Криптология, криптография и криптоанализ

Приступим к разбору теории, которая понадобится тебе при написании итогового проекта. Из этой лекции ты узнаешь больше о криптологии и ее составляющих. А заодно — о шифре, который ты будешь использовать при написании итогового практического проекта.

1. Криптология и ее составляющие

Криптология — это область знаний, которая включает в себя:

- **Криптографию** (наука о шифрах).

Предмет изучения криптографии — шифрование информации для ее защиты от несанкционированного доступа. Такой информацией может быть текст, цифровое изображение, звуковой сигнал и т.д. При шифровании образуется зашифрованная версия информации (данных), которую называют шифротекстом, закрытым текстом, криптограммой.

- **Криптоанализ** (методы раскрытия этих шифров).

Криптоанализ изучает методы вскрытия шифров и способы их применения. То есть, выполняет обратную задачу: изучает способы превратить зашифрованную информацию в открытую.

2. Криптографический ключ

Ключ — это набор данных, с помощью которого выполняется шифрование и расшифровка информации. Успешность дешифровки зависит от используемого ключа. Если по какой-то причине к нему утерян доступ, расшифровать данные будет невозможно.

Объем информации, который хранится в криптографических ключах, измеряют в битах. А это значит, что у криптографического ключа есть **длина**. Максимальная надежность шифрования обеспечивается при длине от 128 бит.

Разновидности криптографических ключей

1. Симметричные (секретные). Их используют в алгоритмах симметричного типа. Основное назначение — обратное или прямое криптографическое преобразование (шифрование/дешифрование, проверка кода аутентификации сообщения).

2. Ассиметричные. Применяются в в шифровальных алгоритмах асимметричного типа (например, при проверке электронной цифровой подписи).

Мы будем работать с симметричным алгоритмом шифрования, поэтому не будем вдаваться в лишние подробности.

3. Алфавит в криптографии

Алфавит — это законченное множество символов, которые используют для кодирования информации символов.

4. Подходы к криптоанализу

Существует много разных подходов и методов к криптоанализу (взлому шифров).

Опишем самые простые из них:

1. Brute force (брутфорс, поиск грубой силой) — перебор ключей, который выполняется до того момента, пока не найдем подходящий. Плюс метода состоит в простоте, минус — в том, что он не подходит для шифров, которые используют большое количество возможных ключей.

2. Криптоанализ на основе статистических данных — при таком подходе собирается статистика по вхождению разных символов в зашифрованном тексте, а потом для их расшифровки используются статистические данные о частоте вхождения в открытый текст разных символов.

Например: мы знаем, что использование буквы “П” в текстах составляет 8%. Анализируя зашифрованный текст, мы ищем символ, который встречается в процентном соотношении такое же количество раз и делаем вывод, что это буква “П”.

Минус этого подхода — зависимость от языка, авторство текста и его стилистика.

5. Шифр Цезаря[3]

Это один из самых простых и известных методов шифрования. Назвали его, само собой, в честь императора Гая Юлия Цезаря, применявшего его для секретной переписки с генералами.

Шифр Цезаря — это шифр подстановки: в нем каждый символ в открытом тексте заменяется на символ, который находится на некотором постоянном числе позиций левее или правее него в алфавите.

Допустим, мы устанавливаем сдвиг на 3. В таком случае А заменится на Г, Б станет Д, и так далее.

Это минимум теоретических данных, которые понадобятся тебе для выполнения итогового проекта. Переходим к описанию задания!

Итоговый проект к модулю Java Syntax. Пишем криптоанализатор

Задача: написать программу, которая работает с шифром Цезаря

За основу криптографического алфавита возьми все буквы русского алфавита и знаки пунктуации (. , ”” : - ! ? ПРОБЕЛ). Если попадаются символы, которые не входят в наш криптографический алфавит, просто пропусти их.

Основные требования

У программы должно быть 2 режима:

1. Шифрование / расшифровка. Программа должна зашифровывать и расшифровывать текст, используя заданный криптографический ключ.

Программа должна получать путь к текстовому файлу с исходным текстом и на его основе создавать файл с зашифрованным текстом.

2. Криптоанализ. Программа должна взламывать зашифрованный текст, переданный в виде текстового файла. У пользователя программы должна быть возможность выбрать один из двух методов криптоанализа.

Нюансы, связанные с выбором метода криптоанализа

1. Если пользователь выбирает brute force (брутфорс, поиск грубой силой), программа должна самостоятельно, путем перебора, подобрать ключ и расшифровать текст.

Подумай, какой критерий программа должна воспринимать как сигнал успешного подбора ключа.

Возможно, нужно обратить внимание на пробелы между словами или правильность использования знаков пунктуации.

2. Если пользователь **выбирает метод статистического анализа**, ему нужно предложить загрузить еще один дополнительный файл с текстом, желательно — того же автора и той же стилистики.

На основе загруженного файла программа должна составить статистику вхождения символов и после этого попытаться использовать полученную статистику для криптоанализа зашифрованного текста.

Дополнительные требования

1. Все диалоговые окна с пользователем делай на свое усмотрение. При желании можно использовать графические фреймворки Swing, JavaFX.
2. Готовое решение загрузи в публичный Git-репозиторий.