**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Криптографические методы обеспечения информационной безопасности»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

«Анализ исторических шифров с помощью программного средства Cryptool 2»

**Выполнили:**

Бакалавры гр. N34491

Хоанг Вьет Зунг

Подпись: \_\_\_\_\_\_A signature on a white background

Description automatically generated\_\_\_\_\_\_\_\_

**Проверил:**

Таранов Сергей Владимирович,

к.т.д., доцент ФБИТ

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Санкт-Петербург

2024 г.

Содержание

[Содержание 3](#_Toc146231518)

[Введение 4](#_Toc146231519)

[1 Порядок выполнения работы 6](#_Toc146231520)

[1.1 Шифр Цезаря 6](#_Toc146231521)

[1.2 Substitution Cipher (Шифр с заменой) 10](#_Toc146231522)

[1.3 Транспозиционный шифр (Transposition Cipher) 12](#_Toc146231523)

[1.4 Vigenère Cipher 14](#_Toc146231524)

[1.5 Роторная машина Энигма (Enigma Cipher Machine) 15](#_Toc146231525)

[Заключение 20](#_Toc146231526)

Введение

Цель работы – с помощью программного средства CrypTool 2 изучить принципы работы исторических шифров, а также провести их криптоанализ.

Для достижения поставленной цели необходимо решить следующие задачи:

* Шифр Цезаря, шифры перестановки и замены (как примеры моноалфавитных шифров);
* Шифр Виженера (как пример полиалфавитного шифра);
* Структуру и процесс шифрования в роторной машине Энигма.

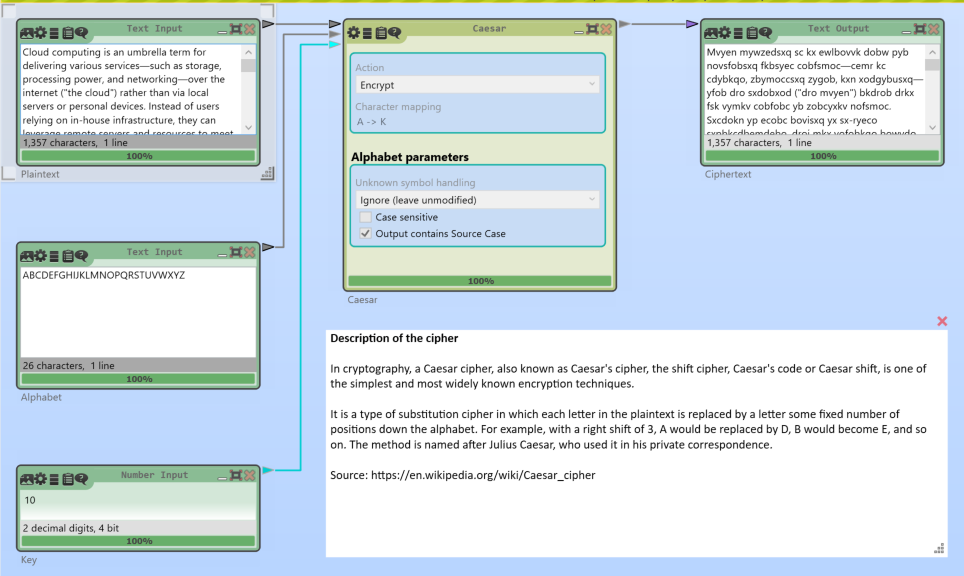
Открытый текст:

Cloud computing is an umbrella term for delivering various services—such as storage, processing power, and networking—over the internet ("the cloud") rather than via local servers or personal devices. Instead of users relying on in-house infrastructure, they can leverage remote servers and resources to meet their computing needs, making it cost-effective and scalable. Recently, advances in cloud architecture have allowed businesses to streamline operations, scale globally, and offer enhanced flexibility. Cloud computing is applied across industries in areas like data storage, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), where developing and maintaining on-premise infrastructure would be too costly or complex. The foundational technologies that support cloud computing include virtualization, networking, and large-scale distributed computing systems. Edge computing is a related (parallel) field of study, focusing on processing data closer to the source to reduce latency and bandwidth usage. Cloud computing is crucial in addressing modern business challenges, offering predictive scalability, enhanced collaboration, and on-demand availability. Although cloud computing spans many areas, its core relies heavily on reliable network infrastructure and efficient resource management systems.

