IV региональная научно-исследовательская конференция

"НЬЮТОНиЯ-2020"

«Шифры и криптография»

Работу выполнили:

Атапина Полина,

г. Ленинск-Кузнецкий,

МБНОУ «Гимназия №18»,

5б класс

Научный руководитель:

Стаценко Анастасия Игоревна,

учитель математики

Оглавление

Введение

Общеизвестен афоризм британского политического деятеля Уинстона Черчилля: «Кто владеет информацией, тот владеет миром».

Поскольку информация становится все более и более ценным товаром, а революция в сфере коммуникаций изменяет общество, процесс зашифровывания сообщений, или иначе, шифрование, начинает играть все большую роль в повседневной жизни. Сегодня наши телефонные разговоры передаются по спутниковым каналам, а наши электронные письма проходят через различные компьютеры, и можно с легкостью осуществить перехват передаваемой информации по обеим этим видам связи, что ставит под угрозу нашу частную жизнь. Точно также, поскольку коммерческая деятельность во все большей степени осуществляется через Интернет, следует вводить меры безопасности, чтобы защитить компании и их клиентов.

Шифрование — единственный способ защитить нашу частную жизнь и гарантировать успешное функционирование электронного рынка. Искусство секретной связи, иначе известное как криптография, даст нам замки и ключи информационного прогресса.

С первыми шифрами я столкнулась в детстве, читая роман "Дети капитана Гранта", где герои пытались найти исходный текст письма из нескольких языковых вариантов. Еще тогда я почувствовала, как интересно разгадывать языковые головоломки. Позже были танцующие человечки Шерлока Холмса, которые только подкрепили мой интерес.

Мы взяли тему проекта «Шифры и криптография» в ходе работы над которым мы разгадаем некоторые тайны шифровки, сами придумаем несколько шифров и проверим их на криптостойкость.

Цель работы: создание собственного способа шифрования.

Задачи:

- изучить возникновение и историю развития криптографии и шифров при помощи литературой по данной теме;
- исследовать некоторые известные криптограммы;
- создать собственный шифр и проверить его на криптостойкость.

Объект работы - некоторые виды шифров.

Предмет - собственный алфавитный шифр.

В работе использовались такие методы, как изучение литературы, анализ, синтез, классификация, практический метод.

1. Что такое криптография и шифр

Тысячи лет короли, королевы и полководцы управляли своими странами и командовали своими армиями, опираясь на надежно и эффективно действующую связь. В то же время все они осознавали последствия того, что произойдет, если их сообщения попадут не в те руки, если вражескому государству будут выданы ценные секреты, а жизненно важная информация окажется у противника. И именно опасение того, что враги перехватят сообщение, послужило причиной активного развития кодов и шифров — способов скрытия содержания сообщения таким образом, чтобы прочитать его смог только тот, кому оно адресовано.

Стремление обеспечить секретность означало, что в государствах функционировали подразделения, создающие коды и шифры и отвечающие за обеспечение секретности связи путем разработки и использования самых надежных шифров. А в это же самое время дешифровальщики врага старались раскрыть эти шифры и выведать секреты. Дешифровальщики использовали науки от алхимии до лингвистики — племя колдунов, пытающихся с помощью магии получить осмысленные слова из бессмысленного набора символов. История кодов и шифров — это многовековая история поединка между создателями шифров и теми, кто их взламывает, интеллектуальная гонка вооружений, которая оказала разительное влияние на ход истории.

Криптография – наука о методах преобразования (шифрования) информации с целью её защиты от незаконных пользователей. Термин «криптография» происходит от двух греческих слов: «криптос» - тайна и «графейн» - писать, и означает тайнопись.

Что такое информация, от кого и как её надо защищать?

Информация – основное понятие научных направлений, изучающих процессы передачи, переработки и хранения различных данных (средства массовой информации, научно-техническая информация, генетическая информация.) Информация, которая является защищаемой, конфиденциальной, секретной, нуждается в защите. Для наиболее часто встречающихся ситуаций введены специальные понятия:

- военная тайна;
- государственная тайна;
- коммерческая тайна;

- врачебная тайна.

Защищаемая информация имеет следующие признаки:

- имеется какой-то круг законных пользователей;
- имеются незаконные пользователи, которые стремятся овладеть этой информацией с тем, чтобы обратить себе во благо, а законным пользователям во вред.

Между людьми происходит интенсивный обмен информацией, и она бывает открытой – телеграф, телефон, радио, телевидение и закрытой, защищаемой – тайнопись.

