Криптография и шифры

Азы шифрования

Подготовил: ученик 7 «Э» класса

Столовой Александр

Руководитель:

Кулакова Татьяна Валерьевна

Цели и задачи

- Узнать о понятии «криптография» и шифрах

- Создать собственный шифр
- Закодировать цитату известного человека
- Изучить различные методы кодирования с помощью криптографии
- Узнать историю криптографии

Шифрование

Один из методов защиты информации от несанкционированного доступа – это шифрование, то есть кодирование специального вида.

Шифрование – это преобразование (кодирование) открытой информации в защищенную, то есть такую, что для понимания [illegible] шифрования и расшифровывания сообщения изучает наука криптология.

Криптология

Криптограф

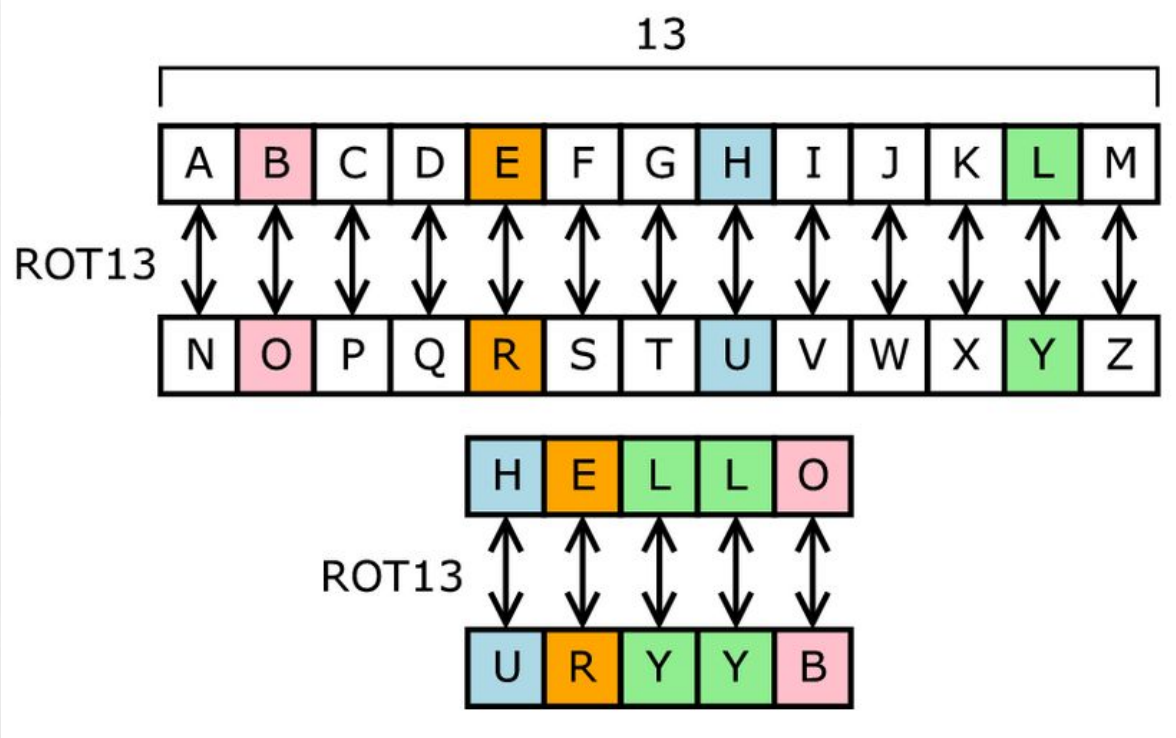
способы шифрования информации

Криптоаналитик

способы дешифрования (вскрытия шифров)

Методы шифрования с помощью криптографии

- ROT13 — распространенный тип шифрования сообщений. В нём каждая буква алфавита сдвигается на 13 позиций, как показано на рисунке:



Зашифруем фразу известного человека

- «Когда орлы молчат, болтают попугаи»
- Переведем эту фразу Уинстона Черчилля на тип шифрования ROT13, который мы рассматривали на предыдущем слайде.
- Для этого нам требуется перевести фразу на английский язык, после чего сдвинуть все буквы во фразе на 13 в алфавитном порядке.

+

- When the eagles are silent, the parrots chatter
- W J h u e n - t h e - E a g l e s - a r e - s i l e n t , - t h e - P a r r o t s - c h a t t e r
- J u r a - g u r - n t v r f - n e r - f v r a g , - g u r - c n e e b g f - p u n g g r e
- When the eagles are silent, the parrots chatter
- Когда орлы молчат, болтают попугаи

Создаем собственный шифр

Возьмем за основу шифр Цезаря (ROT13), только с русским алфавитом и с другим методом шифрования, не много отличающегося от ROT13.
Допустим, сместим алфавит на 4 буквы, а не на 13.

- а-д б-е в-ё г-ж з-к и-л й-м н-р о-с п-т у-ц ф-ч х-ш щ-ь ъ-э ы-ю я-я

История криптографии

- Криптография — одна из самых древних научных дисциплин. В истории криптографии условно можно выделить три периода. Первый период — эра донаучной криптографии, когда она являлась скорее не научной дисциплиной, а искусством, доступным узкому кругу посвященных лиц, умевших так записывать тексты, чтобы они становились непонятны посторонним.

Второй период начинается с конца XIX — начала XX в., когда происходит коренное изменение способов кодирования и обработки информации, появляются телеграф, телефон, электромеханические печатные машины и иная техника. Кульминацией этого этапа явился 1949 г., когда появилась работа известного американского математика, одного из основоположников кибернетики К. Шеннона «Теория связи в секретных системах». В ней впервые математически строго была сформулирована задача защиты информации, показаны условия невскрываемости шифров. Это событие послужило началом развития современной научной симметричной криптографии, основанной на переосмыслении и развитии принципов доклассической криптографии. В технической плане этому

Третий период начинается с появлением в 1976 г. революционной работы двух других американских математиков У. Диффи и М. Хеллмана «Новые направления в криптографии», где было показано, что секретная связь возможна и без предварительной передачи секретного ключа по физически защищенному каналу связи. Это работа послужила началом второй основной ветви современной криптографии — асимметричной криптографии. В техническом плане дальнейшему развитию криптографии содействовало бурное развитие информационно-телекоммуникационных систем, что сделало возможным реализацию сложных криптографических протоколов. Несмотря на то, что два направления различны по возрасту: симметричная криптография берет свое начало из древнего и средневекового искусства тайнописи, а асимметричной всего около 40 лет, — сегодня они имеют примерно равное значение на практике.

Сегодня мы узнали

- О таких понятиях как «криптография» и «шифры»
- Сделали собственный шифр и провели на нем диалог
- Закодировали цитату известного человека
- Изучили популярные методы шифрования
- Узнали историю криптографии