ОГАОУ ОК «Алгоритм Успеха»

ИНДИВИДУАЛЬНЫЙ ИТОГОВЫЙ ПРОЕКТ НА ТЕМУ

«От тайности к криптографии»

Выполнил:
Мирошниченко Денис Андреевич
Ученик 9 “А” класса
Руководитель проекта:
Гарус Михаил Юрьевич
Учитель математики
ОГАОУ ОК «Алгоритм Успеха»

Оглавление:

Введение

После изученного списка литературы мною была выбрана в качестве проектного исследования тема «От тайности к криптографии». Данная тема мне интересна, так как она тесно связана с математикой и информатикой, а также с информационной безопасностью.

Моя работа является актуальной, так как с давних времен и по сей день люди использовали, используют и будут использовать криптографию, хотя во все времена её применения значительно отличались. Также мне показалось интересным узнать, как люди и известные личности в древности шифровали свои послания.

Цель моей исследовательской работы – изучить то, как сильно изменилась криптография с древних времён и узнать какое сейчас для неё есть применение.

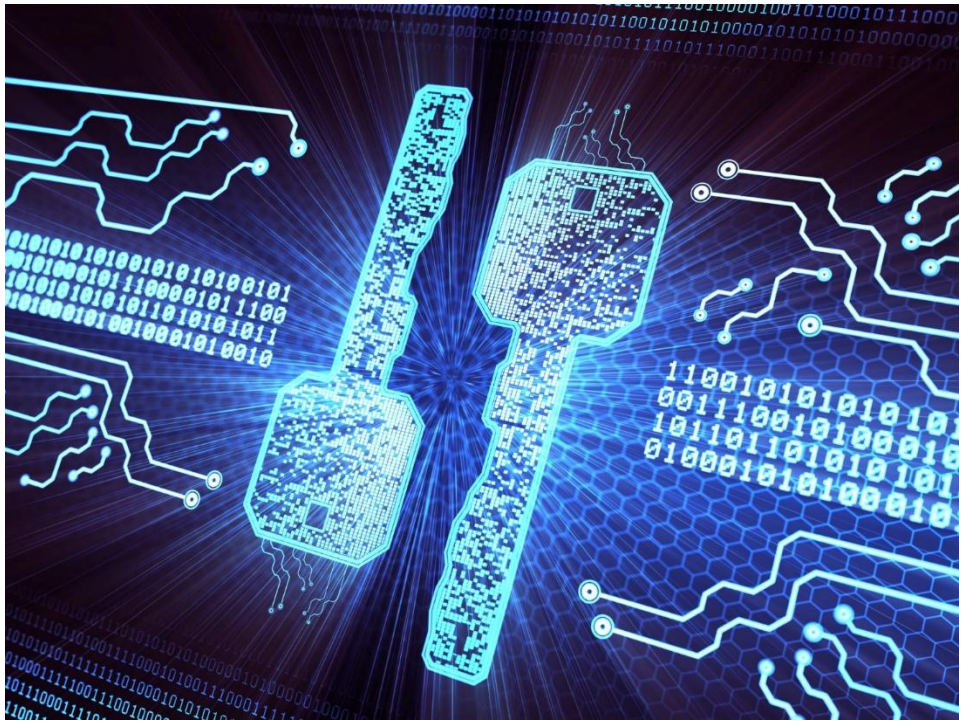
Объектом моего исследования является – история применения шифрования с древних времен и по наши дни.

Предмет исследования – популярные шифры

Глава 1. Теоретический блок:

1.1. Криптография и её применение

Криптогра́фия — наука о математических методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.



Криптография в свою очередь решает такие задачи как:

- Конфиденциальность – чтобы человек, который перехватил данные во время их передачи не смог узнать содержание.
- Целостность – чтобы получатель был уверен, что сообщение не было переписано или как-либо изменено треть ей стороной.
- Аутентификация – чтобы получатель сообщения был уверен, что сообщение пришло от определенной стороны, а не от кого-либо ещё.
- Отказ от ответственности – чтобы предотвратить отказ отправителя за свою причастность к отправлению или созданию файла.

