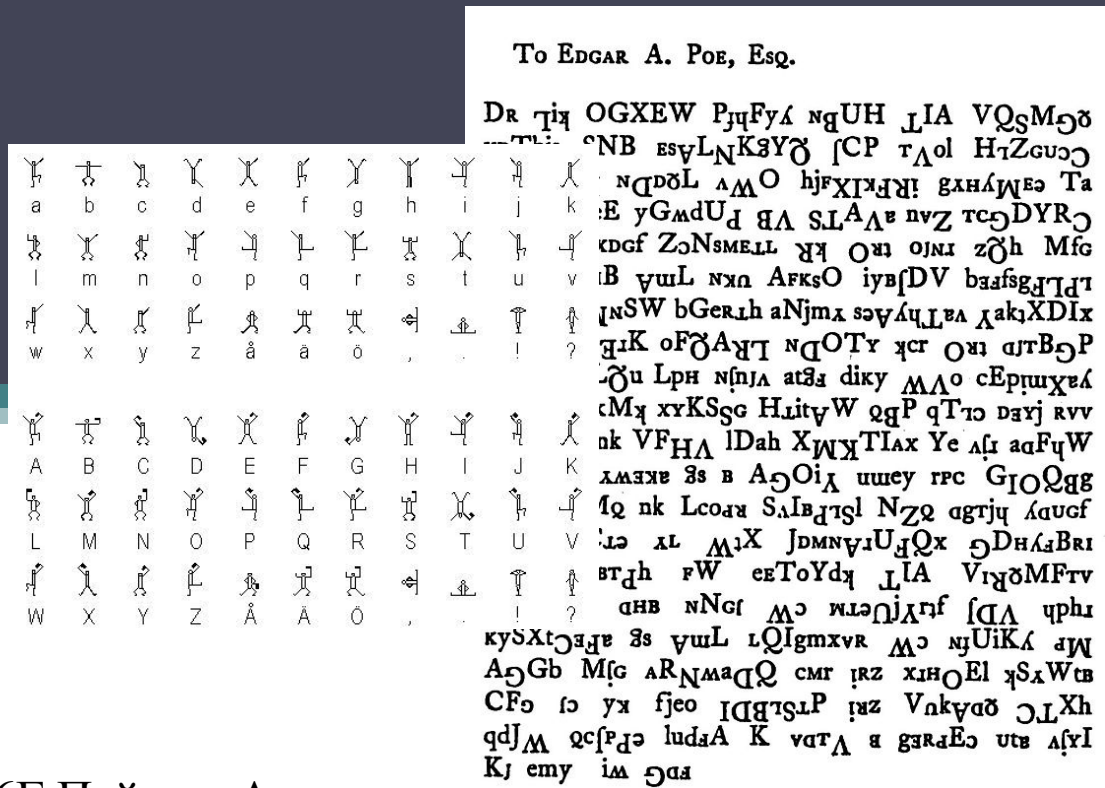
Шифры и коды



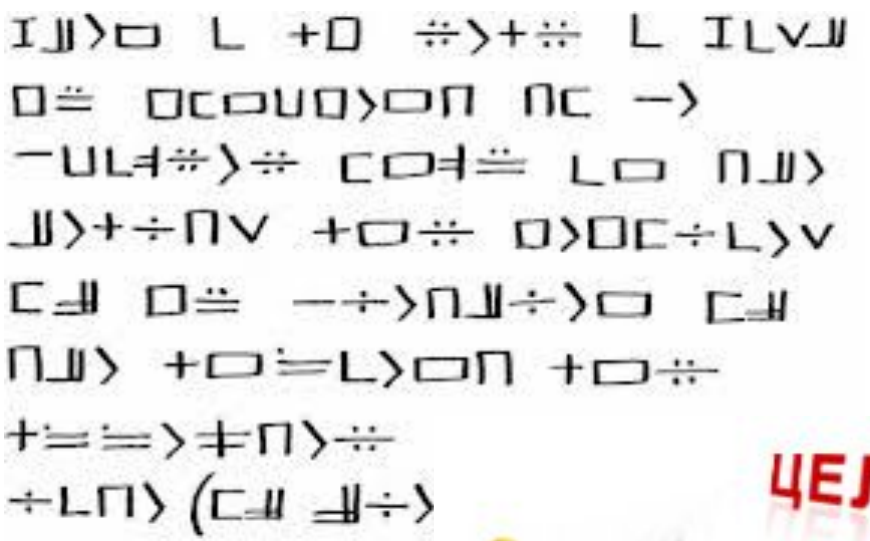
Подготовил ученик 6Г Паймин Антон
г.о. Железнодорожный
2014

