Содержание

Немного о криптографии и цели создания приложения

Проблема защиты информации путем её преобразования волновала человечество с давних времен. С распространением письменности появилась потребность в обмене письмами и сообщениями, что вызвало необходимость сокрытия их содержимого от посторонних. Так начала формироваться наука под названием криптография и именно поэтому её можно считать ровесницей истории человеческого языка.

Первые криптосистемы встречаются уже в начале нашей эры. В основном развитию криптографии способствовали войны. Письменные приказы и донесения обязательно шифровались, чтобы пленение курьеров не позволило противнику получить важную информацию. Так, древнеримский политический деятель и полководец Гай Юлий Цезарь в своих переписках активно использовал уже более-менее систематический шифр, получивший его имя.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

На сегодняшний день криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности. Например, для портативных компьютеров, физически защитить которые крайне трудно, только криптография позволяет гарантировать конфиденциальность информации даже в случае кражи. Что уж говорить про важность криптографии в глобальной сети «Интернет», по которой ежедневно передаются колоссальные объемы информации государственного, военного, коммерческого и частного характера, которая нуждается в защите от доступа к ней посторонних лиц.

Переоценить возможности криптографии для человечества сложно. С момента появления она прошла множество модификаций и сейчас представляет собой систему безопасности, которая практически не может быть взломана. Современные методы криптографии применяются практически во всех отраслях, в которых присутствует необходимость безопасной передачи или хранения данных.

Данное приложение предназначено для шифрования и дешифрования текста популярными и относительно безопасными алгоритмами.

Описание функций программы

Функционал

В программе имеются следующие функции:

- Выполнить — выполнить выбранную операцию;
- Обновить — обновить все поля и данные;
- Сгенерировать ключ — сгенерировать ключ в зависимости от выбранного алгоритма;
- Открыть — открыть файл с исходным текстом или ключом
- Сохранить — перезаписать текст в выбранный файл;
- Сохранить как... — сохранить исходный текст, зашифрованный текст или ключ;
- О программе — открыть справку с описанием основных вещей в приложении;
- Выбор операции — шифрование или дешифрование;
- Способ шифрования — выбрать метод, которым будет шифроваться или дешифроваться исходный текст;
- “+” — увеличить размер шрифта в поле;
- “-” — уменьшить размер шрифта в поле;
- Очистить — очистить выбранное поле от текста;
- Дополнительные действия — выбрать дополнительные действия, которые необходимо выполнить вместе с успешным выполнение операции;
- Выход — выйти из программы.

Горячие клавиши

Для более удобной работы с приложением предусмотрены следующие горячие клавиши:

- “F1” — Выполнить;
- “F2” — Обновить;
- “F3” — Сгенерировать ключ;
- “F4” — Открыть файл с исходным текстом;
- “F5” — Открыть файл с ключом;
- “F6” — Сохранить;
- “F7” — Сохранить исходный текст;
- “F8” — Сохранить зашифрованный/дешифрованный текст;
- “F9” — Сохранить ключ;
- “F11” — О программе;
- “F12” — Выход.

Описание алгоритмов и принципов их работы

Транспозиция

Первым методом шифрования рассмотрим транспозицию или как его по-другому называют – шифр перестановки. Он относится к симметричным криптосистемам перестановочного типа. Принцип работы этого метода заключается в том, что элементы открытого текста меняются местами. Элементами текста могут быть как отдельные символы, так и их пары, тройки и так далее, а также комбинирование этих случаев.

Плюсами этого метода можно считать высокую скорость шифрования и дешифрования так как символы всего лишь переставляются на другие позиции.

Минусами этого метода можно считать сохранение частотных характеристик текста и малое количество возможных ключей шифрования, что делает его уязвимым к криптоатакам. Главным недостатком этого и других симметричных алгоритмов шифрования можно считать передачу ключа. Ведь для того, чтобы он не попал в чужие руки для его передачи требуется обеспечить дополнительную безопасность, его также требуется регулярно обновлять, а после его смены опять же возникает нужда в его безопасной передаче.

