



# Содержание

1. Введение
2. Теоретическая часть
3. Практическая часть
4. Заключение
5. Развитие темы
6. Библиографический список

# Введение



Имя	Возраст	Пол	Рост	Вес	Цвет волос	Цвет глаз	Дата рождения	Место рождения	Уровень образования	Профессия	Стаж	Зарплата	Семейное положение	Количество детей	Средний балл
Иван	35	М	180	75	Светлый	Синие	1985-05-15	Москва	Высшее	Инженер	10	120000	Женат	2	4.5
Петр	42	М	175	80	Темный	Серые	1978-03-22	Санкт-Петербург	Среднее	Рабочий	25	80000	Женат	1	3.8
Анна	28	Ж	165	55	Светлый	Зеленые	1992-08-10	Новосибирск	Высшее	Учитель	5	90000	Не замужем	0	4.2
Сергей	50	М	185	90	Седые	Голубые	1970-11-05	Казань	Среднее	Пенсионер	30	60000	Женат	3	3.5
Елена	38	Ж	170	65	Темный	Карие	1980-02-18	Владивосток	Высшее	Адвокат	15	150000	Женат	1	4.8



Тысячи лет короли управляли, опираясь на эффективно действующую связь и осознавая последствия того, что произойдет, если жизненно важная информация окажется у противника. И именно опасение того, что враги перехватят сообщение, послужило причиной создания кодов и шифров.

Я же взял данный проект потому, что мне было интересно, как создаются шифры.

IJ] > 0 L + 0 # > + # L I L V J  
 0 # 0 c 0 u 0 > 0 n n c - >  
 - u l # # > # c 0 # # L 0 n J >  
 J > + # n v + 0 # 0 > 0 c # L > v  
 c # 0 # - # > n J # > 0 c #  
 n J > + 0 # L > 0 n + 0 #  
 + # # > # n > #  
 + L n > ( c # # # )



J, Z, 7, U, O, n, O,  
 a, b, c, d, e, f, g,

n, U, L, L, F, H, /,  
 h, i, j, k, l, m, n,

~, 7, T, /, /,  
 o, p, q, r, s,

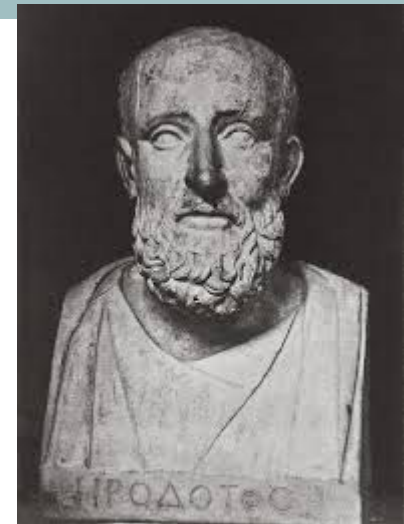
/, X, /, /, /, /,  
 u, v, x, y, z. n

Целью данного проекта является объяснить одноклассникам, как создаются шифры и создать свой шифр.