1.2. Криптография в древнем мире и её развитие

- Первым известным применением криптографии принято считать использование Египетскими писцами специальных иероглифов около 4000 лет назад. Она использовалась писцами со стремлением превзойти друг друга в остроумии и оригинальности, а также для привлечения к своим творениям, а не для усложнения чтения.

Атбаш- это довольно простой шифр подстановки для алфавитного письма, упоминания о котором впервые появились в священных иудейских книгах, в том числе в книге пророка Иеремии. Он является очень простым в использовании, но и настолько же простым в дешифровке.

Формула шифрования: n-i+1, где n – количество букв в алфавите, а i – последовательность выбранной буквы в этом алфавите.

Исходный текст	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Зашифрованный текст	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

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

Исходный текст	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Зашифрованный текст	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Ещё одним известным шифром является Скитала, которую придумали и применяли в древней Спарте. С помощью неё в Спарте доставляли тайные послания. Суть заключалась в деревянном стержне, который нужно было обернуть специальной лентой из пергамента, на котором были написаны символы или же буквы. На ленту наносился текст вдоль оси скиталы, так, что после разматывания он становился нечитаемым. Для дешифровки нужна была скитала с определённым количеством граней и размером. Но несмотря на это способ был не сильно надёжным.

Квадрат Полибия

Одним из моих любимых древних шифров является Квадрат Полибия. Суть этого шифра заключается в абсолютной замене букв на какие-либо цифры или буквы. К каждому языку отдельно составляется таблица шифрования с одинаковым количеством строк и столбцов, параметры которой зависят от количества букв в алфавите. Для составления таблицы необходимо взять два целых числа, которые ближе всего к количеству букв в алфавите (например, для Русского алфавита можно взять квадрат 6*6, пустые клетки можно заменить оставшимися цифрами, если оно того требует, а если клеток будет не хватать, то можно поместить две буквы в ячейку). Позже я покажу действие этого шифра на практике.

Шифр Цезаря

Также существует шифр сдвига, который придумал сам Цезарь, который использовал его для секретных переписок. Этот тип шифра довольно простой в освоении и настолько же ненадёжный. Суть зависит в сдвиге алфавита на определённое количество букв. Для каждого случая составляется таблица, состоящая из двух строк и такого количества столбцов, сколько букв в выбранном алфавите. Слабость шифра состоит в том, что, чтобы дешифровать послание перебором даже для английского алфавита в худшем случае понадобится 25 попыток.