# Порядок выполнения работы

## Шифр Цезаря

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.



1. Шифрование Шифром Цезаря

Получаем закрытый текст.

Потом сделаем дешифрование:

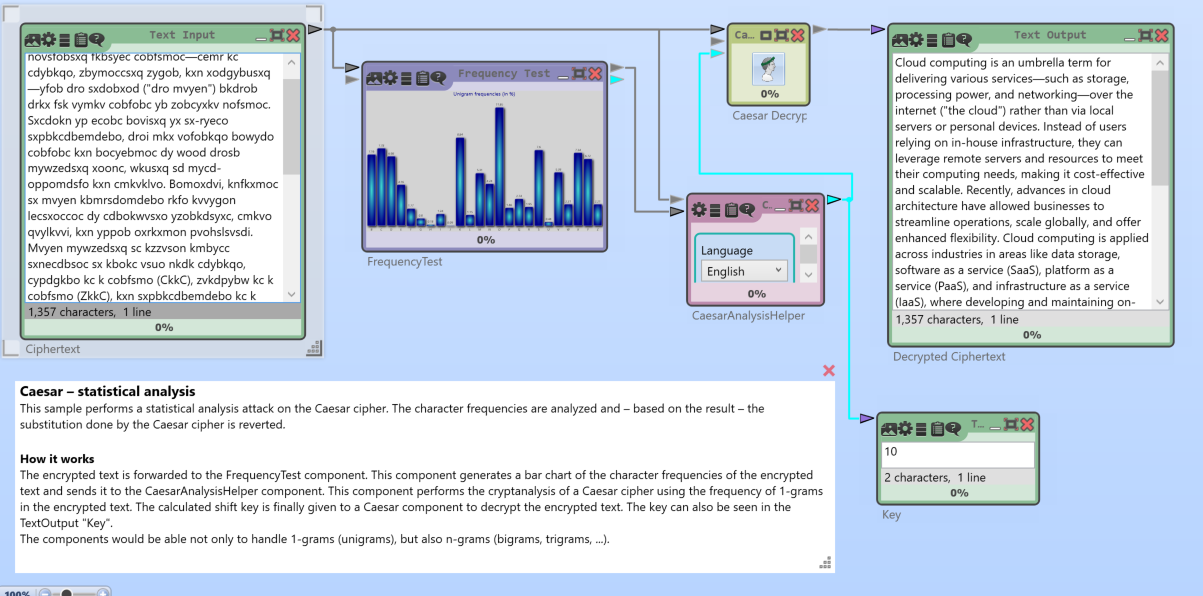
A screenshot of a computer

Description automatically generated

1. Дешифрование Шифром Цезаря

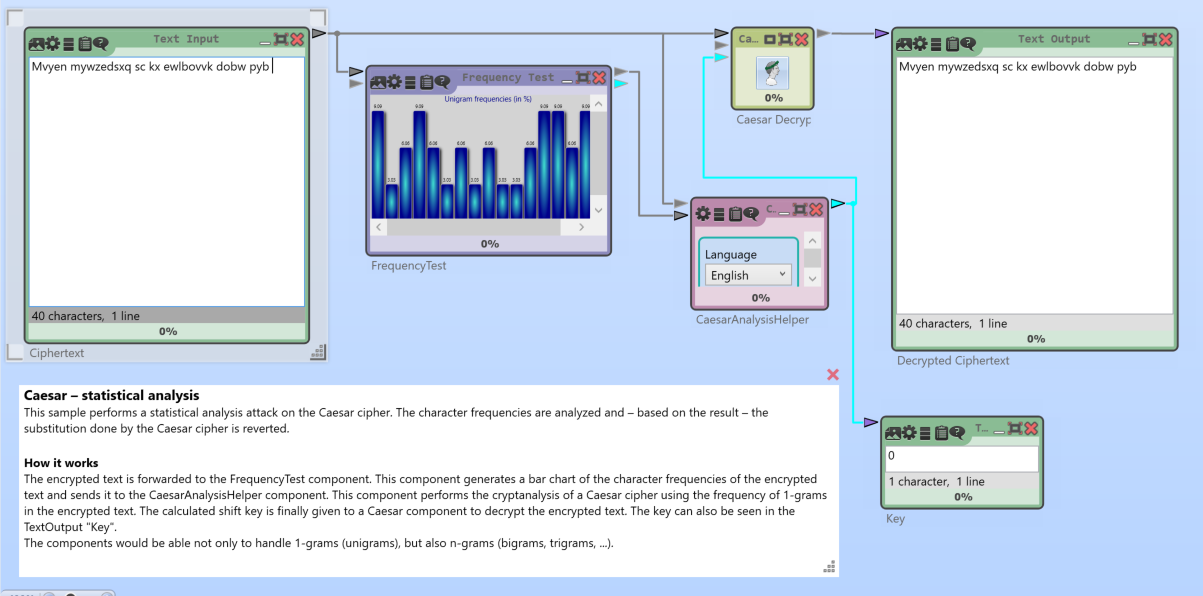
* Совпадает с открытом ключом.

Выполнить простейший криптоанализ, используя шаблоны из программы Cryptool 2 (шаблон для атаки на основе частотного анализа находятся по пути Templates -> Cryptoanalysis -> Classical -> Caesar Analysis using character frequencies). Целью криптоанализа является восстановление секретного ключа на основе закрытого текста. Часто на практике применяется методы расшифровки сообщений за счет различных методов криптоанализа. Так, например, один из них – частотный анализ. На Рисунке 3 видно, что расшифровка частотным анализом прошла успешно.



1. Частотный анализ шифра Цезаря

С малым текстом частотный анализ может выдавать неправильный результат:



1. Частотный анализ на малом объёме текста

* На успешность частотного анализа влияет длина открытого текста.

Если удалить пробела между словами:

