УДК 004.056 **DOI: 10.18413/2518-1092-2022-8-1-0-3**

Кузьминых Е.С.
Маслова М.А.

АНАЛИЗ СИММЕТРИЧНЫХ МЕТОДОВ ШИФРОВАНИЯ, ПРОБЛЕМЫ И ПУТИ ВОЗМОЖНОГО ИХ РЕШЕНИЯ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: egor2014ru@mail.ru, mashechka-81@mail.ru

Аннотация
Человеку необходимо постоянно общаться, и он это делает на улице с друзьями, знакомыми, звоня по телефону, переписываясь в мессенджерах, пишет письма на почту. Всё это является информацией, которая передаётся по каналам передачи и может подвергаться различного рода кражам и рисковым ситуациям, которые необходимо правильно защищать, чем и занимается информационная безопасность. В эру квантовых компьютеров, конечно, базовые шифры ставятся под сомнение, но никто не запрещает комбинировать различные шифры, чтобы максимально себя обезопасить. В работе будут приведены методы шифрования, проанализированы несколько из них, а именно симметричного шифрования текста, выявлены их основные проблемы и предложены способы устранения их.
Ключевые слова: шифрование; криптография; шифр; текст; защита текста; шифр Цезаря; шифр Atbash; проблема шифров; информационная безопасность; каналы утечки
Для цитирования: Кузьминых Е.С., Маслова М.А. Анализ симметричных методов шифрования, проблемы и пути возможного их решения // Научный результат. Информационные технологии. – Т.8, №1, 2023. – С. 38-45. DOI: 10.18413/2518-1092-2022-8-1-0-3

Kuzminykh E.S.
Maslova M.A.

ANALYSIS OF SYMMETRIC ENCRYPTION METHODS, PROBLEMS AND WAYS OF THEIR POSSIBLE SOLUTION

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: egor2014ru@mail.ru, mashechka-81@mail.ru

Abstract
Person needs to constantly communicate, and he does this on the street with friends, acquaintances, making phone calls, chatting in instant messengers, writing letters to the post office. All this is information that is transmitted over transmission channels and can be subject to various kinds of theft and risk situations that must be properly protected, which is what information security does. In the era of quantum computers, of course, basic ciphers are being questioned, but no one forbids combining different ciphers in order to protect themselves as much as possible. The paper will present encryption methods, analyze several of them, namely symmetric text encryption, identify their main problems and propose ways to eliminate them.
Keywords: encryption; cryptography; cipher; text; text security; Caesar cipher; Atbash cipher; cipher problem; information security; leak channels
For citation: Kuzminykh E.S., Maslova M.A. Analysis of symmetric encryption methods, problems and ways of their possible solution – T.8, №1, 2023. – P. 38-45. DOI: 10.18413/2518-1092-2022-8-1-0-3

ВВЕДЕНИЕ

В 21 веке люди всё больше делятся информацией в пространстве интернета, общаются в социальных сетях, пишут письма, делятся различными файлами. Если брать в расчёт компании, то они могут делиться важной документацией, чертежами, а допускать утечку таких файлов не допустимо.

Для защиты информации используются различные методы и приемы, например: в переговорных комнатах ставят физические устройства для устранения каналов утечки информации;

в мессенджерах и почте используется шифрование баз данных и все сообщения передаются в зашифрованном виде, чтобы злоумышленник не мог напрямую увидеть что пишет пользователь. Но базовой защите не всегда доверяют и поэтому пользуются дополнительными мерами защиты шифруя свои сообщения специальными методами и своими уникальными ключами, о которых знает определённый круг лиц. Ведь если организации будут обмениваться документами, их необходимо защитить от кражи и даже если их украдут, чтобы у злоумышленника не было возможности расшифровать их.

Чтобы защищать текст разработаны специальные алгоритмы защиты текста с помощью шифрования, которое дает возможность преобразовывать информацию в целях ее сокрытия от неавторизированных пользователей, в свою очередь с возможностью авторизированным пользователям доступа к ней. Т.е. оно служит для конфиденциальности предоставляемой информации за счет использования ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

Из самых простых методов защиты текста существуют шифры подстановки, которые будут рассмотрены в работе далее. Шифр подстановки – представляет собой метод, в котором элементы начального текста меняются на другой текст с помощью зашифрованного текста по определенному правилу.