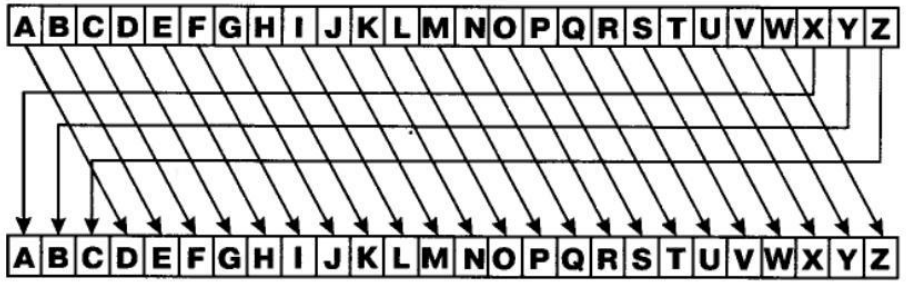
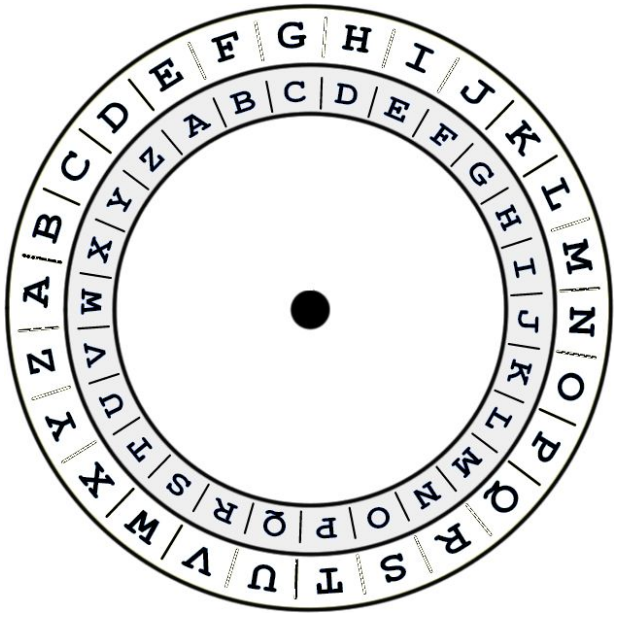
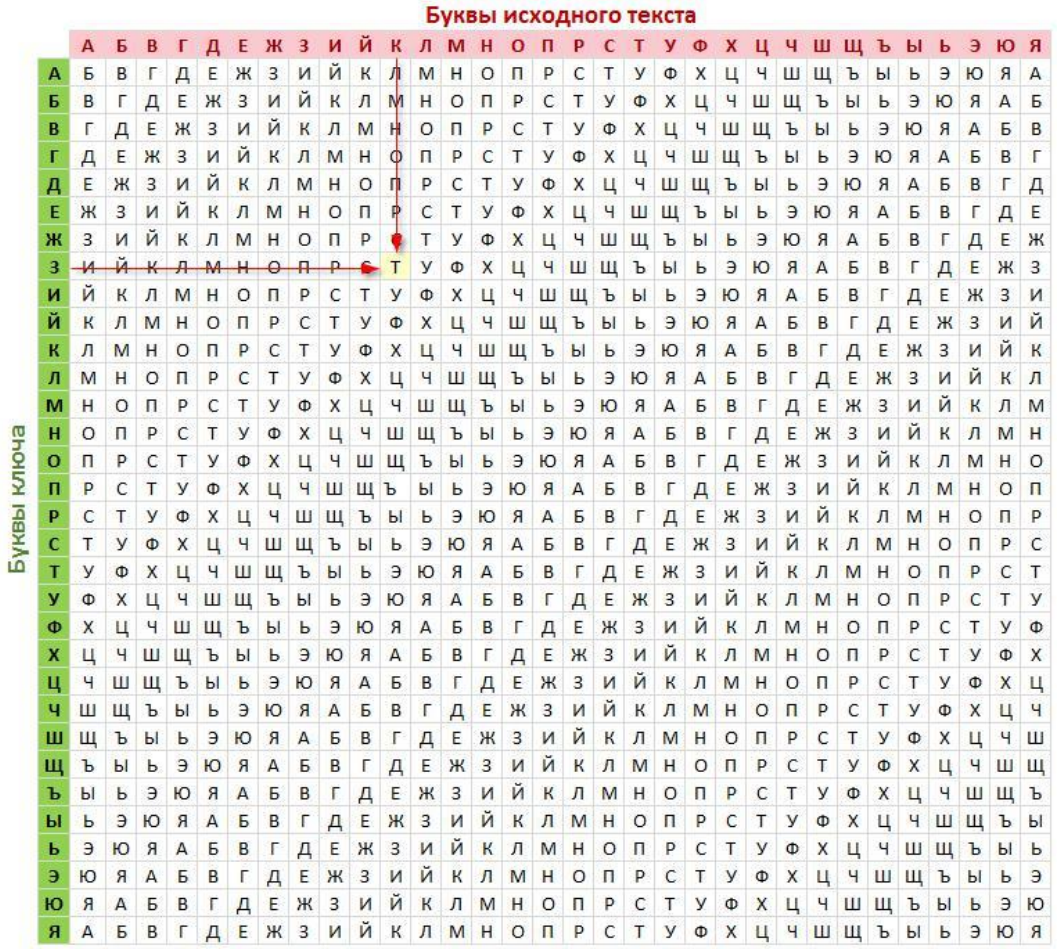


