Стеганография

Стеганография - это метод организации связи, который собственно скрывает само наличие связи. В отличие от криптографии, где неприятель точно может определить является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

Криптография

На протяжении всей своей истории человек испытывал потребность в шифровке той или иной информации. Неудивительно, что из этой потребности выросла целая наука — криптография. И если раньше криптография по большей части служила исключительно государственным интересам, то с приходом интернета ее методы стали достоянием частных лиц и широко используются хакерами, борцами за свободу информации и любыми лицами, желающими в той или иной степени зашифровать свои данные в сети

Криптоанализ

Криптоанализ — наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа и сам процесс такой расшифровки. В большинстве случаев под криптоанализом понимается выяснение ключа; криптоанализ включает также методы выявления уязвимости криптографических алгоритмов или протоколов.

Криптология: подстановочно-перестановочный шифр и его применение

Работу выполнила
ученица 10 А класса
МОУ «СОШ №12 ЗАТО Шиханы
Саратовской области»
Киреева Александра

Актуальность проекта

Криптографический инструментарий является единственным и высоконадежным методом, обеспечивающим защиту информации в сетевых компьютерных технологиях различного уровня и назначения. Актуальность этого направления является однозначно безусловным неоспоримым фактором во всех сферах управления государственной и коммерческой деятельности: оборонной, правоохранительной, экономической, банковской, коммерческой, образовательной

Описание проекта

Цель:

создание проекта на тему «Криптология: подстановочно-перестановочный шифр и его применение»

Задачи:

- собрать информацию по заданной теме
- продумать формат своего проекта, его продукт и применение
- познакомиться с данной темой и направлениями в этой сфере
- составить план проекта
- найти картинки и наглядные примеры, для более точного объяснения своей темы
- объединить всю собранную информацию в единый проект

Проблемный вопрос:

- Как сохранить информацию в тайне?
- Как передать информацию адресату в тайне от других?

План

1. Криптология. Что это за наука?
2. Основные составляющие криптологии
3. Шифры и их применение

Криптология и ее происхождение

Со времен появления письменности стала развиваться такая отрасль научных знаний как полеография– историко - филологическая дисциплина, изучающая памятники древней письменности с целью установления места и времени их создания.

В основе знаний полеографии лежит также изучение сокращений письма и тайнописи, методов их расшифровки. Все это повлекло появление нового направления научных знаний-полеографии, что, в свою очередь, привело к формированию научно-прикладного направления – криптологии .

3 вида криптологии

Научное направление «криптология» подразделяется на три функционально зависимых логико-математических и технических направления:

криптография, криптоанализ, стеганография.

Шифр простой перестановки

э	т	о	с	л	о
в	о	б	у	д	е
т	з	а	ш	и	ф
р	о	в	а	н	о

Передадим в канал связи криптограмму, разбив ее для удобства представления на шесть групп:

ЭВТР ТОЗО ОБАВ СУША ЛДИН ОЕФО

Шифр Гронсфельда

- **Сообщение:**

Это сообщение будет зашифровано

- **ключ**

31431431431431431431431431

- **Шифровка**

АЦТФЦЦДЫИРКИДФЗЖЛГЩНМХФСГДРП

Чтобы понять принцип шифрования, нужно вспомнить алфавит русского языка. Итак. Например, возьмем букву «Э». Ей в ключе присвоена цифра 3. Начинаем отсчитывать от буквы «Э» 3 буквы вперед и следующая после 3 по алфавиту буква является шифровальной. В нашем случае это буква «А»

Перестановочный шифр с ключевым словом

Буквы открытого текста записываются в клетки прямоугольной таблицы по ее строчкам. Буквы ключевого слова пишутся над столбцами и указывают порядок этих столбцов (по возрастанию номеров букв в алфавите). Чтобы получить зашифрованный текст, надо выписывать буквы по столбцам с учетом их нумерации:

Открытый текст: Прикладная математика

Ключ: Шифр

Ш	И	Ф	Р
4	1	3	2
п	р	и	к
л	а	д	н
а	я	м	а
т	е	м	а
т	и	к	а

Криптограмма:
Раяеи кнааа идмм кплатт
Ключевое слово (последовательность столбцов) известно адресату, который легко сможет расшифровать сообщение.

Применение данных шифров

Это открытие в математике позволило применять криптографические методы и в нетрадиционных ранее областях, особенно в банковской деятельности. Хранить банковскую информацию в тайне, конечно, необходимо, но более важной задачей в бизнесе, связанном с управлением финансами, является надежная аутентификация участников процесса управления денежными потоками. Этот процесс легко осуществим при помощи электронной цифровой подписи.

Вывод:

Мой проект – это маленький экскурс в одну из областей огромной и сложной науки – информатика. Шифрование, на мой взгляд, это очень интересное направление в такой науке, как криптология. Углубленное изучение данной темы погружает в отдельный собственный мир вычислений, загадочных кодов, запутанных ключей и тд. Шифрование, несмотря на то, что мы сами того не подозреваем , живет с нами настолько тесно, что если бы данная отрасль просто перестала существовать, неизвестно , какая бы жизнь нас ожидала. Мы живем в то время, когда компьютеры, телефоны и многие приборы, связанные с хранением и передачей информации являются нашей неотъемлемой частью, и , конечно, безопасное хранение личных данных, передача секретной информации не может осуществляться без ее шифровки и секретности. Поэтому знать, хотя бы кусочек данной темы необходимо для уверенного перемещения по самой глобальной сети мира – Интернет.

Источники

- https://ru.wikipedia.org/wiki/Криптоанализ
- https://ru.wikipedia.org/wiki/Стеганография
- https://ru.wikipedia.org/wiki/Криптология
- www.rbardalzo.narod.ru/kripto1.html
- https://dic.academic.ru/dic.nsf/ruwiki/301891

Спасибо за внимание!!!