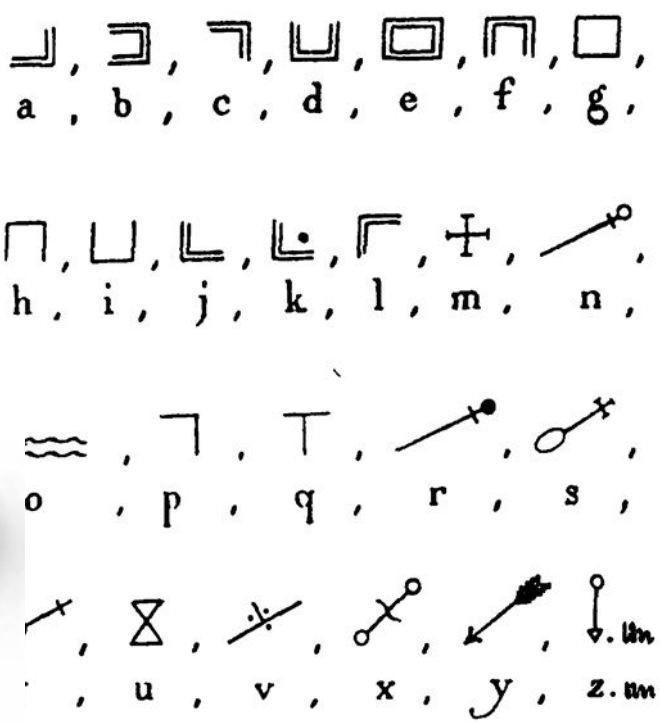
Содержание

Введение

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.

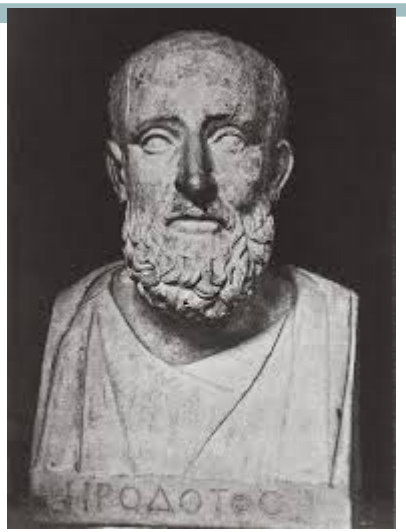




Целью данного проекта является объяснить одноклассникам, как создаются шифры и создать свой шифр.

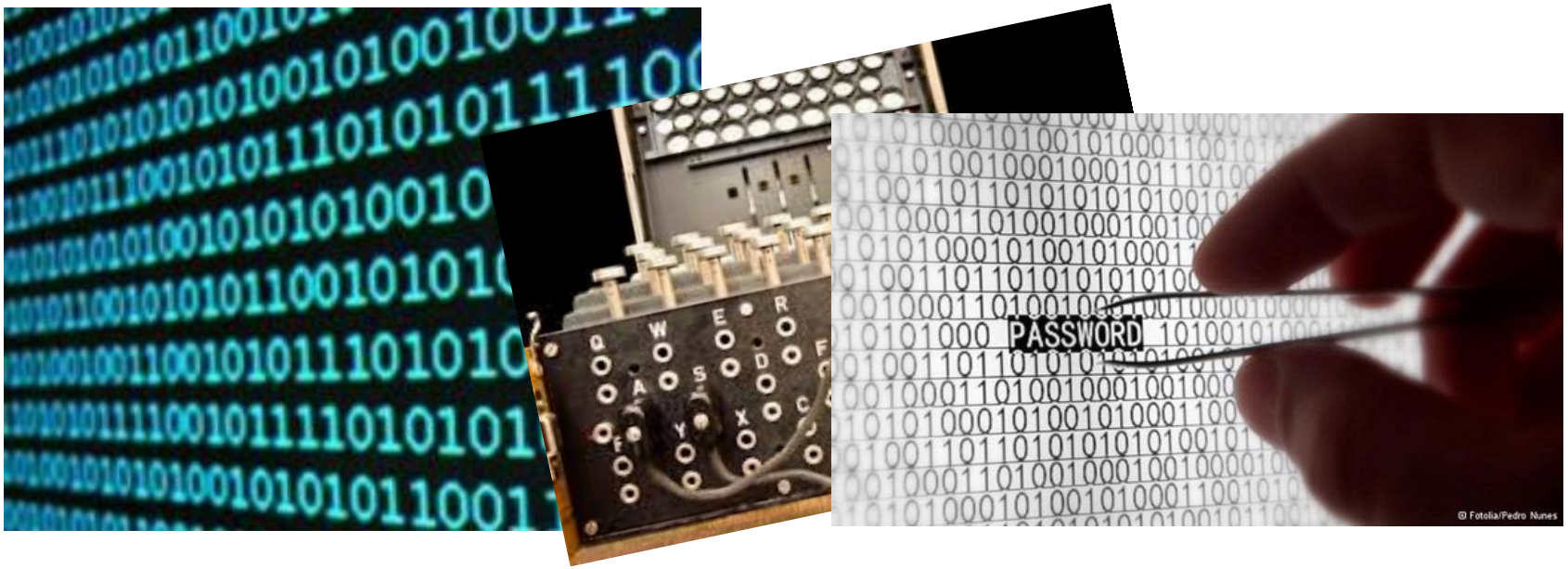
Теоретическая часть

Ксеркс. Царь Персии.



