Шифровальные устройства эпохи Возрождения

Ученицы
5«А» класса
школы № 12

Искусство тайнописи.

- С зарождением человеческой цивилизации возникла необходимость передачи информации одним людям так, чтобы она не становилась известной другим.

- После возникновения письменности появилось искусство тайнописи, искусство «тайно писать» - набор методов , предназначенных для секретной передачи записанных сообщений от одного человека другому.

Наука криптография

- Криптография возникла как практическая дисциплина, изучающая и разрабатывающая способы шифрования сообщений,

то есть не скрывать сам факт передачи, а сделать сообщение недоступным посторонним.

История криптографии.

- До эпохи Возрождения имеется мало сведений о применяемых шифрах. Известен ряд значковых шифров, при котором буквы открытого текста заменяются на специальные знаки. Таким является шифр Карла Великого (780-814г.)

Шифр Скитала

- Самым первым шифровальным устройство можно считать шифр Скитала. Полоску пергамента наматывали спиралью на палочку и писали на нем вдоль палочки текст сообщения, после снятия полоски буквы на ней расположатся хаотично.

Шифр Цезаря

- Каждая шифруемая буква смешалась на три буквы вправо по алфавиту.
- Никто из современников Цезаря не смог прочесть его послания, потому что никто не знал, в каком порядке располагались буквы в алфавите Цезаря.

Еврейский шифр

- Известен так называемый «еврейский шифр»,в котором замена букв осуществляется по подстановке.
- Алфавит разбивается на две половины. Буквы второй половины пишутся под буквами первой половины в обратном порядке.

Криптография в эпоху Возрождения.

- В эпоху Возрождения в итальянских городах-государствах стали расцветать науки и ремесла.
- Шифры применялись не только государственной или церковной властью, но и учеными для защиты приоритета научных открытий.

Криптография в эпоху Возрождения.

- Известно, что шифрами пользовался Галилео Галилей. Великий учёный и художник эпохи Возрождения Леонардо да Винчи также владел криптографией и пользовался ею в своих рукописях.

Шифр Виженера

- Существенный шаг в развитии криптографии сделал французский посол в Риме Блез Виженера.

В 1585 году он написал книгу «Трактат о шифрах», в которой излагал основы криптографии.

Шифр Виженера .

- Блезу Виженеру принадлежит мысль:

«Все вещи в мире представляют собой шифр. Вся природа является просто шифром и секретным письмом».

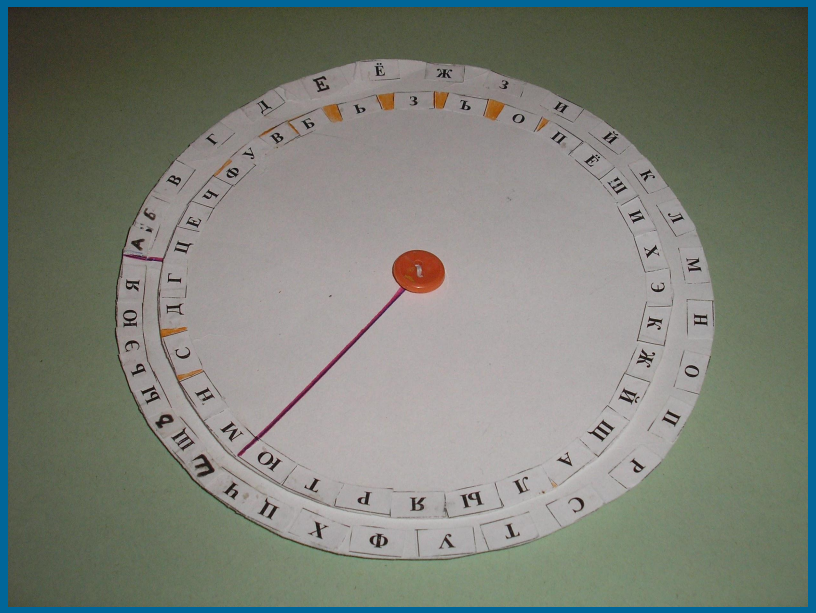
- Эту мысль повторил позднее Блез Паскаль и в наше время Норберт Винер.

Шифрующие диски

- Криптографическое устройство состояло из двух шифрующих дисков, на внешнем диске было 27 делений (26 букв латинского алфавита и «пробел»), а на внутреннем – 26 делений с другой алфавитной последовательностью.

Шифрующие диски

Слово зашифровывалось путем поворота внешней ручки так, чтобы она указывала на нужную букву текста, при этом на внутреннем диске отображалась шифрующая буква.



Цилиндр Этьена Базери

- Это устройство состояло из нескольких вращаемых дисков (у самого Базери их было 20, а у нас – 5), закрепленных на общей оси.
- На каждый диск была нанесена произвольная алфавитная последовательность.
- При шифровании текст разбивался на группы, длина которых соответствовала числу используемых дисков.

Цилиндр Этьена Базери

- Каждая группа шифруемого текста устанавливалась на цилиндре в одну строку, а в качестве шифротекста выбирался любой из остальных 25 рядов (33 ряда для русского варианта).

Линейка Сен-Сира

- Линейка представляет собой длинный кусок картона с напечатанными на нем буквами алфавита.
- Эта последовательность букв называется «неподвижной шкалой».

Линейка Сен-Сира

- Снизу, под неподвижной шкалой, в линейке были сделаны вырезы, через которые легко перемещался «движок» – узкая полоска из картона с нанесенным на него (с двойным повторением) тем же самым алфавитом. Полоска (движок) перемещается в положение, образуется простая замена открытого текста.

Семафорная азбука

- Испокон веков для передачи информации на расстоянии моряками использовалась семафорная азбука.

Кодирование в нашей жизни.

- Буквы русского языка кодируют речь.
- Нотные знаки кодируют любое музыкальное произведение.
- Правила дорожного движения кодируются с помощью символических рисунков.
- Каждый населенный пункт имеет свой код из 6 цифр.
- Месторасположение любого объекта на географической карте кодируется координатами: долготой и широтой.

Что мы сделали, изучая кодирование

- Изучая кодирование эпохи Возрождения мы познакомились с различными способами шифрования текста.
- Также мы выяснили, что одни и те же устройства могли быть придуманы разными людьми в разное время.

Что мы сделали, изучая кодирование

- Разными способами мы зашифровали около 20 высказываний таких мыслителей эпохи Возрождения, как Блез Паскаль, Мишель Монтень, Томазо Комапанелла и Леонардо да Винчи…