В крупных предприятиях, организациях, корпорациях необходимы сотрудники IT сферы, а в наиболее престижных корпорациях, которые хотят защищать свою информацию, необходимы сотрудники высокой квалификации, а именно сотрудники из сферы информационной безопасности. Сотрудникам из сферы информационной безопасности необходимо проходить каждый год переквалификацию и никогда не останавливаться в саморазвитии иначе им грозит отстать от громадных скачков развития IT-сферы и потерять свою работу. В крупных компаниях есть постоянные проблемы с защитой информации, её могут украсть как хакеры, так и сами сотрудники, а именно инсайдеры, или же просто от неосторожности, поэтому сотрудники информационной безопасности составляют нормативно-правовые акты для защиты информации, правила пользования приложениями, которые установлены на рабочих компьютерах у сотрудников, а также обучают этих сотрудников пользоваться ими. Помимо этого, они обучают сотрудников как стоит себя вести в определенных ситуациях, как действовать при экстренных ситуациях, какие письма не стоит открывать и многое другое. Обязательным так же есть функция распределения доступа к информации между сотрудниками, чтобы, например, обычный рядовой сотрудник не мог посмотреть бухгалтерскую информацию, а бухгалтер не мог распространять эту информацию открыто. Самое сложное для сотрудника информационной безопасности - это защитить информацию компании от внешнего проникновения, а именно хакеров. Необходимо правильно защитить информацию, а также грамотно зашифровать, защитить и укрыть секретные файлы, чтобы даже при проникновении в базу данных хакер не мог так легко украсть самые важные файлы. В основном сотрудники умеющие шифровать информацию нужны или в самых крупных компаниях, или в силовых структурах, ведь секретной информацией в силовых структурах постоянно делятся между собой и для её защиты необходимо грамотно шифровать информацию, как сам текст, так и каналы передачи информации [1].

ОСНОВНАЯ ЧАСТЬ

Люди каждый день делятся колоссальным количеством информации между собой, начиная с обычных приветов и вопросов о том, как провёл день и заканчивая деловыми встречами и передачей важных документов, казалось бы, что всё просто, отправил сообщение в мессенджере и оно моментально отправилось собеседнику, ноне все так просто. Обычный рядовой пользователь и не подозревает, насколько серьёзна защита обычных переписок, какие методы защиты существуют в каждой системе и какие методы шифрования используются для передачи текста. Методы шифрования очень важны для передачи информации между компаниями, так как довольно часто документы, пересланные по почте, могут иметь внушительную юридическую ценность, и утечка таких документов может понести серьёзные проблемы, а абсолютной защите почтового сервиса

верить не стоит. Именно поэтому важные документы дополнительно защищаются различными методами шифровки текста, или же самого документа.

Существует множество разных методов шифровки текста, но для начала стоит разобраться в самих способах, их уже не так и много:

– Симметричное шифрование. Метод шифрования, где для шифровки и расшифровки используется один и тот же криптографический ключ.

– Ассиметричное шифрование. Метод шифрования, предполагающий использование двух криптографических ключей, один из них открытый, который передаётся по незащищённому каналу, а второй закрытый, который знаете только вы, он используется для расшифровки текста.

– Хеширование. В отличии от двух предыдущих методов хеширование является односторонней функцией. Данный способ превращает текст в хеш и обратить данный процесс нельзя, данный хеш используется для проверки целостности файла, просматривая не редактировался ли он.

– Цифровая подпись. Включает в себя объединение хеширования и ассиметричного метода шифрования. Сообщение сначала хешируется, а потом шифруется закрытым ключом, затем получатель расшифровывает открытым ключом и извлекает хеш, после сообщение снова хешируется, для сравнения с исходным хешем [2-4].

