Информатика
Способы шифрования информации

Провёл исследование:
Ученик 10 Г класса
Руководитель: Ермакова Татьяна Григорьевна

Оглавление

ВВЕДЕНИЕ

Актуальность исследования: Еще до начала нашей эры была необходимость людьми сохранить информацию от посторонних глаз при ее передаче или хранении. В нашем времени в течение войн была необходимость зашифровать информацию во время ее передачи от противника. Сейчас, когда наш мир полностью поглощен интернетом и повсюду идет ее информация, тайно передавать важную информацию от мошенников встаёт очень актуальной и важной проблемой.
Изученность проблемы: На протяжении многих лет было много разных ученых криптологов, занимающихся как новыми и совершенными способами шифрования, так и дешифрованием важнейших исторических данных. Такими были Дэвид Кан, Дмитрий Витальевич Скляров, Фред Коэн. Что показывает актуальность данной проблемы у ученых в данной сфере.
Цель работы: Изучение истории криптографии и некоторых способов шифрования текстовой информации, с которых зарождалась сама криптография. Разработать программу по шифрованию текстовой информации на основе одного из способов шифрования, используя язык олимпиадного программирования.
Задачи работы:
-1)ознакомиться с материалом о зарождении и истории наук криптографии и криптоанализа.
-2)изучить способы шифрования текстовой информации;
-3)разработать программу для шифрования текстовой информации.
Объект исследования: криптография и криптоанализ.
Предмет исследования: способы шифрования текстовой информация.
Гипотеза исследования: если воспользоваться алгоритмом шифрования одного из изученных шифров и изученный язык олимпиадного программирования, то в конечном итоге мы сможем получить программу для шифрования текстовой информации.
Новизна работы: после изучения способов шифрования текстовой информации мы проведем проверку заинтересованности респондентов в олимпиадном программировании или в такой науке как криптография и создадим программу для шифрования текстовой информации на основе полиалфавитного шифра.
Актуальность и значимость исследования: программа для шифрования текстовой информации позволит людям быстро и удобно шифровать текст для некоммерческого использования, исключительно для индивидуального развлечения и увлечения в тайнописи между людьми или группами людей

История криптографии

- История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования.
- Первый период (приблизительно с 3-го тысячелетия до н. э.) характеризуется господством моноалфавитных шифров (основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).
- Второй период (хронологические рамки — с IX века на Ближнем Востоке (Ал-Кинди) и с XV века в Европе (Леон Баттиста Альберти) — до начала XX века) ознаменовался введением в обиход полиалфавитных шифров.
- Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.
- Четвёртый период — с середины до 70-х годов XX века — период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости для различных известных атак — линейного и дифференциального криптоанализа. 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. Правовое регулирование использования криптографии частными лицами в разных странах сильно различается — от разрешения до полного запрета.
- 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 (включая цифровые подписи), телекоммуникации и других.

Шифр Цезаря

- **Шифр Цезаря**, также известный как **шифр сдвига**, **код Цезаря** или **сдвиг Цезаря** — один из самых простых и наиболее широко известных методов шифрования.
- Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.
- Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.
- Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и всё ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет почти никакого применения на практике.
- Шифрование с использованием ключа . Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее:
- Исходный 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
- Шифрованный: 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 А Б В
- Оригинальный текст:
- Съешь же ещё этих мягких французских булок, да выпей чаю.
- Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:
- Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб.