Рис. 2.3. Шифр Цезаря



Шифр Виженера

На смену шифру Цезаря пришел шифр Виженера, который являлся усовершенствованным шифром сдвига. Шифр Виженера отличается тем, что состоит из последовательности нескольких шифров Цезаря с разными значениям сдвига. Для шифрования обычно используется квадрат. Размеры квадрата зависят от мощности алфавита, который взят. Например, для латинского алфавита он будет размером 26X26. Подробнее об этом и как применять эти шифры я покажу в практической части.



1.3. Криптография в наше время

Симметричный вид шифрования – это вид шифрования, в котором для шифровки и дешифровки используется один и тот же ключ. Этот ключ закрытый и является общим как для отправителя, так и для получателя. Данный вид начал использоваться очень давно, еще со второй мировой войны. Проблема симметричного шифрования заключается в передаче ключа от отправителя к получателю, так как для дешифровки, как я и писал ранее нужен один и тот же ключ. Передавать ключ в переписках или по e-mail не является безопасным, так как во время передачи ключа, злоумышленники спокойно могут его перехватить и в будущем использовать этот ключ в своих целях. Поэтому для этого вида используются защищённые каналы связи, однако для обычного человека найти этот канал проблематично.

В этом случае нам может прийти более новый и безопасный способ – Ассиметричный. Для применения этого вида используется уже два ключа. Отправитель шифрует сообщение публичным ключом, а получатель дешифрует личным закрытым ключом. С помощью открытого публичного ключа возможно только шифровать сообщение, но не дешифровать. После шифровки сообщения публичным ключом, человек, который это сделал не сможет дешифровать сообщение этим же ключом, а поэтому этот способ и является более безопасным. Чтобы объяснить действие ассиметричного шифрования я как пример взял почтовый ящик. Абсолютно каждый может положить в него письмо, но никто, кроме получателя забрать его оттуда не может. Таким образом становится очевидно, что переписки, например, в Telegram работают полностью с помощью ассиметричного способа шифрования. Каждый может отправить сообщение, но прочитать его может только получатель. (Как пример я привёл Telegram, потому что официально известно, что это один из немногих мессенджеров, который предоставляет полную анонимность переписки для посторонних лиц, в отличие от остальных). Более подробно об ассиметричном виде шифровки я расскажу и покажу в практической части этого проекта.

Глава 2. Практический блок:

2.1. Квадрат Полибия

Шифр: Квадрат Полибия

Алфавит: Латинский

Фраза для шифрования: Hello World

Таблица: 6x6

	1	2	3	4	5	6
1	A	B	C	D	E	F
2	G	H	I	J	K	L
3	M	N	O	P	Q	R
4	S	T	U	V	W	X
5	Y	Z	0	1	2	3
6	4	5	6	7	8	9

2.2.Шифр цезаря и Шифр Виженера

Шифр: Шифр Цезаря

Алфавит: Русский

Фраза для шифрования: Криптография – это интересно

Смещение: 7 символов

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
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	Г	Д	Е	Ё