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Рассмотрим, пожалуй, два самых популярных и наиболее простых метода шифрования текста: метод Цезаря и метод Atbash. Метод Цезаря известен как шифр сдвига, относится к шифру подстановки, в котором каждый символ текста заменяется на другой символ из алфавита с определённым шагом. На пример буква «А» с шагом +2 заменится на букву «В». Метод Atbash, тоже довольно прост, относится к шифру подстановки и в его основе лежит формула (1), проще говоря, алфавит переворачивается, буква А заменится на букву Я и так далее.

$$n - i + 1, \tag{1}$$

где: n – число букв в алфавите,
i – номер выбранной буквы.

Рассмотрим код 1-й программы: шифровка методом Цезаря [5]. Суть работы программы: в начале описан буквенный алфавит, который может распознать программа. Переменной “should_end” присваивается значение “False”, что означает, что программа ещё не закончена, после идёт проверка, не закончена ли программа и начинается работа самой программы. Программа просит ввести тип его работы, шифровка, или расшифровка и записывает значение в переменную “direction”. После просит ввести текст и записывает в переменную “text”, далее просит ввести шаг для шифровки и записывает значение в переменную “shift”. На следующем этапе программа проверяет, не ввёл ли пользователь слишком большой шаг (26 максимум) и если ввёл, то производит специальное вычисление, чтобы взять другой шаг. Далее запускается функция “Caesar”, в которой происходит сама шифровка текста. Создаётся переменная “end_text”, куда запишется конечный текст. Производится проверка, введена ли фраза decode, если да, то шаг становится отрицательным. Далее входим в цикл, где сначала переменной “position” присваивается значение индекса введённой буквы, после переменной “new_position” присваивается значение, позиции прошлой буквы + указанный шаг, далее к переменной “end_text” добавляется новая буква. Если символа нет в алфавите, то она добавляется к конечному тексту без шифровки. В конце выводит результат, и программа просит указать, желает ли пользователь перезапустить её и если да, то процедура повторяется, если нет, то программа завершается и выводит на экран фразу “Goodbye”.

Листинг 1

Пример работы 1-й программы

Listing 1

An example of the 1st program

```
alphabet = ['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', 'a', 'b',
'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q',
'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']

def caesar(start_text, shift_amount, cipher_direction):
  end_text = ""
  if cipher_direction == "decode":
    shift_amount *= -1
  for char in start_text:
    if char in alphabet:
      position = alphabet.index(char)
      new_position = position + shift_amount
      end_text += alphabet[new_position]
    else:
      end_text += char
 print(f"Here's the {cipher_direction}d result: {end_text}")

should_end = False
while not should_end:

  direction = input("Type 'encode' to encrypt, type 'decode' to decrypt:\n")
  text = input("Type your message:\n").lower()
  shift = int(input("Type the shift number:\n"))
  shift = shift % 26

  caesar(start_text=text, shift_amount=shift, cipher_direction=direction)

  restart = input("Type 'yes' if you want to go again. Otherwise type
'no'.\n")
  if restart == "no":
    should_end = True
    print("Goodbye")
```

В листинге 2 будет представлен собственный разработанный код для шифровки методом Атбаш. Данная программа берёт файл формата “.txt” и шифрует содержимое файла по заданному алфавиту. Помимо букв она также заменяет все символы на другие. Для тестирования кода данной программы была зашифрована англоязычная книга, с предоставлением скриншотов работы программы. У данной программы есть один дефект, она не сохраняет табуляцию, но читаемость текста от этого не теряется.

