|  |  |  |
| --- | --- | --- |
|  |  | |
|  | **МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**  **ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «КАЗАНСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕЛОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»**  **КАЗАНСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ** |

**Реферат по дисциплине**

**Основы теории информации**

**на тему «Шифры»**

**Выполнил работу**

**обучающийся группы 892**

**Маряшин Дмиирий**

**Проверил работу**

**преподаватель**

**Абзалимов Ришат Рафикович**

**Казань, 2020**

Оглавление

[Введение 3](#_Toc54284446)

[Типы шифров 4](#_Toc54284447)

[Асимметричный шифр 5](#_Toc54284448)

[Симметри́чные криптосисте́мы 6](#_Toc54284449)

[Транспозиция 7](#_Toc54284450)

[Транспонирование 8](#_Toc54284451)

[Штакетник 10](#_Toc54284452)

[Скитала 11](#_Toc54284453)

[Литература 12](#_Toc54284454)

**Введение**

Шифр - это какая-либо система преобразования текста с секретом (ключом) для обеспечения секретности передаваемой информации. Шифры применяются для тайной переписки дипломатических представителей со своими правительствами, в вооруженных силах для передачи текста секретных документов по техническим средствам связи, банками для обеспечения безопасности транзакций, а также некоторыми интернет-сервисами по различным причинам. Важным параметром любого шифра является ключ — параметр криптографического алгоритма, обеспечивающий выбор одного преобразования из совокупности преобразований, возможных для этого алгоритма. В современной криптографии предполагается, что вся секретность криптографического алгоритма сосредоточена в ключе, но не деталях самого алгоритма Не стоит путать шифр с кодированием — фиксированным преобразованием информации из одного вида в другой. В последнем отсутствует понятие ключа и не выполняется принцип Керкгоффса. В наше время кодирование практически не используется для защиты информации от несанкционированного доступа, а лишь от ошибок при передаче данных (помехоустойчивое кодирование) и других целях, не связанных с защитой.

# 

# Типы шифров

Шифры могут использовать один ключ для шифрования и расшифрования или два различных ключа. По этому признаку различают:

Симметричный шифр использует один ключ для шифрования и расшифрования.

Асимметричный шифр использует два различных ключа.

Шифры могут быть сконструированы так, чтобы либо шифровать сразу весь текст, либо шифровать его по мере поступления. Таким образом существуют:

Блочный шифр шифрует сразу целый блок текста, выдавая шифротекст после получения всей информации.

Поточный шифр шифрует информацию и выдаёт шифротекст по мере поступления, таким образом имея возможность обрабатывать текст неограниченного размера, используя фиксированный объём памяти.

# Асимметричный шифр

система шифрования и/или электронной цифровой подписи (ЭЦП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу, и используется для проверки ЭЦП и для шифрования сообщения. Для генерации ЭЦП и для расшифровки сообщения используется секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), SSH. Также используется в PGP, S/MIME.

# Симметри́чные криптосисте́мы

способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в тайне обеими сторонами, должны осуществляться меры по защите доступа к каналу, на всем пути следования криптограммы, или сторонами взаимодействия посредством криптообъектов, сообщений, если данный канал взаимодействия под грифом "Не для использования третьими лицами". Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.



# Транспозиция

Допустим, у нас есть фраза: «МОЖНО, НО НЕЛЬЗЯ». И мы хотим её зашифровать. Самый простой способ - это записать всю фразу задом наперёд: «ЯЗЬЛЕН ОН, ОНЖОМ». Можно порядок слов в предложении оставить исходным, но каждое слово записать задом наперёд: «ОНЖОМ, ОН ЯЗЬЛЕН». А можно менять местами каждые две буквы: «ОМНЖ,ООНЕНЬЛЯЗ». Это называется «транспозиция» или простая перестановка в чистом виде.