Разработкой мер защиты занимается криптография – тайнопись – способ письма, имеющий целью сделать написанное понятным только для посвящённых или рассчитанной на разгадывание.

Для тайнописи используется шифр – способ, метод преобразования информации с целью её защиты от незаконных пользователей.

2. История развития шифров и криптографии

История криптографии насчитывает около 4 тысяч лет. Имеются свидетельства, что криптография как техника защиты текста возникла вместе с письменностью, и способы тайного письма были известны уже древним цивилизациям Индии, Египта и Месопотамии.

Самым важным зашифрованным посланием древней культуры острова Крит стал Фестский диск (рис. 1) – изделие из глины, найденное в городе Фест в 1903 году. Обе его стороны покрыты иероглифами, нанесёнными по спирали. Специалисты сумели различить 45 видов знаков, но из них лишь несколько опознаны как иероглифы, которые использовались в додворцовом периоде древней истории Крита.

Рисунок 1 – Фестский диск.

Первым упоминанием об использовании криптографии принято считать использование специальных иероглифов около 3900 лет назад в Древнем Египте. В

дальнейшем встречаются различные упоминания об использовании криптографии, большая часть относится к использованию в военном деле.

Порой священные иудейские тексты шифровались методом замены. Вместо первой буквы алфавита писалась последняя буква, вместо второй - предпоследняя и так далее. Этот древний метод шифрования назывался «Акбаш». Известно, что так шифровалась переписка Юлия Цезаря (100 - 44 гг. до н. э.) с Цицероном (106 - 43 г.г. до н. э.).

Алфавитные шифры широко применялись вплоть до начала XX века. С начала и до середины XX века появились электромеханические устройства для работы шифровальщиков. При этом продолжалось использование полиалфавитных шифров.

Криптос (рис. 2) – скульптура, которую американский художник Джеймс Сэнборн установил в 1990 году в Лэнгли. Зашифрованное послание, нанесённое на неё, до сих пор не могут разгадать.

Рисунок 2 – Криптос.

С середины XX века до 70-х годов XX века был период перехода к математической криптографии. В работе Клода Э́лвуда Ше́ннона (американский инженер, криптоаналитик и математик) появляются строгие математические определения количества информации, передачи данных, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным атакам. Однако до 1975 года криптография оставалась "классической", или же, более корректно, криптографией с секретным ключом.

Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления – криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами. Современная криптография образует отдельное научное

направление на стыке математики и информатики – работы в этой области публикуются в научных журналах, организуются регулярные конференции. Практическое применение криптографии стало неотъемлемой частью жизни современного общества – её используют в таких отраслях как электронная коммерция, электронный документооборот, телекоммуникации и других.

3.Типы шифров

3.1 Симметричные шифры

Симметричные шифры – способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ.

Простая перестановка.

Шифрующие таблицы

В качестве ключа в шифрующих таблицах используются:

- размер таблицы;
- слово или фраза, задающие перестановку;
- особенности структуры таблицы.

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы. Например, сообщение:

Я ЛЮБЛЮ МАТЕМАТИКУ!!!!

записывается в таблицу поочередно по столбцам (рис. 3). После заполнения таблицы текстом сообщения по столбцам для формирования шифротекста считывают содержимое таблицы по строкам.

Я	***Ю***	***М***	***У***
Л	***М***	***А***	***!***
Ю	***А***	***Т***	***!***
Б	***Т***	***И***	***!***
Л	***Е***	***К***	***!***

Рисунок 3 – Шифрующая таблица

Если шифротекст записывать группами по четыре буквы, получается такое шифрованное сообщение:

ЯЮМУ ЛМА! ЮАТ! БТИ! ЛЕК!

Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Следует заметить, что объединение букв шифротекста в 4-буквенные группы не входит в ключ шифра и осуществляется для удобства записи не смыслового текста. При расшифровании действия выполняют в обратном порядке.

Одиночная перестановка по ключу.

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Шифрование простой перестановкой осуществляется следующим образом:

- выбирается ключевое слово с неповторяющимися символами;
- шифруемый текст записывается последовательными строками под символами ключевого слова;
- зашифрованный текст выписывается колонками в той последовательности, в которой располагаются в алфавите буквы ключа (или в порядке следования цифр в натуральном ряду, если ключ цифровой).

Пример шифрования способом простой перестановки сообщения:
БУДЬТЕ ОСТОРОЖНЫ С ПРЕДСТАВИТЕЛЕМ ФИРМЫ "ФЕНИКС".
При этом применим цифровой ключ 5-8-1-3-7-4-6-2. В исходном тексте вместо пробелов используется символ *.