Листинг 2

Пример работы 2-й программы

Listing 2

An example of the 2nd program

```
lookup_table = {'A' : 'Z', 'B' : 'Y', 'C' : 'X', 'D' : 'W', 'E' : 'V',
        'F' : 'U', 'G' : 'T', 'H' : 'S', 'I' : 'R', 'J' : 'Q',
        'K' : 'P', 'L' : 'O', 'M' : 'N', 'N' : 'M', 'O' : 'L',
        'P' : 'K', 'Q' : 'J', 'R' : 'I', 'S' : 'H', 'T' : 'G',
        'U' : 'F', 'V' : 'E', 'W' : 'D', 'X' : 'C', 'Y' : 'B', 'Z' : 'A',
        'a': 'z', 'b': 'y', 'c': 'x', 'd': 'w', 'e': 'v',
        'f': 'u', 'g': 't', 'h': 's', 'i': 'r', 'j': 'q',
        'k': 'p', 'l': 'o', 'm': 'n', 'n': 'm', 'o': 'l',
        'p': 'k', 'q': 'j', 'r': 'i', 's': 'h', 't': 'g',
        'u': 'f', 'v': 'e', 'w': 'd', 'x': 'c', 'y': 'b', 'z': 'a',
```

```
        '1': '0', '2': '9', '3': '8', '4': '7', '5': '6', '6': '5', '7': '4',
        '8': '3', '9': '2', '0': '1', '.': '.', ',': ',', '!': '!', '?': '?',
        '"': '"'}
def atbashPrompt():
    codeChoice = input(str(" \nВведите \"а\" для шифрования файла.\nВведите
\"б\" для рисшифровки текста.\n"))
    if codeChoice == "а":
        with open("kniga.txt") as f:
            text = f.read()
        new_text = atbash(text)
        with open("Шифр.txt", 'w') as f:
            f.write(new_text)
    elif codeChoice == "б":
        with open("Шифр.txt") as f:
            text = f.read()

        new_text = atbash(text)
        with open("Расшифр.txt", 'w') as f:
            f.write(new_text)
def atbash(message):
  cipher = ''
  for letter in message:
    if (letter in lookup_table):
      cipher += lookup_table[letter]
    else:
      cipher += ' '
  return cipher
atbashPrompt()
```

Суть работы программы: в начале описан английский алфавит и символы, используемые для написания текстов. Запускаем функцию atbashPrompt, изначально программа ждёт ответа от пользователя, необходимо зашифровать, или расшифровать файл. Затем открывается файл книги, или шифрованного текста и запускается вторая функция atbash, которая непосредственно шифрует, или расшифровывает текст. Функция проходится по каждой букве по очереди, если буква присутствует в алфавите, то она заменяется на установленную, если же символа нет в прописанном алфавите, то ставится пробел. Далее программа заканчивает шифровку и сохраняет новый файл.

На рисунках 1-3 предоставлена работа программы шифрования файла англоязычной книги.

```
1  Pride and Prejudice
2  Jane Austen
3
4  Chapter 1
5  It is a truth universally acknowledged, that a single man in possession of a good fortune, must be in want of a wife.
6  However little known the feelings or views of such a man may be on his first entering a neighbourhood, this truth is so well
   fixed in the minds of the surrounding families, that he is considered the rightful property of some one or other of their
   daughters.
7  "My dear Mr. Bennet," said his lady to him one day, "have you heard that Netherfield Park is let at last?"
8  Mr. Bennet replied that he had not.
9  "But it is, returned she; "for Mrs. Long has just been here, and she told me all about it.
10 Mr. Bennet made no answer.
11 "Do you not want to know who has taken it?" cried his wife impatiently.
12 "YOU want to tell me, and I have no objection to hearing it."
13 This was invitation enough.
14 "Why, my dear, you must know, Mrs. Long says that Netherfield is taken by a young man of large fortune from the north of
   England; that he came down on Monday in a chaise and four to see the place, and was so much delighted with it, that he agreed
   with Mr. Morris immediately; that he is to take possession before Michaelmas, and some of his servants are to be in the house
   by the end of next week."
15 "What is his name?"
16 "Bingley."
17 "Is he married or single?"
18 "Oh! Single, my dear, to be sure! A single man of large fortune; four or five thousand a year. What a fine thing for our girls!"
19 "How so? How can it affect them?"
20 "My dear Mr. Bennet," replied his wife, "how can you be so tiresome! You must know that I am thinking of his marrying one of
   them."
21 "Is that his design in settling here?"
22 "Design! Nonsense, how can you talk so! But it is very likely that he MAY fall in love with one of them, and therefore you must
   visit him as soon as he comes."
23 "I see no occasion for that. You and the girls may go, or you may send them by themselves, which perhaps will be still better,
   for as you are as handsome as any of them, Mr. Bingley may like you the best of the party."
24 "My dear, you flatter me. I certainly HAVE had my share of beauty, but I do not pretend to be anything extraordinary now. When
   a woman has five grown-up daughters, she ought to give over thinking of her own beauty."
25 "In such cases, a woman has not often much beauty to think of."
```