A screenshot of a computer

Description automatically generated

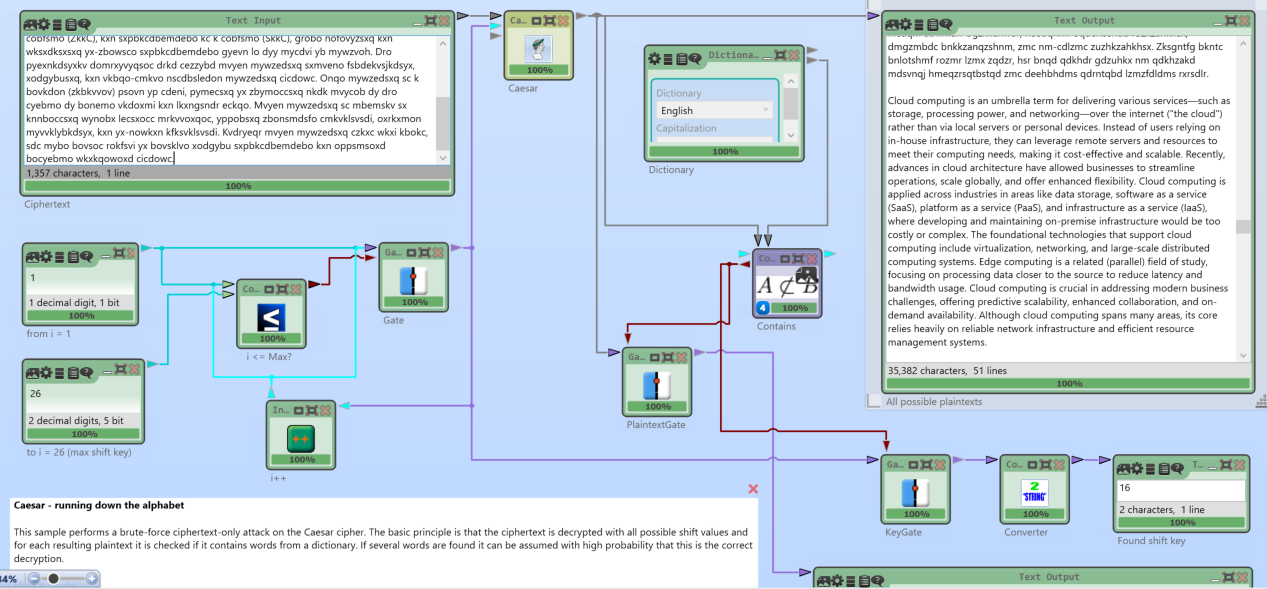
1. Удалить пробела между словами

* Совпадает с открытом ключом.

Аналогично если удалить специальные символа и вставочки, которые не входят в алфавит шифра.

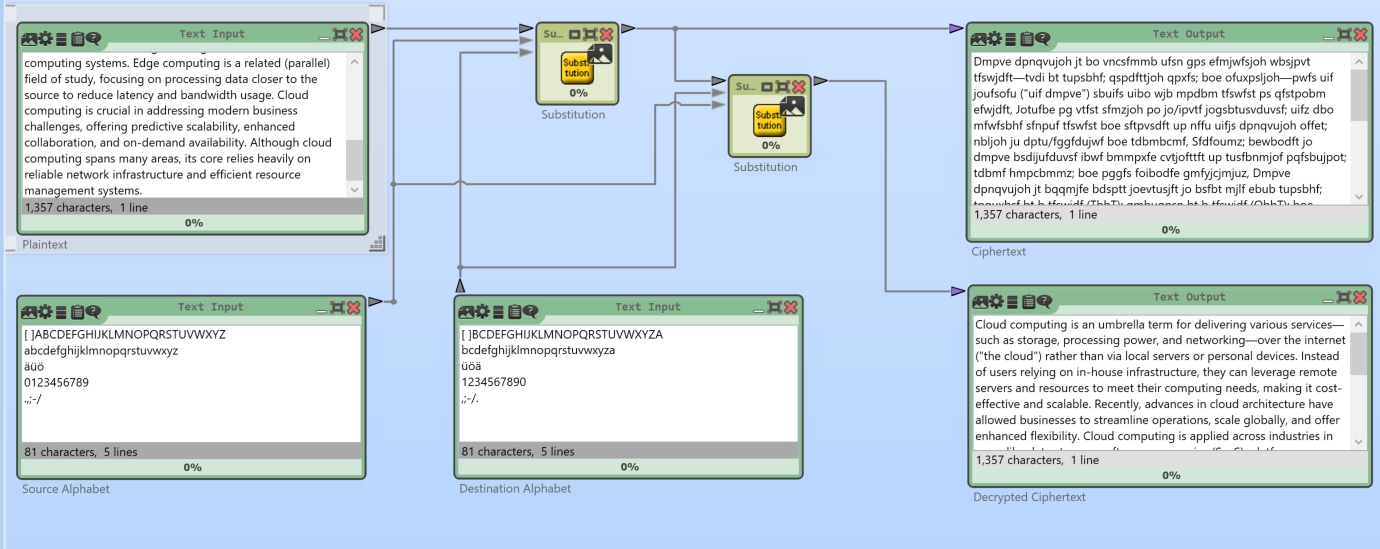
Вывод: на частотный анализ влияет длина текста, но не специальные символы или пробелы.

Перейдём к следующему методу – выполнение криптоанализа шифра Цезарь, используя шаблон, реализующий атаку полным перебором.



1. Брутфорс Шифром Цезаря

## Substitution Cipher (Шифр с заменой)



1. Шифрование

* Закрытый совпадает с открытом ключом.

A screenshot of a computer

Description automatically generated

1. Monoalphabetic Substitution Analyzer

* Алгоритм успешно расшифровал закрытый текст.

Если удалить специальные символа и вставочки, которые не входят в алфавит шифра, получается лучший результат.