	Ключ							
	5	8	1	3	7	4	6	2
Текст	Б	У	Д	Ь	Т	Е	*	О
	С	Т	О	Р	О	Ж	Н	Ы
	*	С	*	П	Р	Е	Д	С
	Т	А	В	И	Т	Е	Л	Е
	М	*	Ф	И	Р	М	Ы	*
	Ф	Е	Н	И	К	С	*	*

Выписывая текст по колонкам и группируя символы по пять, получаем зашифрованный текст в виде:

ДО*ВФ НОЫСЕ **ЬРП ИИИЕЖ ЕЕМСБ С*ТМФ *НДЛЫ *ТОРТ РКУТС А*Е**

Расшифрование выполняется в следующем порядке:

- подсчитываем число знаков в зашифрованном тексте и делим на число знаков ключа;
- выписываем ключевое слово и под его знаками в соответствующей последовательности выписываем символы зашифрованного текста в определенном выше количестве;
- по строкам таблицы читаем исходный текст.

Слабость шифрования простой перестановкой обуславливается тем, что при большой длине шифруемого текста в зашифрованном тексте могут проявиться закономерности символов ключа. Для устранения этого недостатка можно менять ключ после зашифровки определенного числа знаков. При достаточно частой смене ключа стойкость шифрования можно существенно повысить. При этом, однако, усложняется организация процесса шифрования и расшифрования.

Двойная перестановка.

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов были другие, чем в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки.

Перестановка «Магический квадрат».

Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст, вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифротекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью магических квадратов шифротексты охраняет не только ключ, но и магическая сила.

Пример. Зашифруем фразу «МАГИЧЕСКАЯ СИЛА» с помощью магического квадрата размером 4х4. Для этого выберем один из 880 вариантов магических квадратов заданного размера (рис. 4а). Затем вписываем каждую букву сообщения в отдельную ячейку таблицы с номером, соответствующим порядковому номеру буквы в исходной фразе (рис. 4б). При считывании заполненной таблицы по строкам получаем шифртекст: «ГАИАЕССЧЯ_КИАЛМ».

Шифротекст, получаемый при считывании содержимого таблицы по строкам, имеет вполне загадочный вид:

16	3	2	13
9	6	7	12
5	10	11	8
4	15	14	1

а) магический квадрат

	Г	А	И
А	Е	С	С
Ч	Я		К
И	А	Л	М

б) квадрат с сообщением

Рисунок 4 а,б – Магический квадрат

3.2. Асимметричное шифрование

Асимметричное шифрование – система шифрования, при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу, и используется для шифрования сообщения. Для шифрования и расшифровывания сообщения используется секретный ключ.

Рассматривается схема с возможностью восстановить исходное сообщение с помощью «лазейки», то есть труднодоступной информации. Для шифрования текста можно взять большой абонентский справочник, (в нем невозможно по известному номеру найти абонента). Для каждой буквы из шифруемого сообщения выбирается имя, начинающееся на ту же букву. Таким образом, букве ставится в соответствие номер телефона абонента. Отправляемое сообщение, например, «КЛЮЧ», будет зашифровано следующим образом (рис. 5):

Сообщение	Выбранное слово	Криптотекст
К	Косарев	542550
Л	Леонов	538906
Ю	Ющенко	319038
Ч	Чмир	355659

Рисунок 5 - Асимметричное шифрование

3.3 Старинные шифры

Шифр Цезаря.

Шифр Цезаря – один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации – шифр простой замены.

Наше фиксированное число будет 3, вот что получается (рис. 6):

Исходный текст	Зашифрованный
Ш	Ы
И	Л
Ф	Ч
Р	У
Ы	Ю

Рисунок 6 – Шифр Цезаря.

«Тарабарская грамота»

Русские дипломаты XV – XVI в., стремившиеся сохранить тайну переписки, применяли «тарабарскую грамоту», в которой все гласные буквы оставались неизменными, а согласные менялись друг на друга по следующей схеме:

Б В Г Д Ж З К Л М Н

| | | | | | | | | |

Щ Ш Ч Ц Х Ф Т С Р П

Например, вместо «Великий государь» получалось «Шеситий чолуцамь»

3.4 Известные шифры

«Порядковый номер»

Этот шифр встречается очень часто. Он заключается в том, что каждая буква имеет свой порядковый номер. И при шифровании вместо букв пишется это номер. Например, чтобы зашифровать слово «круг», нужно взять числа 12,18,21,4.