Рис. 1. Исходный текст книги

Fig. 1. Source text of the book

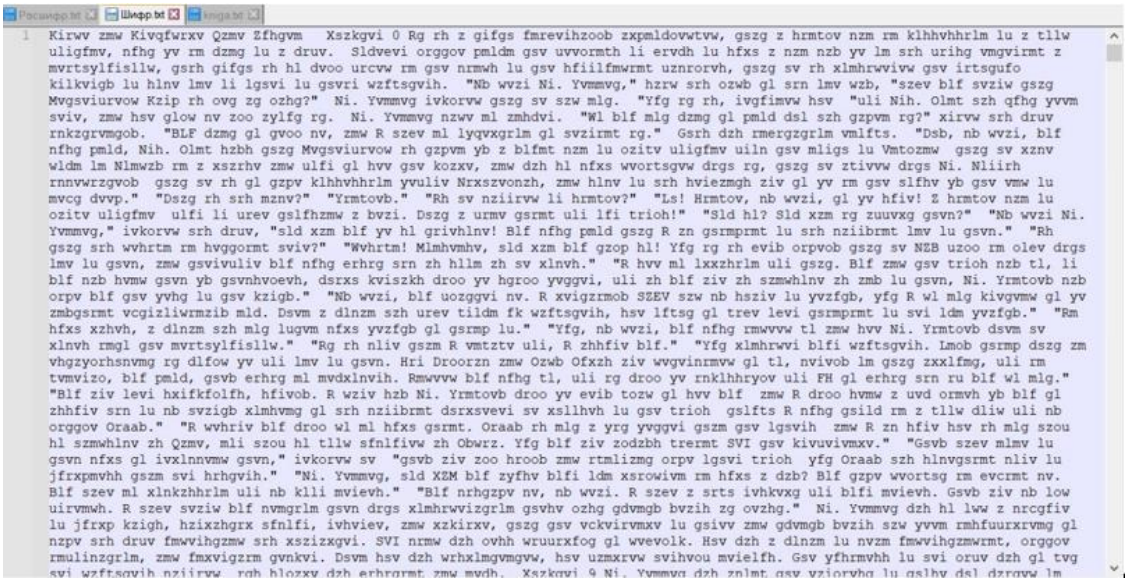

Рис. 2. Зашифрованный текст книги
Fig. 2. Cipher text of the book

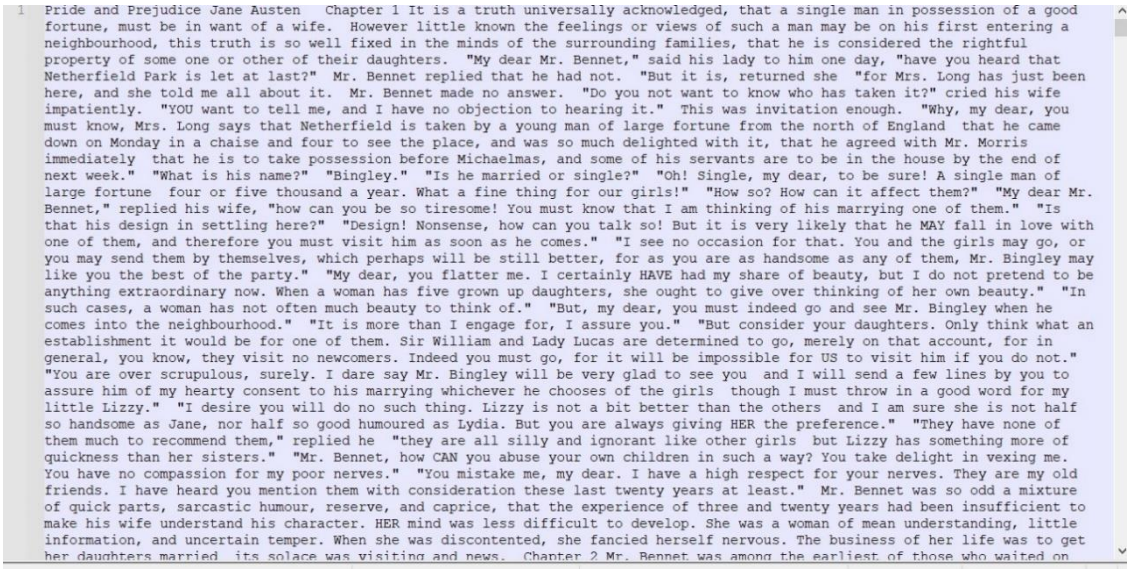

Рис. 3. Расшифрованный текст книги
Fig. 3. The transcribed text of the book

Проанализировав приведённые методы шифрования, можно сделать вывод, что данные методы довольно просты, разработаны эти методы были много лет назад и способы их взлома также просты. Например, шифр Цезаря, допустим необходимо зашифровать слово «hello» с шагом в 3 буквы, получится слово «khoor», количество букв не изменилось, значит нужно методом перебора подставлять буквы, начиная с шага 1 вправо, или влево и так далее, пока не получится слово. Чтобы усложнить задачу взлома такого шифра, можно, к примеру, использовать двойной или тройной шифр, т.е. шифровать текст несколько раз и с разным количеством шагов, тогда взломать будет более проблематично.

Криптография, как наука появилась относительно недавно, но даже у такой молодой науки есть нерешённые проблемы, например:

– ограниченность рабочих схем с открытым ключом. Существует большое количество различных методов и схем шифрования, которые можно комбинировать и по-разному

редактировать, но все они основываются на одной не решённой проблеме и становится понятно, что количество криптографических схем довольно ограничено;

– ненадёжность фундамента шифрования. Была доказана некоторая связь между разными методами шифрования и есть теория, что если будет взломан один шифр, то откроются некоторые двери к другим шифрам, что означает, что шифры тесно связаны и имеют довольно схожую основу;

– отсутствие перспектив. В наши дни развиваются квантовые компьютеры и вычисления, которые могут моментально прорабатывать колоссальное количество информации и в теории взломать любой шифр, прогнав множество комбинаций, что делает шифрование данных, по сути, бесполезным занятием;