A screenshot of a computer

Description automatically generated

1. Удалить специальные символа и вставочки

Если удаляем пробела между словами, получаем правильный открытый ключ:

A screenshot of a computer

Description automatically generated

1. Удалить пробела между словами

Но если делаем анализ с малым текстом, результат получается неправильный:

A screenshot of a computer

Description automatically generated

1. Анализ с малым текстом

## Транспозиционный шифр (Transposition Cipher)

A screenshot of a computer screen

Description automatically generated

1. Транспозиционный шифр

* Совпадает закрытый с открытым ключом.

Для атак на шифр Transposition Brute-Force Analysis:

A blurry image of a computer screen

Description automatically generated

1. Transposition Brute-Force Analysis

* Данный метод криптоанализа успешно справился с расшифровкой закрытый текст.

Для атак на шифр Transposition Crib Analysis:

A blurry image of a computer screen

Description automatically generated

1. Transposition Crib Analysis

* Не успешно.

Для атак на шифр Transposition Genetic Analysis:

A blurry image of a computer screen

Description automatically generated

1. Transposition Genetic Analysis

* Не успешно.

Для атак на шифр Transposition Hill Climbing Analysis:

A screenshot of a computer

Description automatically generated

1. Transposition Hill Climbing Analysis

* Данный метод криптоанализа успешно справился с расшифровкой закрытый текст.

## Vigenère Cipher

A screenshot of a computer

Description automatically generated

1. Шифр Виженера

* Зарытый, получается после дешифрования совпадает с открытым ключом

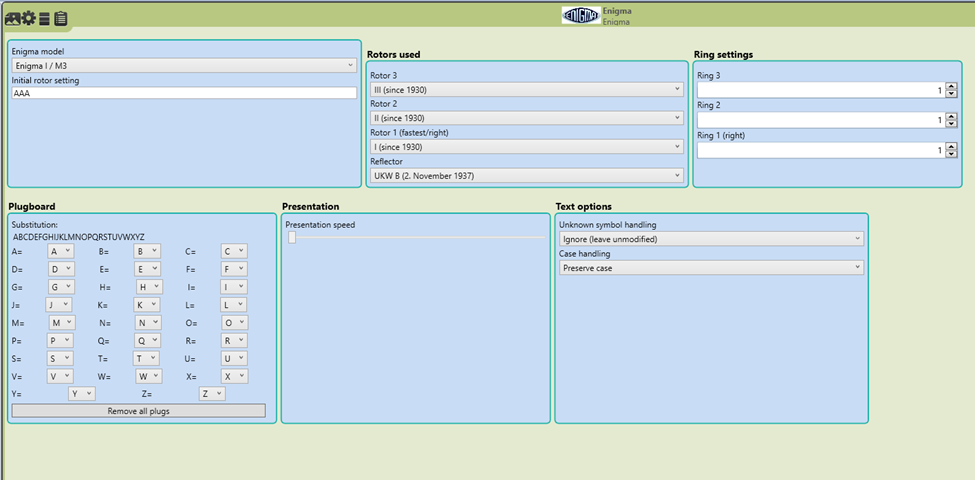
A blurry image of a computer screen

Description automatically generated

1. Криптоанализ шифра Виженера(Vigenère Analysis)

## Роторная машина Энигма (Enigma Cipher Machine)

Настроим машину:



1. Настройки Энигмы

Потом шифруем открытый ключ, получается закрытый

A screenshot of a computer

Description automatically generated

1. Шифрование

A screenshot of a computer

Description automatically generated

1. Процесс шифрования символа C

A screenshot of a computer

Description automatically generated

1. Процесс шифрования символа L

Проведем криптоанализ данного метода шифрования. Воспользуемся методом Gillogly для криптоанализа.

A screenshot of a computer

Description automatically generated

1. Gillogly-атака на Энигму

Далее воспользуемся методом Hillсlimbing для криптоанализа. Даже когда были установлены точные настройки исходной роторной машины, не удалось точно восстановить исходное сообщение.

A screenshot of a computer

Description automatically generated

1. Hillсlimbing-атака на Энигму

Далее воспользуемся методом Simulated Annealing для криптоанализа. Мы видим что закрытый не совпадает с открытым ключом.