Геродот. «Отец истории»

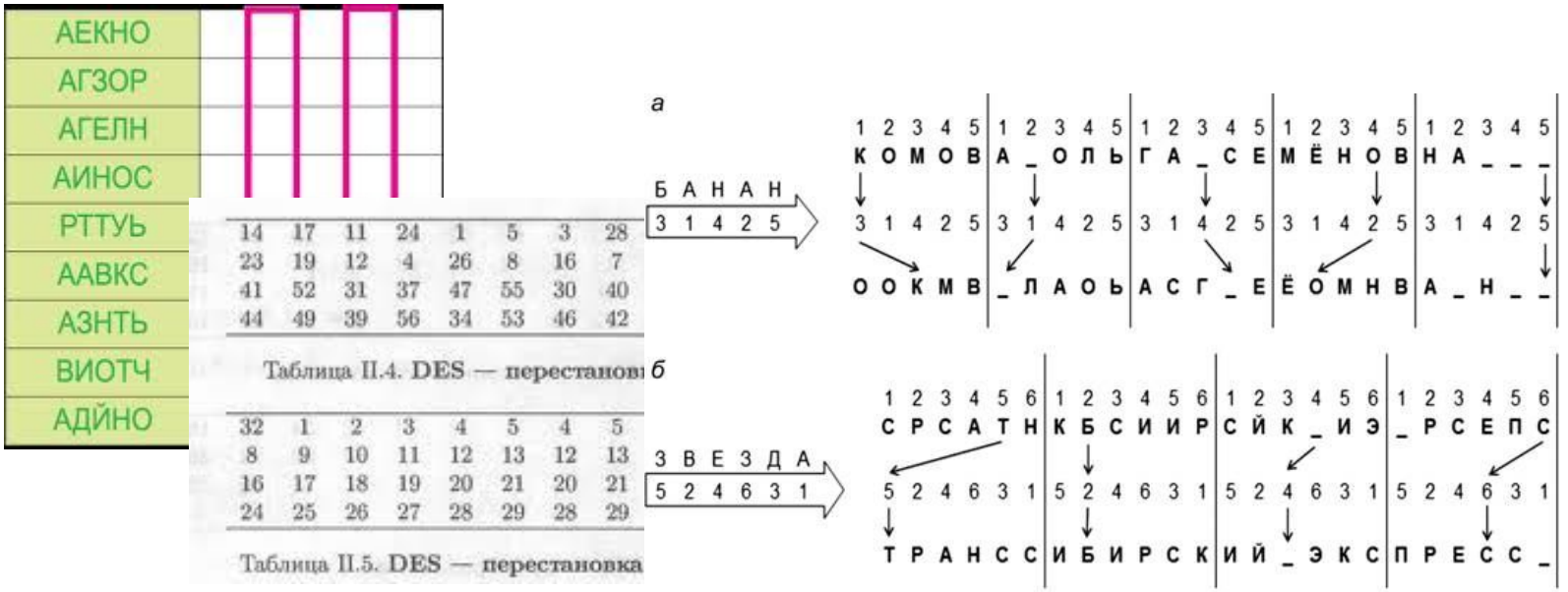
Некоторые из наиболее ранних упоминаний о тайнописи восходят еще к Геродоту, греческому историку. Геродот повествовал о вооруженных столкновениях между Грецией и Персией в V веке до н. э. Согласно его книге, именно искусство тайнописи спасло Грецию от порабощения Ксерксом, деспотичным правителем Персии.



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.

