Муниципальное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа №1
имени Чернявского Якова Михайловича станицы Крыловской
муниципального образования Крыловский район.

"Шифрование Информации"

Автор работы:
Кузнецов Юрий Александрович
9 класс "А"класс
МБОУ СОШ №1 ст.Крыловской
МО Крыловский район
Руководитель:
Кряжимский Артём Сергеевич
учитель информатики
МБОУ СОШ №1 ст.Крыловской

2023 год

Оглавление

Введение

Каждый из нас знает такое слово как "шифрование". шифрование входит в состав криптографии. Криптографии уже более 4-х тысяч лет. Она появилась впервые в Древнем Египте. Имеются свидетельства, что криптография как техника защиты текста возникала вместе с письменностью, и способы тайного письма были известны уже древним целивизациям Индии, Египта и Месопотамии.

Сегодня, в век цифровых технологий , каждый из нас сталкивается с шифрованием даже не замечая этого. Мы ежедневно пользуемся разными

Интернет-ресурсами, которые зашифровывают данные для того, чтобы избежать получения этих данных третьеми лицами.
Набирая текст в поисковой строке , поисковик шифрует доступные ему данные . В наш век очень ценна информация. Вряд ли Вы хотите, чтобы ваше сообщение прочитал кто-то другой, а не получатель. Многие передают в сообщениях очень много конфиденциальной и ценной информации. Как раз, чтобы эта информация не попала злоумышленнику , большинство сервисов обмена сообщениий поддерживают шифрование.

Актуальность темы. Актуальностью проблемы шифрования данных в сфере криптографии являтся то, что использование систем шифрования в сфере защиты информации велико и на сегодняшний день существует множество различных алгоритмов, позволяющих осуществлять шифрование. Главным критерием каждого метода является его криптостойкость.

Объект исследования: способы шифрования информации

Предмет исследования: шифрование как преобразовательный процесс.

Цель работы: изучить способы шифрование информации, как способ конфиденциальности.

Для достижения данной цели в работе поставлены **следующие задачи:**

- изучить литературу по теме;
- рассмотреть простейшии шифры, такие как: шифр Цезаря, Азбука Морезе (Код Морзе);
- проанализировать цифровые, табличные шифры и шифры перестановки, такие как: шифр Атбаш, шифр Сцитала, шифр Ришелье, книжный шифр;

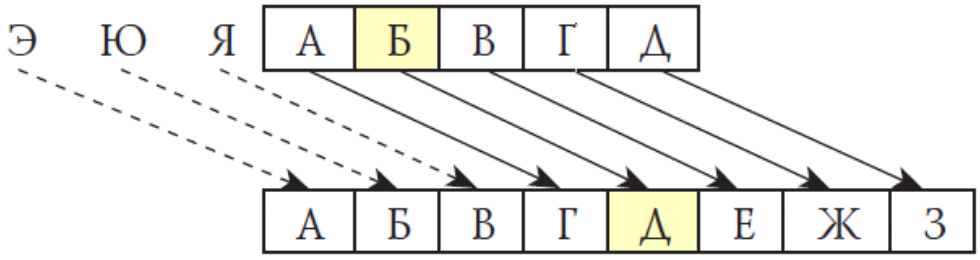
1. Простейшие шифры

Шифр Цезаря

Один из самых известных и в то же время простых шифров. Относится к шифрам моноалфавитной замены.

В данном шифре каждая буква в слове или тексте заменяется другой, которая находится на некоторое постоянное число позицией левее или правее от нее в

алфавите. Для расшифровки нужно только знать сдвиг в шифре. Например, если k=3, то формула у нас получится x=y-3. Здесь x - номер исходного символа в алфавите, y - номер символа шифрованного текста в алфавите.



Азбука Морзе (Код Морзе)

Тоже очень известный шифр. Как и шифр Цезаря, относится к моноалфовитной замене. Назван в честь сэмюэля Морзе. Код усовершенствовал сначала АлфредВейл, а затем Фридрих Герке. И в таком виде код используется и в наши дни. В этом шифре каждый символ заменяется последовательностью коротких и длинных звуковых сигналов. Короткий сигнал набумаге записывается как точка, длинный сигнал как тире.

Код Морзе. Код задает способ кодирования знаков последовательностью звуковых сигналов по определенным правилам. Код позволяет кодировать цифры, буквы, знаки пунктуаации, служебные символы посредством длинных сигналов и коротких.

2. Цифровые, табличные шифры и шифры перестановки

Шифр Атбаш

Атбаш можно считать шифром сдвига на всю длину алфавита или того числа символов, которые представлены к замене. Это простая замена для двух статических алфавитов.

Возьмем два алфавита, один из которых написан наоборот:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

ЯЮЭЬЫЪЩШЧЦХФУТ С Р ПОНМЛКЙИ ЗЖЁ Е ДГВ Б А

Вы видите, взаимное соответствие букв, которые заменяют друг друга.

Закодировать сообщение этим шифром очень простою

Возьмем текст: ШИРОКОЕ ПОЛЕ

Получаем перевод:ЖЦОРФРЪ ПРУЪ

Название Атбаш и само даёт подсказку, как работает этот шифр. В еврейском алфавите слово «атбаш» состоит из двух первых и двух последних букв алфавита: алеф(а), таб(т), бет(б), шин(ш).

Шифр Атбаш был использован в Библии, в Ветхом завете. Там есть кпоминание о царе Сесаха, хотя такой страны не существовало. На самом деле, это защиврованное название Вавилона - Сесах (или Шешах).

