Курсовая работа на тему: "Шифрование информации".

Выполнил: ученик 9^5 класса
Мамалаев Гайдар.

Махачкала 2019г

Актуальность темы

Актуальностью проблемы шифрования данных в сфере криптографии является то, что использование систем шифрования в сфере защиты информации велико и на сегодня существует множество различных алгоритмов позволяющих осуществлять шифрование.

Цель работы:

Знакомство с приемами шифрования и дешифрования текстовой информации.

Задачи работы:

- Изучить и проанализировать актуальную информацию о методах шифрования;

- Научиться шифровать и расшифровывать информацию разными способами.

Немного о теме:

Шифрование — это преобразование информации, делающее ее нечитаемой для посторонних. При этом доверенные лица могут провести дешифрование и прочитать исходную информацию. Существует множество способов шифрования / дешифрования, но секретность данных основана не на тайном алгоритме, а на том, что ключ шифрования (пароль) известен только доверенным лицам.

Шифрование появилось около четырех тысяч лет тому назад. Первым известным примером шифра считается египетский текст, созданный примерно в 1900 г. до н.э., в котором вместо обычных для египтян иероглифов использовались не совпадающие с ними символы.

Шифрование применяется для хранения важной информации в ненадёжных источниках и передачи её по незащищённым каналам связи. Такая передача данных представляет из себя два взаимно обратных процесса:

Перед отправлением данных по линии связи или перед помещением на хранение они подвергаются *зашифровыванию*.

Для восстановления исходных данных из зашифрованных к ним применяется процедура *расшифровывания*.

Шифром называется пара алгоритмов, реализующих каждое из указанных преобразований. Эти алгоритмы применяются к данным с использованием ключа. Ключи для шифрования и для расшифровывания могут различаться, а могут быть одинаковыми.

Криптография - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

Для современной криптографии характерно использование открытых алгоритмов шифрования, предполагающих использование вычислительных средств. Известно более десятка проверенных алгоритмов шифрования, которые при использовании ключа достаточной длины и корректной реализации алгоритма криптографически стойки.

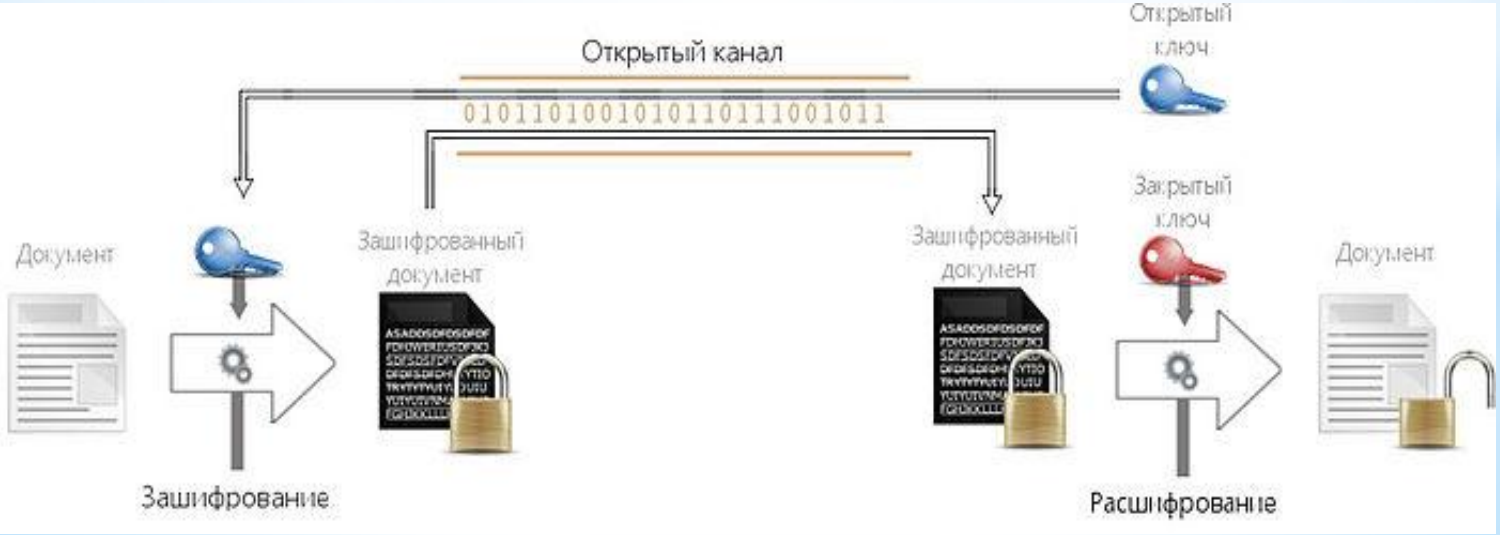
Криптографическая стойкость — свойство криптографического шифра противостоять криптоанализу, то есть анализу, направленному на изучение шифра с целью его дешифрования. Стойким считается алгоритм, атака на который требует от атакующего наличия столь значительных вычислительных ресурсов или огромных затрат времени на расшифровку перехваченных сообщений, что к моменту их расшифровки защищённая информация потеряет свою актуальность.