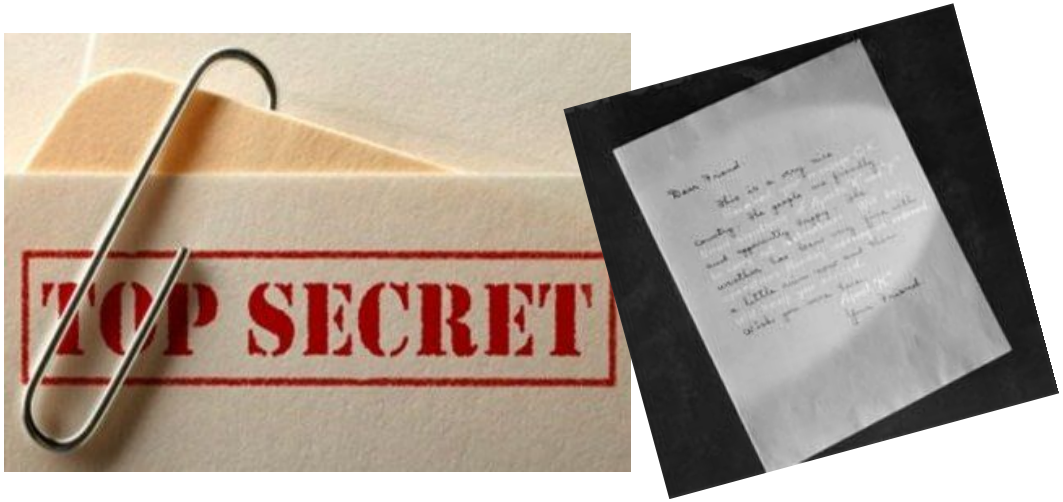
Криптография

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.



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 ониллионов.

Стеганография



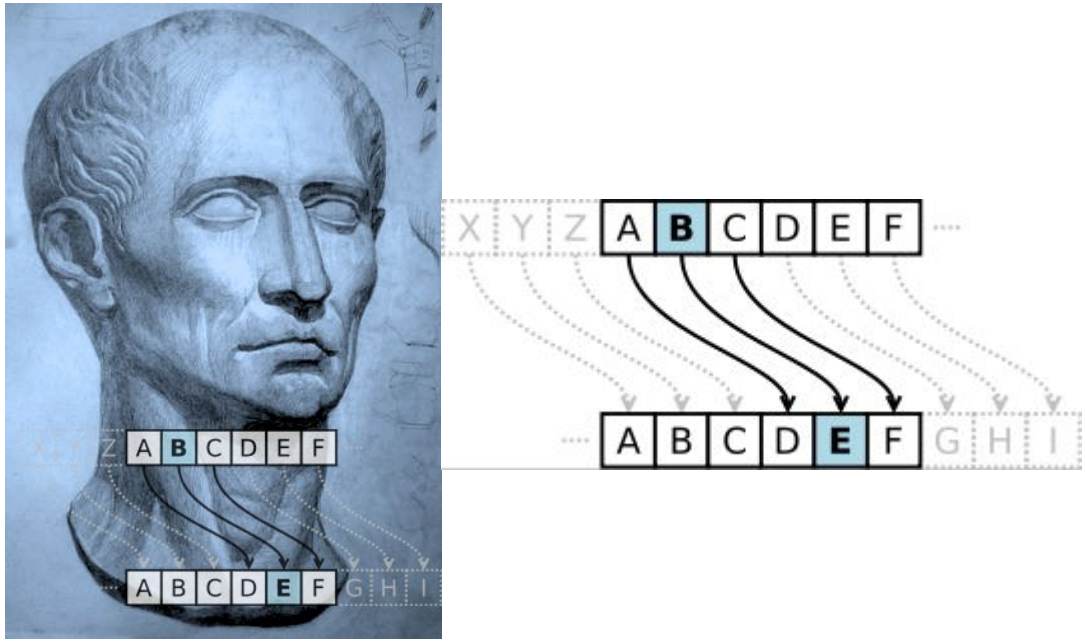
Стеганография – от steganos, «покрытый», и graphein, «писать». В течение двух тысячелетий после Геродота во всем мире применялись различные виды стеганографии. Например, древние китайцы писали сообщения на тонкой шелковой ткани, которая затем сворачивалась в крохотный шарик и покрывалась воском, после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

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» Юлия 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.

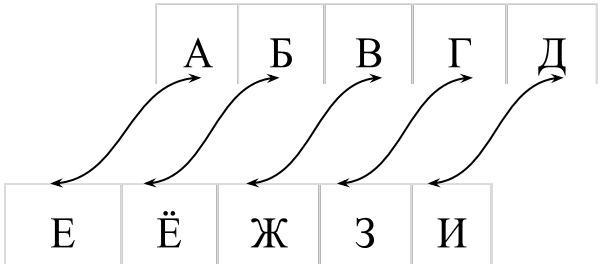
Алфавит открытого текста - алфавит, используемый для создания исходного сообщения,
и шифралфавит, буквы которого подставляются вместо букв алфавита открытого текста.

Практическая часть

Создай свой шифр!

Введя зрителя в курс дела и рассказав основные термины я готов приступить к созданию своего шифра.

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: «жйчхйьейсйдицйсбчеслй».

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