# Теоретическая часть

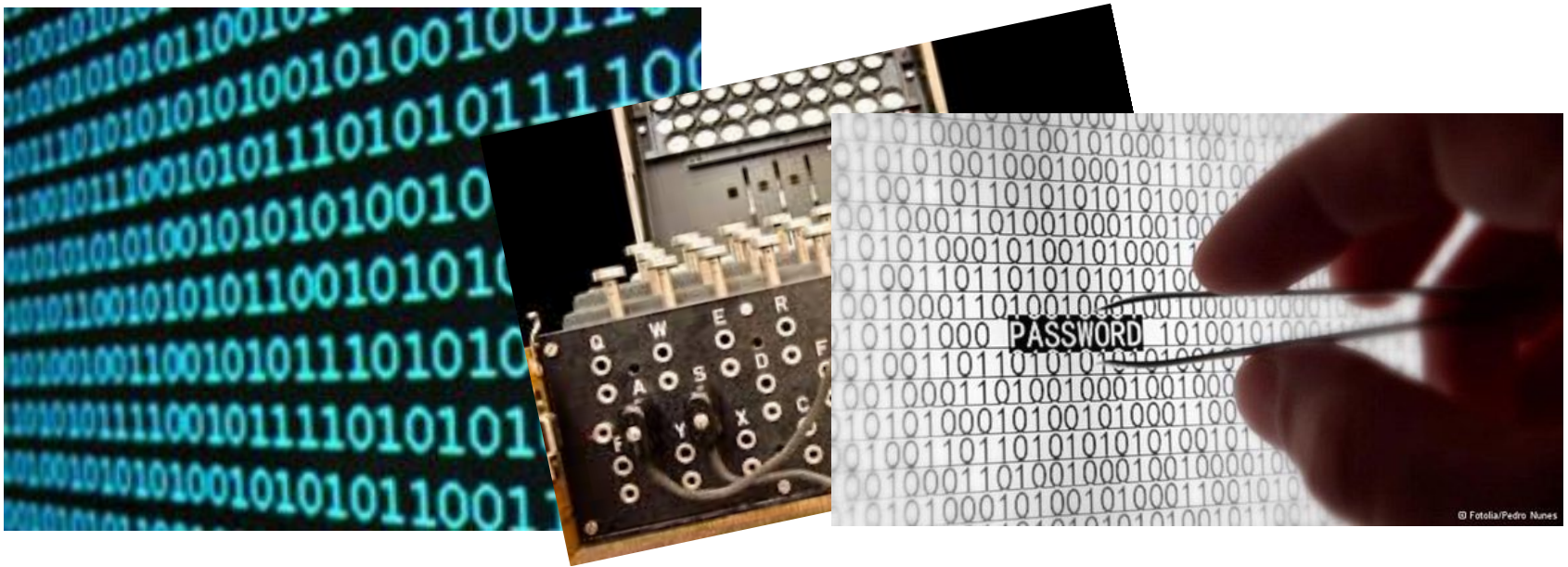


Ксеркс. Царь Персии.



Геродот. «Отец истории»

Некоторые из наиболее ранних упоминаний о тайнописи восходят еще к Геродоту, греческому историку. Геродот повествовал о вооруженных столкновениях между Грецией и Персией в V веке до н. э. Согласно его книге, именно искусство тайнописи спасло Грецию от порабощения Ксерксом, деспотичным правителем Персии.



Непрекращающаяся борьба между создателями и взломщиками шифров содействовала появлению целого ряда замечательных научных открытий. В своих усилиях разрушения и сохранения секретности обе стороны привлекали самые разнообразные научные дисциплины и методы. Взамен же они обогатили эти предметы, а их профессиональная деятельность ускорила научно-технический прогресс.

# Криптография



Криптография - от *kryptos*, «тайный». Цель криптографии состоит не в том, чтобы скрыть наличие сообщения, а в том, чтобы скрыть его смысл, — процесс, известный как шифрование. Чтобы сделать сообщение непонятным, оно зашифровывается по определенному правилу.

АЕКНО				
АГЗОР				
АГЕЛН				
АИНОС				
РТТУЬ				
ААВКС				
АЗНТЬ				
ВИОТЧ				
АДЙНО				

14	17	11	24	1	5	3	28
23	19	12	4	26	8	16	7
41	52	31	37	47	55	30	40
44	49	39	56	34	53	46	42

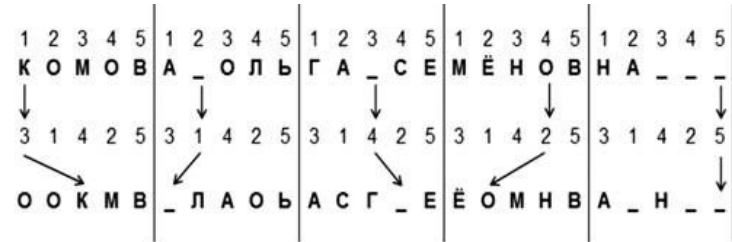
Таблица II.4. DES — перестановка б

32	1	2	3	4	5	4	5
8	9	10	11	12	13	12	13
16	17	18	19	20	21	20	21
24	25	26	27	28	29	28	29