A screenshot of a computer screen

Description automatically generated

1. Simulated Annealing-атака на Энигму

Последним методом криптоанализа будет атака Turing Bombe. Удалось точно восстановить исходное сообщение, установив точные настройки роторной машины, но недостаточно символов открытого текста.

A screenshot of a computer

Description automatically generated

1. Turing Bombe-атака на Энигму

Заключение

В процессе выполнения данной лабораторной работы мы ознакомились с программой CrypTool 2 и изучили принципы работы исторических шифров, таких как Цезаря, Виженера, транспонирования и замены. Также мы провели их криптоанализ и с помощью этого метода смогли восстановить открытый текст и секретный ключ в шифрах Цезаря, Вижнера, транспонирования и замены, но не во всех методах криптоанализа.

Кроме того, мы провели криптоанализ машины Энигма с помощью различных методов и смогли расшифровать исходный текст, когда установили точные настройки роторной машины. Вероятно, длина сообщения оказалась важным фактором в успешном криптоанализе. Однако можно сделать вывод, что шифрование с помощью машины Энигма более устойчиво к криптоанализу, чем другие методы, которые были рассмотрены ранее.

В ходе выполнения работы цель была достигнута, все поставленные задачи выполнены.

Вопросы

1. Что изучают следующие разделы криптографии: криптология, криптография, криптоанализ?

Криптология — наука, занимающаяся методами шифрования и дешифровки. Криптология состоит из двух частей — криптографии и криптоанализа.

Криптография занимается разработкой методов шифрования и дешифрования данных, в то время как криптоанализ занимается оценкой сильных и слабых сторон методов шифрования.

1. Основные отличия, определения, примеры для следующих систем: асимметричные криптосистемы, симметричные криптосистемы, криптографические протоколы.

 Асимметричные криптосистемы:

Система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищенному, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ. Примеры: RSA, DSA, Диффи-Хеллман

Симметричные криптосистемы:

Способ шифрования, в котором для шифрования и расшифрования применяется один и тот же криптографический ключ. Примеры: AES, DES, 3DES, RC5

 Криптографические протоколы:

Криптографический протокол — это абстрактный или конкретный протокол, включающий набор криптографических алгоритмов, часто являющихся последовательностью криптографических примитивов. SSL, TLS, PPTP, IPSec

1. Выделите примеры шифров для каждого этапа развития криптографии: наивная криптография, формальная криптография, математическая криптография.

Наивная криптография

- Шифр Цезаря

- Шифр Атбаш

- Полибиева решетка

Формальная криптография

- Шифр Вернама

- Шифр Плейфера

- Шифр Виженера

Математическая криптография

- RSA

- AES (Advanced Encryption Standard)

- Эллиптические кривые (ECC)

1. Шифры замены, перестановки и сдвига

Шифры замены:

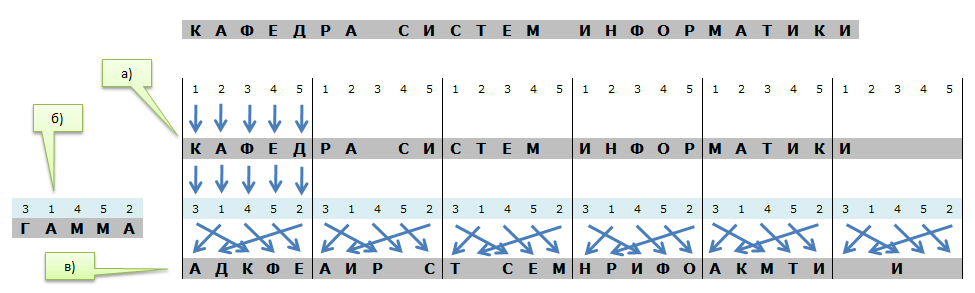
Шифрование состоит в замене каждой буквы в открытом тексте на соответствующую ей нижнюю букву. Чтобы расшифровать шифротекст, нужно каждую его букву найти в нижней строке таблицы и заменить ее соответствующей верхней.