В большом количестве случаев криптостойкость не может быть математически доказана; можно только доказать уязвимость криптографического алгоритма либо свести задачу взлома алгоритма к некоторой задаче, которая считается вычислительно сложной (доказать, что взлом не легче решения этой задачи).

Методы шифрования:

Симметричное шифрование использует один и тот же ключ и для зашифровывания, и для расшифровывания.

Асимметричное шифрование использует два разных ключа: один для зашифровывания (открытый), другой для расшифровывания (закрытый).



Различные приемы шифрования:

Шифр Цезаря.

Этот шифр реализует следующее преобразование текста: каждая буква исходного текста заменяется следующей после нее буквой в алфавите, который считается написанным по кругу. Зашифруем следующее предложение:

Без труда не выловишь и рыбку из пруда.

Русский алфавит.

А	Б	В	Г	Д	Е
Ё	Ж	З	И	Й	К
Л	М	Н	О	П	Р
С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ъ	Ы	Ь
Э	Ю	Я			

Получится: **Вёи усфеб оё гьмпгйщэ й сьвлф йи рсфеб.**

Транспозиция.

В транспозирующих шифрах буквы переставляются по заранее определенному правилу. Могло быть такое, что каждое слово пишется задом наперед. Также могли меняться каждые две буквы.

Зашифруем двумя способами предложение:
Беда никогда не приходит одна
Получится следующее:

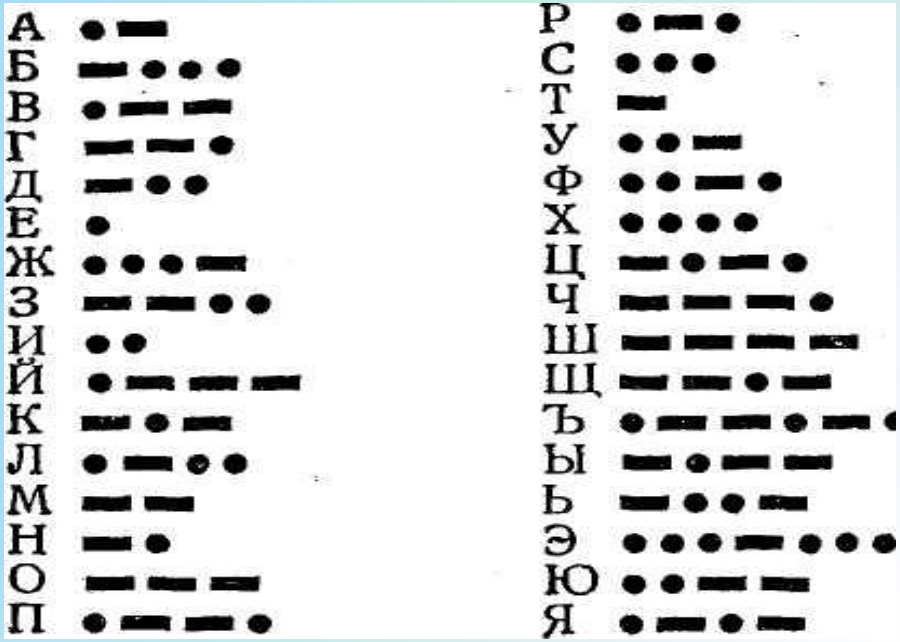
1) **Андо тидохирп ен адгокин адеб**

2) **Еб ад ин ок дг на пе ир ох ид от нд а**

Подобные шифры использовались в Первую Мировую и Американскую Гражданскую Войну, чтобы посылать важные сообщения. Сложные ключи могут сделать такой шифр довольно сложным на первый взгляд, но многие сообщения, закодированные подобным образом, могут быть расшифрованы простым перебором ключей на компьютере.

Азбука Морзе.

В азбуке Морзе каждая буква алфавита, все цифры и наиболее важные знаки препинания имеют свой код, состоящий из череды коротких и длинных сигналов, часто называемых «точками и тире».



Зашифруем предложение:

Всему своё время

Получится: **.-- ... . -- ..- ... .-- --- .-- .-. . -- .-.-**

Шифры Темура и Атбаш.

На Ближнем Востоке один из первых систематических шифров был разработан древними евреями; этот метод называется **темура -** «обмен». Двадцать две буквы еврейского алфавита делились на две части, причем одна помещалась над другой; затем верхние буквы заменялись на нижние или наоборот.