Таблица II.5. DES — перестановка

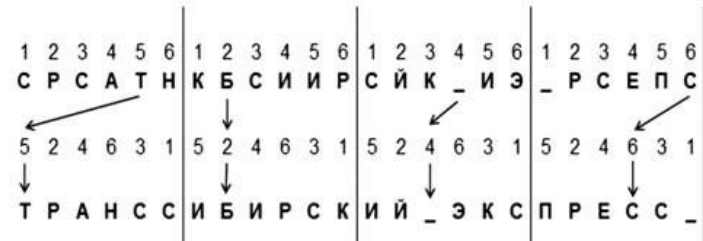
а

Б А Н А Н  
3 1 4 2 5



б

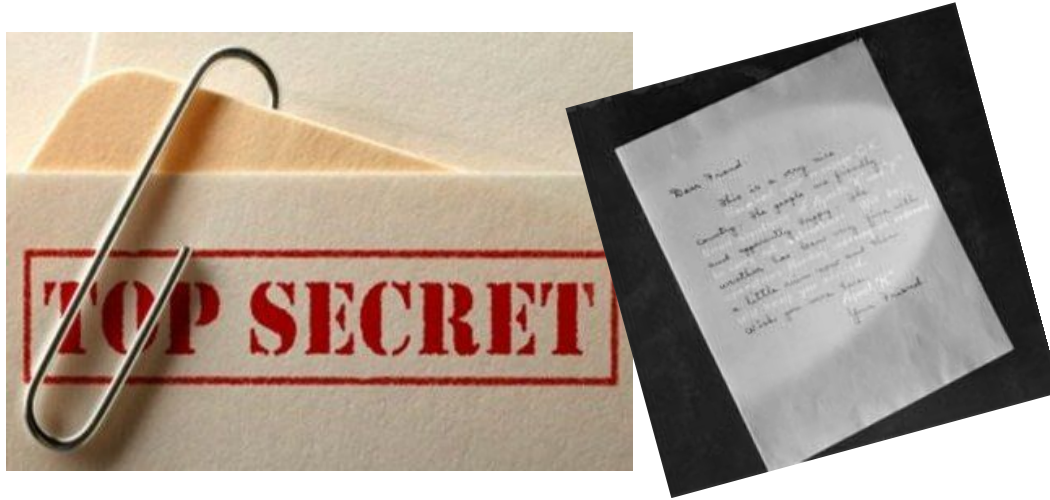
З В Е З Д А  
5 2 4 6 3 1



Криптография разделена на два направления, известные как перестановка и замена. При перестановке буквы сообщения просто переставляются, образуя анаграмму. Для очень короткого сообщения такой способ весьма ненадежен, поскольку существует крайне ограниченное число возможных способов перестановки горстки букв. Так, три буквы могут быть расставлены шестью различными способами. Однако по мере увеличения количества букв число возможных перестановок стремительно растет, и восстановить исходное сообщение становится невозможным. Если в предложении содержится всего 35 букв, то число их различных перестановок составляет более 50 нониллионов.



# Стеганография



Стеганография – от *steganos*, «покрытый», и *graphein*, «писать». В течение двух тысячелетий после Геродота во всем мире применялись различные виды стеганографии. Например, древние китайцы писали сообщения на тонкой шелковой ткани, которая затем сворачивалась в крохотный шарик и покрывалась воском, после чего посланец проглатывал этот восковой шарик.

## Скитала



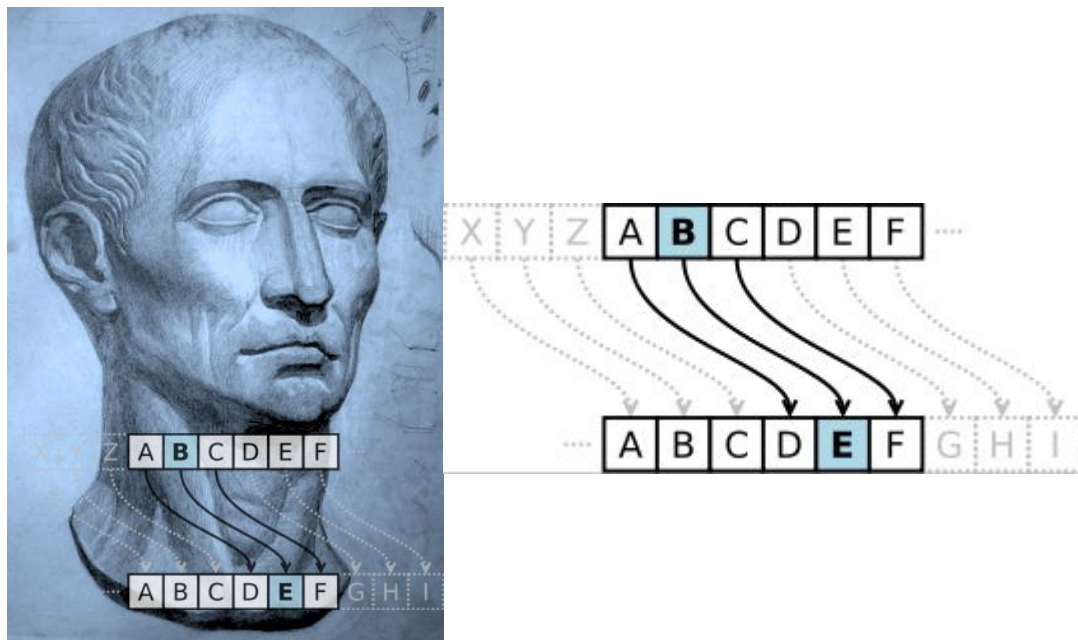
Самое первое из известных шифровальных устройств — спартанской скитала - представляла собой деревянный цилиндр, вокруг которого наматывалась полоска кожи или пергамента. Отправитель писал сообщение по всей длине скиталы, а затем разматывал полоску, на которой после этого оставался бессмысленный набор букв. Вестник брал кожаную полоску и прятал сообщение, то есть кроме зашифровывания применял также и стеганографию. Чтобы получить исходное сообщение, адресат просто наматывал полоску кожи вокруг скиталы того же диаметра, что и скитала, которой пользовался отправитель.