«Английская раскладка»

Этот шифр многие используют для паролей. Смысл этого заключается в том, что слова на русском печатаются в английской раскладке. Например, слово «уравение» будет печататься как «ehfdytybt».

Матричный способ кодирования

Огромную роль в проблеме расшифровки текстов играет, как ни странным это может показаться, математика, прежде всего теория вероятностей и математическая статистика. Чтобы воспользоваться им для шифровки и расшифровки (кодирования и декодирования), достаточно знать лишь простейшую арифметику, порядок букв в алфавите и помнить всего… четыре числа. А расшифровать ваш текст непосвященному человеку будет абсолютно не под силу.

4. Практическая часть

В ходе работы нами было изучено, что такое шифры, криптограммы и виды шифрования. Мы решили составить свой способ шифрования (приложеие1).

Приложение 1.

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

Исходный текст: «Всё, что познается, имеет число, ибо невозможно ни понять ничего, ни познать без него».

Зашифрованный текст: «31 15 27, 9 20 16 13 16 25 19 33 27 20 15 1, 10 14 6 6

20 9 10 15 21 16, 10 2 16 19 6 31 16 25 14 16 8 19 16 19 10 13 16 19 1 20 30 19 10 9 6 4 16, 19 10 13 16 25 19 33 20 30 2 6 25 19 6 4 16»

Чтобы расшифровать сообщение, нужно проделать обратные действия и по таблице вместо цифр записать буквы.

Приложение 2.

Используя различные виды шрифтов, мы зашифровали фразы. Вот что получилось.

1. **Простая перестановка:**

О	Л	И	Н
Д	Ю	Н	О
И	С	Р	Д
Н	О	А	В
П	Д	В	А

Исходный текст: «Один плюс один равно два».

Зашифрованный текст: «Олин дюно исрд ноав пдва»

2. **Одиночная перестановка по ключу:**

Зашифруем фразу «Математика — царица наук», используя ключ 7253416

До перестановки:

7	2	5	3	4	1	6
М	а	т	е	м	а	т
и	к	а	-	ц	а	р
и	ц	а	н	а	у	к

Расставляем ключ в порядке возрастания, получаем:

1	2	3	4	5	6	7
а	а	е	м	т	т	а
а	к	-	ц	а	р	к

у	ц	н	а	а	к	ц

Зашифрованный текст: «ааемттаак — царкуцнаанц»

3. Двойная перестановка:

Используя тот же ключ и ту же фразу зашифруем ее еще раз

До перестановки

7	2	5	3	4	1	6
а	а	е	м	т	т	а
а	к	-	ц	а	р	к
у	ц	н	а	а	н	ц

После перестановки

1	2	3	4	5	6	7
т	а	м	т	е	а	а
р	к	ц	а	-	к	а
н	ц	а	а	н	ц	у

Получаем: «тамтеааркца — канцаанцу»

4. Магический квадрат:

Возьмем один из 880 готовых вариантов магического квадрата и зашифруем фразу, присвоив каждой букве порядковый номер:

«М а т е м а т и к а - т о ч н а я н а у к а»

1 2 3 4 5 67 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

1	15	24	8	17
9	18	2	11	25
12	21	10	19	3

20	4	13	22	6
23	7	16	5	14

Зашифрованный текст: «мокин каа а -наят е аа утчмт»