На иврите Вавилон пишется буквами «бет», и «ламед» (на английском это beth, beth и lamed, что соответствует согласным буквам в слове Babel - Вавилон). При шифровании Атбашем вторая в алфавите буква «бет» заменяется предпоследней в алфавите буквой «шин» (shin), а двенадцатая с начала буква «ламед» - двенадцатой с конца буквой «каф». Таким образом, после всех переводов с языка на язык было выяснено, что в тексте Библии слово Сесах (Шешах) обозначает Вавилон.

Правило зашифрования состоит в замене i-ой буквы алфавита буквой с номером n - i + 1, где n - число букв в алфавите. Для дешифрования сообщения нужно просто повторно применить к нему этот же алгоритм.

Функция, шифрующая строку методом Атбаш, имеет вид:

```
function Atbash(toCode: string): string;

var i: integer;

begin

for i := 1 to length(toCode) do

toCode[i ] := Chr(256 - Ord(toCode[ i ]));

Atbash := toCode;

end;

{ Использование: }

var

s: string;

begin

s := Atbash('Just a test'); { зашифровать }
```

```
writeln(s);

writeln('s = ', Atbash(s)); { расшифровать }

end.
```

Для дешифрования сообщения нужно просто повторно применить к нему этот же алгоритм.

Шифр Сцитала

Одним из первых приспособлений для шифрования, описание которого дошло до нас, был жезл – сцитала, который использовался во время войны Спарты с Афинами в v столетии до н.э. Это устройство представляло собой цилиндр определенного диаметра, на который наматывалась без просветов и нахлестов узкая лента папируса. На этой ленте, как на листе вдоль оси цилиндра записывали обычным способом исходный текст. После этого лента снималась с цилиндра и отправлялась адресату(шифротекст можно было прочесть только намотав ленту на такой же по диаметру цилиндр). По сути, это один из вариантов практической реализации шифра маршрутной перестановки, в котором геометрическая фигура – прямоугольник, размеры которого по количеству строк определяются диаметром цилиндра, а по количеству столбцов – длиной ленты (общее количество клеток должно быть не меньше n , где n – длина исходного текста). Начало маршрутов шифрования и дешифрации совпадают – начало ленты (верхний левый угол прямоугольника), а маршруты следующие: шифрования – по строкам слева направо; дешифрации – по столбцам сверху вниз. Если оценить возможные размеры цилиндра и высоту шрифта, то верхняя оценка числа перестановок (количества ключей) вряд ли превышает 100.

Шифр Ришелье

Шифр Ришелье, как метод защиты информации основан на применении решётки Кардано. Это металлический лист, с прорезанными в нём в случайном порядке прямоугольными окнами высотой, равной величине строки и длиной в произвольное количество символов.

Как использовать шифр Ришелье

Для написания сообщения лист с решёткой Кардано накладывался на лист бумаги, и в окна вписывался текст, содержащий закодированную информацию. Далее сетка убиралась и в промежутки между текстом документа вписывались

произвольные слова или набор букв, имеющие цель запутать того, для кого сообщения не было предназначено.

Дополнительное кодирование

Основной текст тоже кодировался следующим образом:

- Составлялся некий код, например (4213) (32514) (312) (132);
- Буквы в сообщении разбивались на группы по количеству символов в группах кода;
- В каждой группе буквы переставлялись в порядке, указанном цифрами.

Книжный шифр

Шпион должен стараться не вызвать подозрения, и поэтому любые предметы для шифрования, которые он держит дома, не должны бросаться в глаза. Даже единственная решетка может показаться подозрительной, а пачка решеток - это доказательство вины. По этой же причине шпион вряд ли будет пользоваться кодом, если для этого необходимо постоянно иметь под рукой большую кодовую книгу. Поэтому шпиону очень удобно применять шифр, использование которого не требует специального оборудования. Книжный шифр именно таков. Все, что нужно для работы - это книга на любую тему, текст которой набран только латинским алфавитом. Например, это мог бы быть роман, биография или труд по истории на английском языке, но только не книга по органической химии.Чтобы пользоваться книжным шифром, необходимо уметь попарно "складывать и вычитать" буквы алфавита. Эта процедура, как мы уже говорили в главе 1, начинается с того, что каждой букве алфавита присваивается номер (A=0, B=1, C=2, ..., Z=25), далее производится сложение или вычитание (по модулю 26) и обратное преобразование результата в буквы. Поскольку процедура эта утомительная, то проще раз и навсегда составить таблицы, а затем извлекать результат сложения или вычитания из соответствующей таблицы. Чтобы показать, как это делается без помощи таблиц, выполним эти операции для нескольких букв.

ЗАКЛЮЧЕНИЕ

Из вышеизложенного можно сделать следующие выводы :

1. Проблема защиты информации путем ее преобразования, исключающего прочтение посторонним лицом, волновала человеческий ум с жавних времен. В своей работе мы пытались разобраться в этой проблеме. В ходе работы над проектом мы узнали о различных видах шифрования сообщений.

2. Шифрование - прикладная наука, которая использует самые последние достижения фундаментальных наук, и в первую очередь математики и информатики. Практическое применение шифровании стало неотъемлемой частью жизни современного общества - её используют в таких отраслях как электронная коммерция, электронный документооборот, телекоммуникации и др.

3. Криптография связана с шифрованием и расшиврованиемконфинденциальных данных в каналах коммуникаций. она также применяется для того, чтобы исключить возможность искажения информации или подтвердить ее происхождение.

4. Хорошие криптографические системы создаются таким образом, чтобы сделать их вскрытие как можно более трудным делом. Можно построить системы, которые на практике невозможно вскрыть.При этом не требуется очень больших усилий для реализации. Единственное, что требуется- это аккуратность и базовые знания. Нет прощения разработчику, если он оставил возможность для вскыртия системы. Все механизмы, которые могут использоваться для взлома системы надо задокументировать и довести до сведения конечных пользователей.