Увеличенная микроточка с информацией



Хотя криптография и стеганография являются независимыми, но для обеспечения максимальной секретности можно пользоваться обеими. К примеру, во время Второй мировой войны стала популярной микроточка, которая является одним из видов стеганографии. Германские агенты фотографическим способом сжимали страницу текста в точку диаметром менее 1 миллиметра, а затем прикрепляли эту микроточку поверх обычной точки в конце предложения в на первый взгляд совершенно безобидном письме.

## Шифр Цезаря



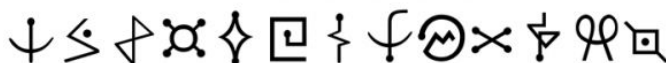
Первое использование шифра замены появилось в «Галльских войнах» Юлиа Цезаря. Цезарь описывает, как он послал сообщение Цицерону, находившемуся в осаде и бывшему на грани капитуляции. В этом письме латинские буквы были заменены греческими, поэтому враг его не смог бы понять.

У нас имеется подробное описание одного из видов шифра замены, применявшегося Юлием Цезарем. Он просто заменял каждую букву в послании буквой, стоящей в алфавите на три позиции дальше.

  
 А Б В Г Д Е Ж З И К Л М

  
 Н О П Р С Т У Х Ъ Э Я



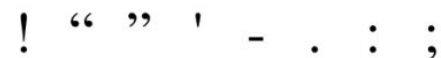


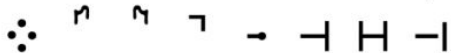



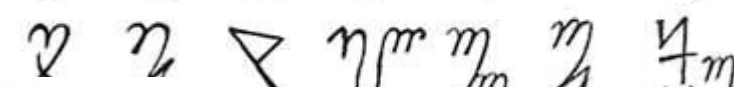










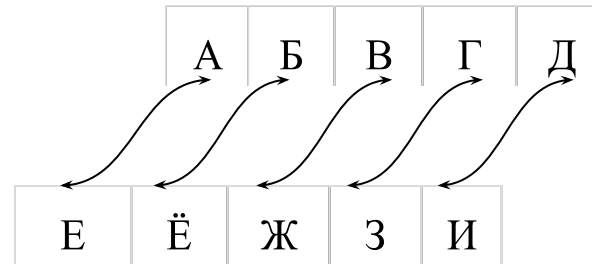
  
 К Л М N O P Q  
  
 R S T U V W X Y Z Ω

Citramon.NET

Алфавит открытого текста - алфавит, используемый для создания исходного сообщения, и шифралфавит, буквы которого подставляются вместо букв алфавита открытого текста.



1. Я заменю букву, на отстоящую от неё на 5 позиций.



2. А так же составлю специальную таблицу, в которую и запишу текст, полученный методом перестановки.

Таким образом получаю текст, зашифрованный два раза!

# Зашифровка

Фраза для зашифровки: «Встречаемся в семь там же».

После перестановки получается следующее: «Жйчхйьейсйд и цйсб чес лй».

Убираем пробелы и заглавные буквы:  
«жйчхйьейсйдйцйсбчеслй».

Вставляем всё в таблицу шириной 7 клеток:

ж	й	ч	х	й	ь	е
й	с	й	д	и	ц	й
с	б	ч	е	с	л	й

Записываем текст списывая столбики слева направо снизу вверх: «сйжбсйчйчедхсийлцьййе».



# Заключение

Создав свой шифр, я выполнил одну из своих целей, но я не объяснил, как они создаются, рассказав лишь об основных терминах и первых шифрах.

Вывод: я выполнил 1 из 2 целей.

## Развитие темы

В будущем я планирую дополнить этот проект теоретическим материалом и создам новый, более совершенный шифр.

# Спасибо за просмотр!

Список использованной литературы:

С. Саймон - Книга шифров. Тайная история шифров и их расшифровки