– увеличение размера шифруемых блоков данных и ключей к ним. Из-за быстрого развития вычислительной техники происходит увеличение размеров блоков данных и их ключей, например, криптосистема RSA, ранее было достаточно 512 бит, теперь же рекомендуемый объём составляет 4096 бит [6-9].

Из вышесказанного можно сделать вывод, что криптография очень важна для защиты информации. Ее еще долго будут применять, комбинируя различные способы шифрования и изменяя их, чтобы запутать потенциального взломщика и усложнить ему работу выгадав время. Так как время часто является положительным фактором, так как если при передаче секретных данных злоумышленник не сможет узнать сразу всю информацию, а узнает её через несколько дней, эта информация уже может обесцениться, и её потеря не принесёт никаких проблем.

ЗАКЛЮЧЕНИЕ

При передаче информации по каналам одним из главных задач есть грамотная ее защита. Каждой организации, которая заботится о своей репутации и безопасности должна обязательно иметь в своем штате квалифицированного сотрудника информационной безопасности, который будет заботиться об этом. Так как необходимо постоянно проводить работу по: составлению различной документации; следить за работой и доступом сотрудников к различным данным, сайтам и информации; настраивать техническое оборудование для обеспечения защиты каналов передачи информации; шифровать информацию, циркулирующую в организации различными методами и т.д.

Обычные пользователи для собственной безопасности могут использовать простые методы шифрования. Можно использовать методы, описанные в статье, но для усиления защиты стоит их немного модифицировать, усложнять, использовать шифрование несколько раз, комбинировать разные шифры, для усложнения взлома такой криптограммы и тогда ваша информация всегда будет под защитой.

