЖЕНИЕ Б. Пример списка использованных источников 12](#_Toc155608323)

# Задание на практическую работу

Целью данной работы является приобретение навыков программной реализации современных алгоритмов симметричного шифрования.

Написать программную реализацию одного из перечисленных ниже симметричных шифров (по выбору студента). Реализация шифра должны быть выполнена студентом самостоятельно без использования готовых библиотечных функций, напрямую реализующих алгоритм шифрования или его отдельные этапы. Варианты шифров:

- Магма;

- Кузнечик;

- AES;

Вариант «Магма» - программу для шифра «Магма»

# Теоретическая часть

## ГОСТ Р 34.12-2015

Действующий российский стандарт симметричного шифрования описан в документе «ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры». Данный стандарт был разработан на смену ГОСТ 28147-89 и введен 1 января 2016 г.

ГОСТ Р 34.12-2015 описывает два симметричных блочных шифра:

- шифр «Магма» с длиной блока 64 бита и длиной ключа шифрования 256 бит;

- шифр «Кузнечик» с длиной блока 128 бит и длиной ключа шифрования 256 бит.

Шифр «Магма» представляет собой тот же самый шифр, который был описан в стандарте ГОСТ 28147-89. Отличие заключается лишь в том, что в шифре «Магма» определена фиксированная таблица замен (один из этапов основного криптографического преобразования в данном шифре заключается в замене 4-битовых подблоков блока данных с помощью специальной таблицы), в то время как в ГОСТ 28147-89 данная таблица не определена и ее выбор оставлен на усмотрение разработчиков средств криптографической защиты информации, реализующих соответствующий алгоритм шифрования.

Важным отличием ГОСТ Р 34.12-2015 от ГОСТ 28147-89 является то, что в новом стандарте определены лишь базовые блочные шифры и не определены режимы их работы. Здесь под базовым блочным шифром понимается шифр, реализующий при каждом фиксированном значении ключа одно обратимое отображение множества блоков открытого текста фиксированной длины в блоки шифртекста такой же длины. Поэтому одновременно со стандартом ГОСТ Р 34.12-2015 был введен дополняющий его стандарт, определяющий режимы работы блочных шифров

## Шифр «Магма»

* Блочный шифр, 64 бита блок, 256 бит ключ.
* Основа: сеть Фейстеля, 32 раунда.
* Режим простой замены (ECB).
* Используемые операции: сложение, сдвиг, подстановка.

# Программный код и описание

## Описание

* язык: Python;
* функции генерация ключей, шифрование/расшифрование блока, обработка файла;
* Особенности реализация без библиотек, работа с файлами поблочно;
* SBOX - фиксированная таблица замен из ГОСТ Р 34.12-2015. (ГОСТ Р 34.12-2015, пункт Приложение А (обязательное);
* generate\_round\_keys - генерирует 32 раундовых ключа из 256-битного ключа;
* G: функция преобразования — сложение по модулю 232232, циклический сдвиг на 11 бит и подстановка по таблице;
* encrypt\_block / decrypt\_block - шифрование и расшифрование одного блока (64 бита) с использованием сети Фейстеля;
* process\_file - читает входной файл поблочно, шифрует/расшифрует и записывает результат.

## Код

# X 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.