М	о	к	и	н
к	а	а		а
-	н	а	я	т
	е		а	а
у	т	ч	м	т

5. **Шифр Цезаря:**

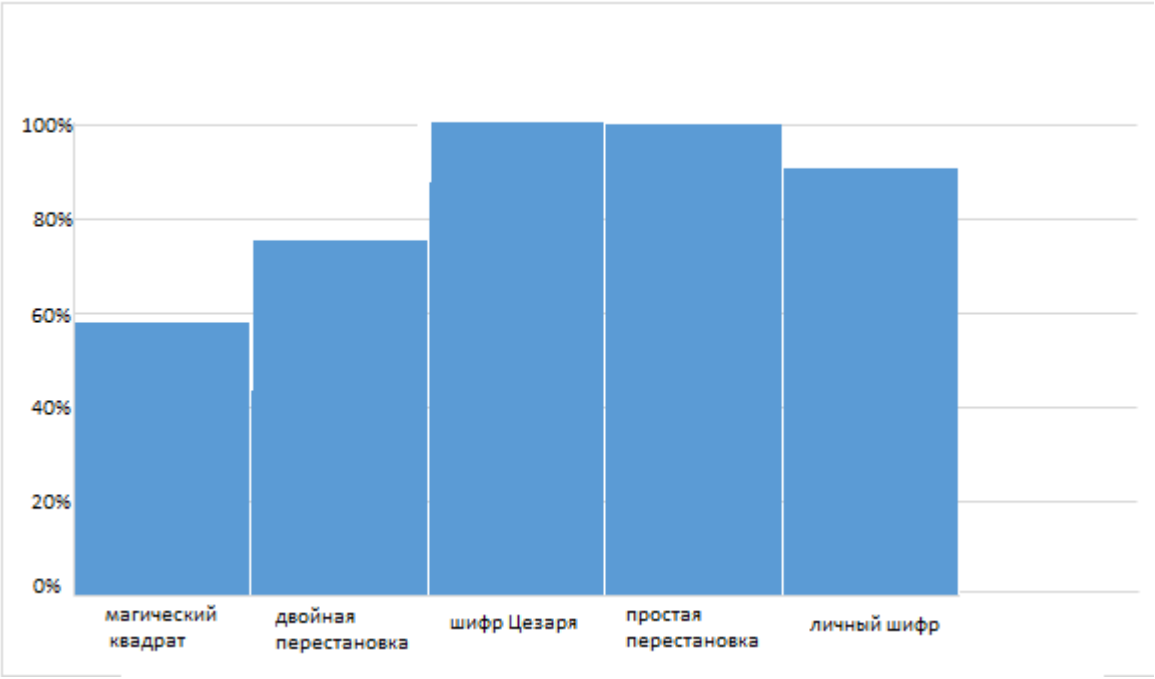
Исходный текст: «Параллельные прямые нигде не пересекаются»

Зашифрованный текст: "чжшжуумудхгм чшяфги хркли хи чишищисжёъщя»

Помимо изложенного выше, нами было проведено исследование шифров на криптостойкость. Все пять шифров были проверены на криптостойкость учащимися моего класса.

На уроке математики мы рассказали одноклассникам историю возникновения криптографии, рассказала о видах и известных способов шифрования. После чего раздали каждому ученику зашифрованные фразы и готовые шаблоны алфавита, магического квадрата, ключ и предложили ребятам самим расшифровать послания.

В ходе исследования было видно, что самым простым оказался шифр «шифр Цезаря». На втором: «Простая перестановка», здесь трудностей у ребят не возникло. На третьем месте оказался составленный мною шифр, он оказался легким в понимании, но занял больше времени в дешифровании чем «Простая перестановка». Четвертое место занимает «Двойная перестановка» и самым сложным для учеников 5 класса оказался шифр «Магический квадрат». Трудность тут возникла в понимании самого способа шифрования.



Из диаграммы видно какое количество учащихся справилось с заданием.

Заключение

В заключении нашей работы хотелось бы сказать, что в настоящее время для шифрования информации используют не только новые виды шифров, но и те, что были придуманы сотни лет назад. Шифрование будет актуальным во все времена, так как всегда будет информация, которую нужно скрыть от посторонних глаз. Также шифрование используется во многих сферах деятельности человека, можно даже сказать в любой, где используется ЭВМ и любая электроника.

В результате наших исследований мы пришли к выводу, что в наше время потребность в кодировании информации не менее актуальна, чем в былые времена. Шифруется дипломатическая и экономическая корреспонденция, военные сообщения и медицинские прогнозы, сенсационные сообщения прессы и информация биржевых маклеров. Поэтому изучаемая нами тема интересна, современна и актуальна. В процессе исследования нами была проделана следующая работа:

- Проанализирована и проработана литература по теме исследования;
- Рассмотрены и изучены различные виды шифрования;
- Представлена классификация шифров;
- Каждый шифр был испробован на практике;
- Разработан свой способ шифрования;
- Выполнено шифрование;

- Проверена криптостойкость шифров в результате исследования, проведенного в 5б классе.

Список литературы

1. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.
2. Анохин, М. И. Криптография в банковском деле [Текст] / М. И. Анохин.- М.: МИФИ, 1997. 231 с.
3. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.
4. Ященко В.В. Введение в криптографию. Москва. МЦНМО, 2012. 342

Интернет ресурсы

5. Основы криптографии [Электронный ресурс] **http://www.rbardalzo.narod.ru/kripto1.html**
6. Энциклопедия Википедия [Электронный ресурс] **http://citforum.ru/security/cryptography/yaschenko/1.html**