Шифр: Шифр Виженера

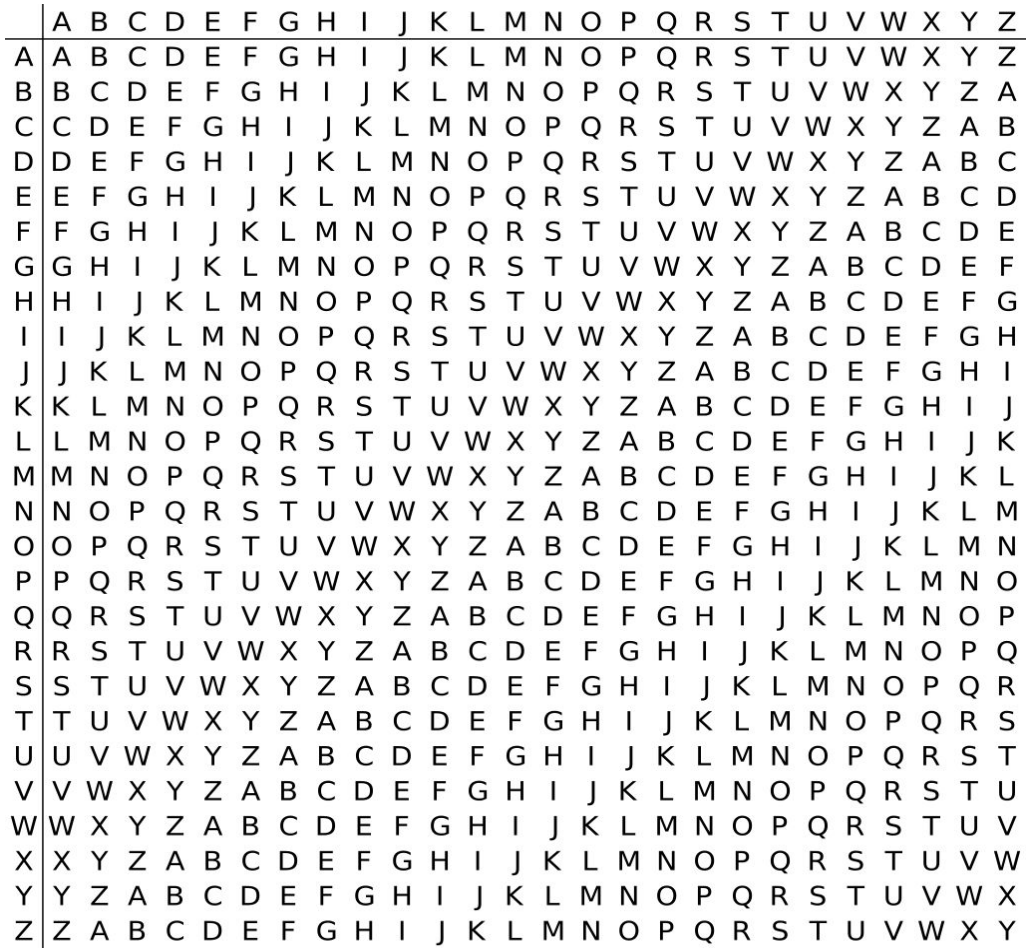
Алфавит: Латиница

Фраза для шифрования: Hello World

Исходный текст: HELLOWORLD

Ключ: APPLEAPPLE

Таблица: 26x26



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

2.3.
Атбаш

Ciphertext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plainrtext Alphabet	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Шифр: Атбаш