Список литературы

1. Ролдугина М.А. Методы шифрования, применяемые для защиты информации / М.А. Ролдугина // Научное сообщество студентов XXI столетия. Технические науки: сборник статей по материалам CII студенческой международной научно-практической конференции, Новосибирск, 10 июня 2021 года. Т. 6(101). – Новосибирск: Общество с ограниченной ответственностью "Сибирская академическая книга", 2021. – С. 46-51. – EDN HUHHGS.

2. Криптография и главные способы шифрования информации [Электронный ресурс]. URL: https://proglib.io/p/methods-of-encryption

3. Волкова П.Л. Методы шифрования / П.Л. Волкова // Наука настоящего и будущего. – 2020. – Т. 1. – С. 220-222. – EDN XMDBNU.

4. Костиков В.А. Необходимость сжатия зашифрованных данных с помощью алгоритмов кодирования LZW и Хаффмана / В.А. Костиков, М.А. Маслова // Теория и практика проектного образования. – 2021. – № 3(19). – С. 62-64. – EDN JASTQT.

5. Проект шифровки метода Цезаря [Электронный ресурс]. URL: https://clck.ru/ZL5ff

6. Криптография. Основные методы и проблемы [Электронный ресурс]. URL: https://moluch.ru/conf/tech/archive/163/8782/

7. Молдовян А.А. Криптография. Скоростные шифры. – БХВ-Петербург, 2002. URL: https://clck.ru/ZL5fD

8. Авдошин С.М., Савельева А.А. Криптоанализ: современное состояние и перспективы развития// Информационные технологии. – 2007. – №. S3. – С. 1-32. URL: https://clck.ru/ZL5ea

9. Карнута Д.С. Квантово-криптографические методы шифрования как актуальное и эффективное средство обеспечения информационной безопасности в сетях IoT / Д.С. Карнута // Вопросы защиты информации. – 2021. – № 2(133). – С. 3-7. – DOI 10.52190/2073-2600_2021_2_3. – EDN XAAADK.

References

1. Roldugina M.A. Encryption methods used to protect information / M.A. Roldugina // Scientific community of students of the XXI century. Engineering sciences: collection of articles based on the materials of the CII student international scientific and practical conference, Novosibirsk, June 10, 2021. Volume 6 (101). - Novosibirsk: Limited Liability Company "Siberian Academic Book", 2021. - P. 46-51. – EDN HUHHGS.

2. Cryptography and the main methods of information encryption [Electronic resource]. URL: https://proglib.io/p/methods-of-encryption

3. Volkova P.L. Encryption methods / P.L. Volkova // Science of the Present and Future. - 2020. - T. 1. – P. 220-222. – EDN XMDBNU.

4. Kostikov V.A. The need to compress encrypted data using LZW and Huffman coding algorithms / V.A. Kostikov, M.A. Maslova // Theory and practice of project education. - 2021. - No. 3(19). – P. 62-64. – EDN JASTQT.

5. The project of encryption of the Caesar method [Electronic resource]. URL: https://clck.ru/ZL5ff

6. Cryptography. Basic methods and problems [Electronic resource]. URL: https://moluch.ru/conf/tech/archive/163/8782/

7. Moldovyan A.A. Cryptography. speed ciphers. – BHV-Petersburg, 2002. URL: https://clck.ru/ZL5fD

8. Avdoshin S.M., Savelyeva A.A. Cryptanalysis: current state and development prospects // Information technologies. – 2007. – No. S3. – P. 1-32. URL: https://clck.ru/ZL5ea

9. Karnuta D.S. Quantum cryptographic encryption methods as an actual and effective means of ensuring information security in IoT networks / D.S. Karnuta // Information security issues. – 2021. – No. 2(133). – P. 3-7. – DOI 10.52190/2073-2600_2021_2_3. – EDN XAAADK.

Кузьминых Егор Сергеевич, студент третьего курса кафедры Информационная безопасность Института информационных технологий
Маслова Мария Александровна, старший преподаватель кафедры Информационная безопасность Института информационных технологий

Kuzminykh Egor Sergeevich, Third-year Student of the Department Information security, Institute of Information Technologies
Maslova Maria Alexandrovna, Senior Lecturer of the Department Information security Institute of Information Technologies