# Транспонирование

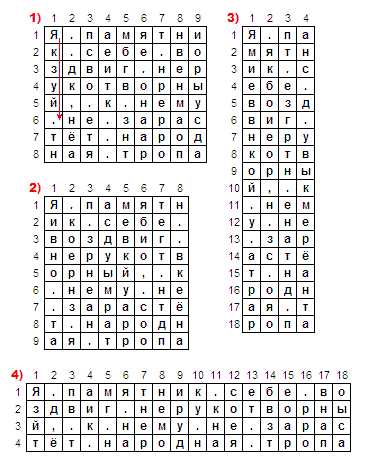
В этом шифре используется таблица. Сообщение записывается в таблицу по строкам, а для образования шифрованного текста считывается по столбцам. Ну или наоборот - записывается на столбцам, а считывается по строкам. Мы как бы переворачиваем таблицу относительно её диагонали, проходящей через верхний левый и нижний правый углы. Математики называют такой способ переворота таблицы транспонированием.

Для шифрования нужно нарисовать подходящего размера таблицу, вписать туда построчно шифруемый текст, а затем выписать его по столбцам в одну строку. Для расшифровки нужно лишь будет сообщить ключ шифра в виде размера таблицы. На рисунке ниже из ABCDEFGHIJKL получается ADGJBEHKCFIL. Согласитесь, понять без картинки, что это был алфавит, уже практически невозможно.

Итак, например, нам нужно зашифровать текст «Я памятник себе воздвиг нерукотворный, к нему не зарастёт народная тропа». В нём 72 символа. 72 - удобное число, оно делится без остатка на 2,4,6,8,12,18,24,36, поэтому можно использовать таблицы 2х36, 3х24, 4х18, 6х12, 8х9, 9х8, 12х6, 18х4, 24х3, 36х2 :). Определяемся с ключом (размером таблицы), вписываем текст по строкам, а затем переписываем его по столбцам.

На рисунке выше показаны варианты с таблицами 9×8, 8×9, 4×18 и 18×4. Для третьего варианта (таблица 4×18) получится вот такой текст:

«Ямиеввнкой у атрар якбоиеор,н зс ояопт езгртн енатнд панс д увыкмерёанта (4:18)»



# Штакетник

Упрощённый вариант транспонирования (с двухстрочной таблицей) - «штакетник». Напоминает «по конструкции» забор-шахматку.

Это очень простой способ шифровки, часто применяемый школьниками. Фраза записывается в две строки: в верхней пишутся нечётные буквы, в нижней - чётные. Затем нужно выписать подряд сначала верхнюю строку, затем нижнюю. Такое шифрование легко проделать и в уме, не выписывая сначала две строки.

«Я памятник себе воздвиг нерукотворный» превращается в «ЯАЯНКЕЕОДИНРКТОНЙ ПМТИСБВЗВГЕУОВРЫ».

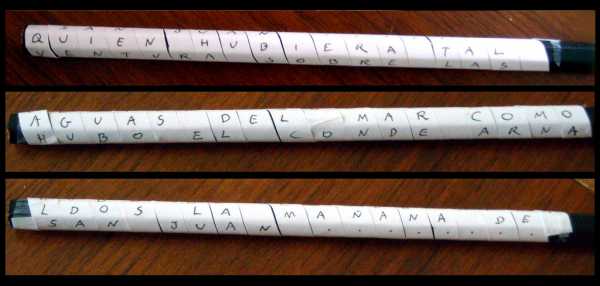


# Скитала

Известно, что в V веке до нашей эры правители Спарты, наиболее воинственного из греческих государств, имели хорошо отработанную систему секретной военной связи и шифровали свои послания с помощью «скиталы», первого простейшего криптографического устройства, реализующего метод простой перестановки.

Шифрование выполнялось следующим образом. На стержень цилиндрической формы, который и назывался «скитала», наматывали спиралью (виток к витку) полоску пергамента и писали на ней вдоль стержня несколько строк текста сообщения. Затем снимали со стержня полоску пергамента с написанным текстом. Буквы на этой полоске оказывались расположенными хаотично. Для восстановления текста требовалась скитала такого же диаметра.

По сути скитала - это наша обычная плоская таблица, обёрнутая вокруг цилиндра.

 Считается, что автором способа взлома шифра скиталы является Аристотель, который наматывал ленту на конусообразную палку до тех пор, пока не появлялись читаемые куски текста.

# Литература

<https://toto-school.ru/raznoe-2/transpoziciya-shifr-perestanovochnyj-shifr-vikipediya.html#i-2>

<https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80>