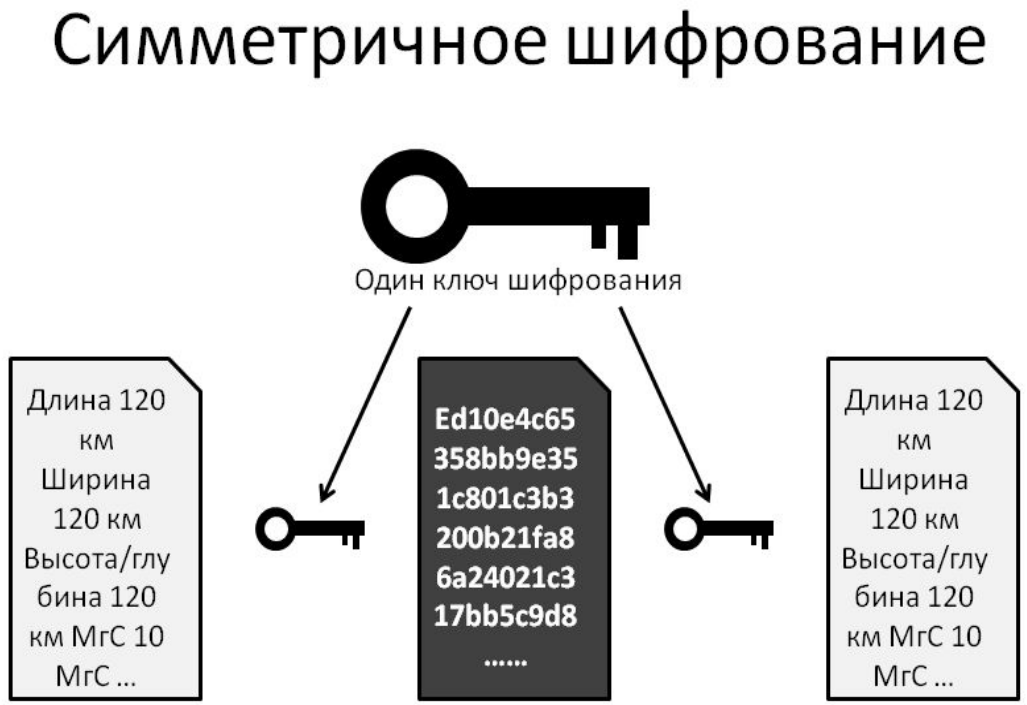
Алфавит: Латиница

Фраза для шифрования: Hello World

Формула: n-i+1

2.4. Симметричный вид шифрования

Задача: Объяснить действия симметричного вида шифрования, привести примеры его применения и показать как Объекту А предать файл Объекту В.



2.5. Асимметричный вид шифрования

Задача: Объяснить действия асимметричного вида шифрования, привести примеры его применения и показать как Объекту А предать файл Объекту В.

Заключение

Вашему вниманию была представлена исследовательская работа по теме «От тайности к криптографии». Криптография носит огромный вклад в развитие современного общества, потому что она активно борется с мошенничеством и ограблениями в интернете и в нашей повседневной жизни. Мною были проиллюстрированы фотоснимки и описаны примеры ситуаций от древней и до современной жизни с применением криптографии. Это еще раз подчеркивает то, что математика и информатика окружают нас повсюду и являются неотъемлемой частью нашей жизни. И благодаря моему исследованию, которое выходит за пределы изучения школьной программы, я понимаю, когда и где я смогу применить эти знания на практике.

Я считаю, что я достиг той цели, которую я ставил в начале своей работы. В ходе работы я сильно заинтересовался темой проекта и возможно этот опыт даст мне толчок к поиску моей будущей профессии.

Список литературы

1. https://science.wikia.org/ru/wiki/Криптография#:~:text=Криптогра́фия%20(от%20греч.%20κρυπτός%20—,невозможности%20отказа%20от%20авторства)%20информации
2. https://yandex.ru/turbo/psiheya-market.ru/s/stati/nauka-2/chto_takoe_kriptografiya_i_gde_ona_primenyaetsya
3. https://tproger.ru/translations/understanding-cryptography/
4. https://ru.wikipedia.org/wiki/История_криптографии#Математическая_криптография
5. https://pikabu.ru/story/starinnyie_metodyi_shifrovaniya_6108284
6. https://youtu.be/pVEyQRZdF2U?t=278
7. https://cryptoworld.su/lesons-of-cryptography-1/#lwptoc4
8. https://webnewsite.ru/kriptografiya-dlya-chajnikov/#Криптография_в_повседневной_жизни
9. https://www.youtube.com/watch?v=sGFbM-X6W_4
10. https://ru.wikipedia.org/wiki/Шифр_Виженера
11. https://pikabu.ru/story/prakticheskoe_primenenie_asimmetrichnoy_kriptografii_ili_kak_otpravlyat_lichnyie_soobshcheniya_na_pikabu_7734836
12. https://www.youtube.com/watch?v=2CwsoGw2coc
13. https://forexdengi.com/threads/133197-kakie-bivayut-tipi-shifrovaniya-informatsii?thread_type=0&p=19906277

Спасибо за внимание