Можно было составлять всевозможные комбинации в зависимости от места разделения алфавита и направления перемещаемых букв. Самый простой способ заключался в разделении алфавита посередине так, чтобы первые две буквы, А и Б, совпадали с двумя последними, Т и Ш. Эти буквы и дали название методу шифровки **«Атбаш».**

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п
я	ю	э	ы	ь	щ	ш	ч	ц	х	ф	у	т	с	р

Зашифруем предложение:

Видна птица по полёту.

Получится: **Эцьтя рнця рс рсфщнм.**

Шифр Полибия.

В криптографии шифр Полибия, также известный как шахматная доска Полибия - оригинальный код простой замены, одна из древнейших систем кодирования, предложенная Полибием(греческий историк, полководец, государственный деятель, III век до н. э.). Данный вид кодирования
изначально применялся для греческого алфавита, но затем был распространен на другие языки.

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е/Ё
2	Ж	З	И/Й	К	Л	М
3	Н	О	П	Р	С	Т
4	У	Ф	Х	Ц	Ч	Ш
5	Щ	Ы	Ь/Ъ	Э	Ю	Я

Существует несколько способов шифрования с помощью шифра Полибия.

Зашифруем предложение: **Друзья познаются в беде.**

1 Способ - Заменяем букву на нижнюю от неё в том же столбце. Если буква в нижней строке, то заменяем на верхнюю из того же столбца. Получится: **Лццове хфоуждшче ь змлм.**

2 Способ - Сообщение преобразуется в координаты по квадрату Полибия, координаты записываются вертикально:

5 4 1 2 3 6 3 2 2 1 1 5 6 5 6 3 2 6 5 6

1 3 4 2 5 5 3 3 2 3 1 5 3 3 5 1 1 1 1 1

Далее координаты преобразуются в буквы по этому же квадрату:

5 1 3 3 2 1 6 6 2 5 1 4 5 3 2 1 3 5 1 1
4 2 6 2 1 5 5 3 6 6 3 2 5 3 3 5 3 1 1 1
Ч ж ь и б щ я т ы ю н к ю п о щ п д а а

Получится: **Чжьибщ ятыюнкюпо щ пдаа.**

3 Способ – Усложненный вариант, который заключается в следующем: полученный первичный шифротекст шифруется вторично. При этом он выписывается без разбиения на пары:

5412363221156563265613425533231533511111

Полученная последовательность цифр сдвигается влево на один шаг:

4123632211565632656134255332315335111115

Эта последовательность вновь разбивается в группы по два:

41 23 63 22 11 56 56 32 65 61 34 25 53 32 31 53 35 11 11 15

И по таблице заменяется на окончательный шифротекст:
Готзаю юияехысив с ьаащ.

Шифр с заменой букв цифрами и обратно.

Ключ к шифру с заменой букв и обратно:

1 2 3 4 5 6 7 8 9 0

о п с д а л н е т к

Таблица соответствия букв и цифр русского алфавита

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
1	2	3	4	5	6	7	8	9	10	11
К	Л	М	Н	О	П	Р	С	Т	У	Ф
12	13	14	15	16	17	18	19	20	21	22
Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
23	24	25	26	27	28	29	30	31	32	33

Зашифруем предложение: **Каждый судит по себе.**

Переведем буквы в цифры:

12 1 8 5 29 11 19 21 5 10 20 17 16 19 6 2 6

Переведем цифры в символы согласно ключу и получим шифротекст:

Оп о е а пт оо от по а ок пк он ол от л п л.

Шифр Виженера.

Шифр Виженера — это последовательность шифров Цезаря с различными значениями сдвига. То есть к первой букве текста применяется преобразование, например, на 2 сдвига, ко второй – на 3, и так далее. Последовательность применяемых преобразований определяется ключевой фразой, в которой каждая буква слова обозначает требуемый сдвиг. Фраза повторяется, пока не будет зашифрован весь текст сообщения.

Зашифруем предложение: **Ложка дёгтя в бочку мёду.**

Ключевая фраза – информация.

Получится: **Фьыщр рёщыю к огёыа мьмт.**

Хотя шифр легко понять и реализовать, на протяжении трех столетий он сопротивлялся всем попыткам его сломать; чем и заработал название **le chiffre indéchiffrable** (с французского 'неразгаданный шифр'). Многие люди пытались реализовать схемы шифрования, которые по сути являлись шифрами Виженера.

Заключение

В заключение можно отметить, что существует множество приемов шифрования текстовой информации, каждый из которых по-своему уникален.

Я изучил и проанализировал актуальную информацию о методах шифрования, а также научился шифровать и расшифровывать текстовую информацию разными способами.