Азбука Морзе

- Все мы слышали об Азбуке Морзе, которую более века использовали военные и гражданские специалисты в области связи. Изобрел ее американец Сэмюэл Финли Бриз Морзе в 1838 году.
- Вначале она применялась в специальных телеграфных аппаратах (которые к слову тоже изобрел Сэмюэл Морзе) для осуществления передачи и приема сообщений посредством телеграфной связи. На одном конце провода находился передатчик, так называемый телеграфный ключ, а на другом – электромагнитный приемник, который осуществлял управление механизмом, пишущим на бумажную ленту.
- Данный аппарат практически в неизменном виде просуществовал с конца 30-х годов XIXстолетия до середины XX века. Да, конечно, он модернизировался с развитием научно-технического прогресса, но основная технология не менялась.
- Азбука Морзе представляет собой телеграфный код. Каждая буква алфавита, цифра или знак обозначаются серией коротких или длинных включений электрического тока. Короткие включения — это точки, длинные – тире.
- В телеграфии неравномерный код Морзе был заменен равномерным кодом, однако даже в настоящее время энтузиасты радиолюбители используют Азбуку Морзе для общения. Телеграфная азбука, «Морзянка» — так называют изобретение Сэмюэла Морзе.

Азбука Морзе

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

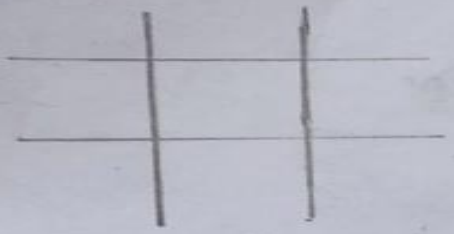
Шифр Американских школьников

- В Американских школах популярен шифр с помощью геометрических фигур и частей клеток,в первый раз его показали на сайте Пикабу

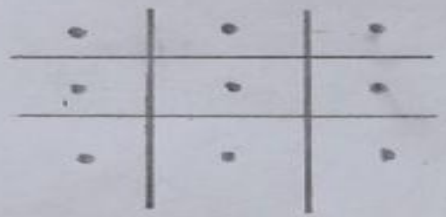
Мой шифр

- В своей проектной работе я решил русифицировать данный шифр и сделать его более популярным у учеников. Вот как он будет выглядеть

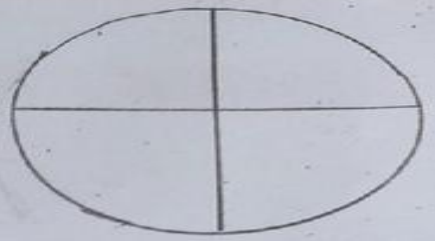
ШИФР ДЛЯ ТАЙНЫХ ПОСЛАНИЙ.



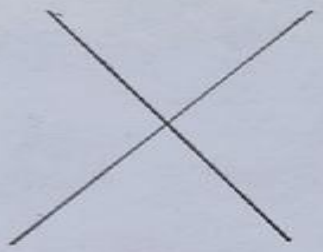
А Б В
Г Д Е
Ж З И



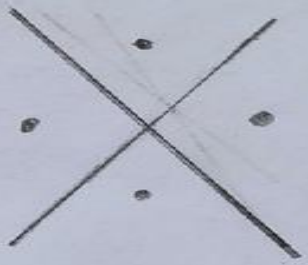
К Л М
Н О П
Р С Т



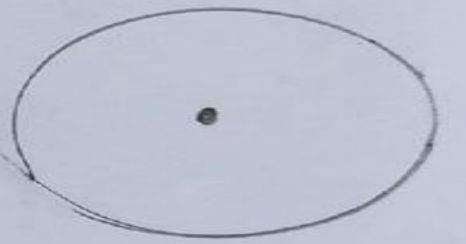
Ы Ъ
Э Ю



Ф
У Х
Ц



Ш
Ч Щ
Ь



Я

ПРИМЕР:

МЕНЯ – ЗОВУТ – ГЕОРГИЙ

ЬСЭЮ – ПШЦЖ – ЗСШЛЗГЙ

Вывод

- В своей проектной работе я затронул одну из интересных для меня тем-Шифрование,в качестве продукта я получил закодированное предложение,я считаю,что в будущем шифры будут ещё более распространёнными.

Список доп.литературы

- Фомичёв В. М. Дискретная математика и криптология: Курс лекций / под ред. Н. Д. Подуфалов — М.: Диалог-МИФИ, 2013. — 397 с. — ISBN 978-5-86404-185-7
- Суляев Х.Е.; М.: Детгиз, 1948.- 32 с.

Спасибо за внимание