Министерство образования и науки РФ
ФГБОУ ВО «Новосибирский государственный педагогический университет»
Факультет технологии и предпринимательства

Криптография,криптология, криптоанализ

Выполнил: студент группы 33

Студент: Кудымов А.С

Проверил: канд. пед. наук Лейбов А.М.

2016

Содержание

1. Иерархия криптологии
2. Способы шифрования
3. Шифр цезаря
4. Квадрат Полибия
5. Основные методы криптоанализа
6. Криптографические методы
7. Обзор криптографических методов

•Криптология -
•Наука о математических аспектах информации
- Криптография –
- Наука о шифровании

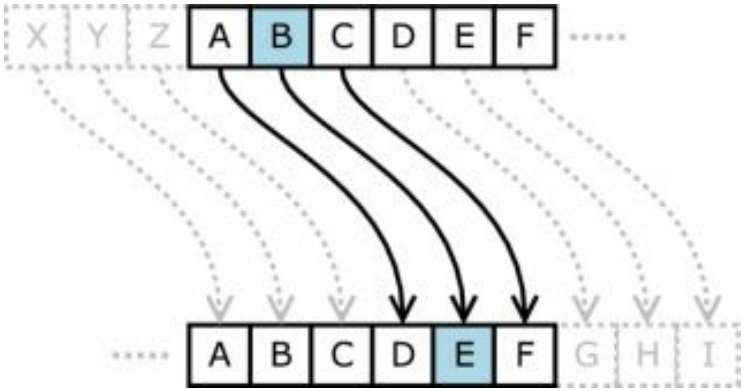
- Криптоанализ –
- Наука о взломе

Существуют некоторые способы шифрование информации, вот некоторые из них:

- Шифр цезаря
- Квадрат Полибия
- Шифр перестановки
- Гаммирование
- Блочные шифры

Шифр цезаря

Шифр Цезаря, также известный как *шифр сдвига*, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования. Шифр Цезаря — это вид *шифра подстановки*, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее. Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.



Квадрат Полибия

Формирование таблицы шифрования

К каждому языку отдельно составляется таблица шифрования с одинаковым количеством пронумерованных строк и столбцов, параметры которой зависят от его мощности. Берутся два целых числа, произведение которых ближе всего к количеству букв в языке — получаем нужное число строк и столбцов. Затем вписываем в таблицу все буквы алфавита подряд — по одной на каждую клетку. При нехватке клеток можно вписать в одну две буквы.

Квадрат Полибия

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ж	З	И	Й	К	Л
3	М	Н	О	П	Р	С
4	Т	У	Ф	Х	Ц	Ч
5	Ш	Щ	Ь	Ы	Ъ	Э
6	Ю	Я				

Пример:

Г Р Е Ц И Я

14 35 16 45 23 62

Основные методы криптоанализа

Атаки на основе шифротекста

Допустим, криптоаналитик обладает некоторым числом шифротекстов, полученных в результате использования одного и того же алгоритма шифрования. В этом случае криптоаналитик может совершить только атаку на основе шифротекста. Целью криптографической атаки в этом случае является нахождение как можно большего числа открытых текстов, соответствующих имеющимся шифро-текстам, или, что ещё лучше, нахождение используемого при шифровании ключа.

Входные данные для подобного типа атак криптоаналитик может получить в результате простого перехвата зашифрованных сообщений. Если передача осуществляется по открытому каналу, то реализация задачи по сбору данных сравнительно легка и тривиальна. Атаки на основе шифротекста являются самыми слабыми и неудобными.

Криптографические методы

Обзор криптографических методов.

Прежде чем говорить о шифровании давайте обсудим и остальные криптографические методы:

1. Электронная подпись используется для подтверждения целостности и авторства данных. Целостность данных означает, что данные не были случайно или преднамеренно изменены при их хранении или передаче.
Алгоритмы электронной подписи используют два вида ключей:

- секретный ключ используется для вычисления электронной подписи;
- открытый ключ используется для ее проверки.

При использовании криптографически сильного алгоритма электронной подписи и при грамотном хранении и использовании секретного ключа (то есть при невозможности использования ключа никем, кроме его владельца) никто другой не в состоянии вычислить верную электронную подпись какого-либо электронного документа.

2. Аутентификация позволяет проверить, что пользователь (или удаленный компьютер) действительно является тем, за кого он себя выдает. Простейшей схемой аутентификации является парольная - в качестве секретного элемента в ней используется пароль, который предъявляется пользователем при его проверке. Такая схема является слабой, если для ее усиления не применяются специальные административно-технические меры.

3. Методы криптографического контрольного суммирования:

- ключевое и бесключевое хэширование;
- вычисление имитовставок;
- использование кодов аутентификации сообщений.

Фактически, все эти методы различным образом из данных произвольного размера с использованием секретного ключа или без него (бесключевое хэширование) вычисляют некую контрольную сумму фиксированного размера, однозначно соответствующую исходным данным.
Такое криптографическое контрольное суммирование широко используется в различных методах защиты информации, например:

- для подтверждения целостности любых данных в тех случаях, когда использование электронной подписи невозможно (например, из-за большой ресурсоемкости) или является избыточным;
- в самих схемах электронной подписи - "подписывается" обычно хэш данных, а не все данные целиком;
- в различных схемах аутентификации пользователей.

4. Генераторы случайных и псевдослучайных чисел позволяют создавать последовательности случайных чисел, которые широко используются в криптографии, в частности:

- случайные числа необходимы для генерации секретных ключей, которые, в идеале, должны быть абсолютно случайными;
- случайные числа применяются во многих алгоритмах электронной подписи;
- случайные числа используются во многих схемах аутентификации.

Список литературы :

1. http://alexinternetclic.ru/Kriptograf.php
2. http://dic.academic.ru/dic.nsf/ruwiki/17909
3. http://www.chinapads.ru/c/s/kvadrat_polibiya
4. https://habrahabr.ru/post/271257/