A close-up of a grid

Description automatically generated

Шифры перестановки:

Шифр перестановки - это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее. Типичными примерами перестановки являются анаграммы



Шифры сдвига

Процесс шифрован ия заключается в замене каждой буквы на другую, отстоянную от исходной на определенное число позиций в алфавите в зависимости от значения ключа.

A close up of a word

Description automatically generated

1. Атака полного перебора ключа и частотный анализ символов

Атака полного перебора выполняется по следующему алгоритму:

− атакующий перехватывает шифротекст, а также некоторую малую часть открытого текста;

− атакующий дешифрует шифротекст, перебирая все возможные криптографические ключи;

− eсли при дешифровании полученный текст совпадает с перехваченной частью открытого текста, то считается что ключ подобран.

Алгоритм проведения атаки частотного анализа следующий:

− определяем частоту появления каждого символа шифротекста;

− распределение частот символов шифротекста будет близка к распределению частот символов в языке вообщем;

− сопоставляются символы шифротекста и частота встречаемости символов в языке и таким образом восстанавливается ключ.

1. Модульная арифметика. Простые примеры.

A black text on a white background

Description automatically generated

15 mod 4 = 3

- 15 делим на 4, получаем 3 (остаток 3). Значит, 15 mod 4 = 3

10 mod 7 = 3

- 10 делим на 7, получаем 1 (остаток 3). Значит, 10 mod 7 = 3

1. Шифр Виженера. Тест Казисского

Шифр Виженера — это форма кодирования алфавитной замены, в которой каждый символ открытого текста кодируется сдвигом на основе повторяющегося ключевого слова. Каждая буква в ключевом слове определяет количество сдвигов в алфавите для каждого соответствующего символа текста.

Тест Казисского состоял из двух шагов:

− анализ триграмм и биграмм для получения длины ключа

− шифротекст делится на блоки, равные длине ключа и впоследствии используется стандартный метод частотного анализа по отношению к каждому блоку

1. Принцип Кергоффса

Криптосистема должна сохранять криптостойкость даже в случае, если атакующий знает все детали о самой криптосистеме за исключением криптографического ключа.

1. Роторные машины. Краткое описание принципа работы и внутренней структуры. Пространство ключей роторной машины.

Роторные машины — это класс механических устройств, используемых для шифрования текста. Их основным элементом являются вращающиеся роторы с алфавитами, которые при каждом вводе символа изменяют положение и обеспечивают сложную замену символов. Когда пользователь вводит символ, ток проходит через серию роторов, изменяя каждый раз путь, таким образом создавая многослойное шифрование.

Пространство ключей роторной машины зависит от количества роторов, их возможных начальных позиций и внутренних конфигураций соединений. Чем больше роторов и вариаций, тем больше возможных ключей, что усложняет взлом.

1. Криптостойкость. Вычислительная и практическая криптостойкость

Криптостойкость — это способность криптографического алгоритма противостоять попыткам его взлома.

Вычислительная криптостойкость — это оценка времени и ресурсов (вычислительной мощности), необходимых для взлома алгоритма, основываясь на известных методах атаки. Чем больше требуется ресурсов, тем выше вычислительная стойкость.

Практическая криптостойкость — это реальная защита в условиях использования, учитывающая не только вычислительную сложность, но и возможные уязвимости, ошибки в реализации, социальную инженерию и другие факторы, которые могут облегчить взлом.

1. Криптоанализ. Классический криптоанализ. SCA.

Криптоанализ — это наука о методах взлома криптографических систем, направленных на нахождение слабостей алгоритмов шифрования.

Классический криптоанализ — анализ криптосистем, основанный на математических и лингвистических закономерностях, часто применяемый к традиционным шифрам (например, Цезаря или Виженера). Цель — восстановление исходного текста или ключа без знания секрета.

SCA (Side-Channel Attacks) — атаки по побочным каналам, использующие утечки информации, такие как время выполнения, энергопотребление или электромагнитные излучения, для взлома криптосистем. Эти атаки направлены не на алгоритм, а на его физическую реализацию.