Моноалфавитный шифр

Следующий метод шифрования – моноалфавитный шифр или по-другому – шифр простой замены. Он относится к симметричным криптосистемам подстановочного типа. К этому типу относятся, наверное, самый известный шифр – шифр Цезаря, в котором каждый символ алфавита сдвигается на три позиции правее. Принцип работы подстановочных шифров сводится к созданию таблицы шифрования (по определённому алгоритму), в которой каждой букве открытого текста соответствует единственная сопоставимая ей буква шифротекста. Само же шифрование заключается в замене букв согласно созданной таблице. Как можно заметить, всё очень просто.

Отмечу также, что в шифрах замены не всегда подразумевается замена буквы на какую-то другую букву. Допускается использовать замену на число. Соответственно в создаваемой таблице каждой букве используемого алфавита приравнивается любое число.

Плюсами этого метода можно считать высокую скорость шифрования и дешифрования.

Минусами этого метода можно считать то, что в шифротексте не скрывается частота появления символов открытого текста, что делает его уязвимым к криптоатакам и то, что максимальный количество ключей равно количеству букв в используемом алфавите. Также здесь имеется проблема передачи больших объёмов текста (чем больше текст, тем легче его взломать). Так как алгоритм относится к симметричным опять же требуется дополнительная безопасность при передаче ключа и его регулярное обновление.

Полиалфавитный шифр

Рассмотрим метод шифрования – полиалфавитный шифр или по-другому – многоалфавитный шифр.

Как и моноалфавитный шифр он относится к симметричным криптосистемам подстановочного типа принцип работы которых был описан ранее.

Суть работы полиалфавитного шифра заключается в циклическом применении нескольких моноалфавитных шифров к некоторому количеству букв открытого текста.

Плюсами этого метода можно считать высокую скорость шифрования и дешифрования, а также маскировку частот появления тех или иных букв в тексте.

Минусами этого метода можно считать передачу больших объёмов текста, а также распространение ключей и их обновление.

Исключающее ИЛИ (XOR)

Метод исключающего ИЛИ (XOR) относится к симметричным криптосистемам типа гаммирование. Принцип работы этого типа шифров заключается в «наложении» последовательности, состоящей из случайных чисел на открытый текст. То есть генератор случайных чисел выдаёт последовательность битов (гамму), которая накладывается на открытый текст с помощью побитовой операции исключающего ИЛИ, в результате чего получается шифротекст.

Плюсами этого метода можно считать высокую скорость шифрования и дешифрования, а также его стойкость, определяющаяся гаммой (длительностью периода и равномерностью статических характеристик).

Минусами являются: распространение ключей и их обновление.

Одноразовый блокнот

Шифр Вернама или одноразовый блокнот – представляет собой систему симметричного шифрования типа гаммирование, так как использует булеву функцию «исключающее ИЛИ». Этот метод был изобретён в 1917 году Гилбертом Вернамом. При правильном использовании этого метода, текст, который был им зашифрован невозможно взломать. Этот метод является примером системы с абсолютной криптографической стойкостью при этом считаясь одной из простейших криптосистем.

Так как работает этот метод основываясь на XOR, алгоритм шифрования такой же, как был описан выше. Единственная разница в том, что длина ключа обязательно должна быть равна длине открытого текста.

Плюсами этого метода можно считать высокую скорость шифрования и дешифрования, а также его абсолютную криптографическую стойкость при правильном использовании.

Минусами являются: существенный размер ключа, а также распространение ключей и их регулярное обновление (настолько регулярное, что ни один ключ не должен использоваться более одного раза).

Rivest, Shamir, Adleman (RSA)

Последний метод, который мы рассмотрим называется RSA (аббревиатура от фамилий его создателей Rivest, Shamir, Adleman). Он относится к асимметричным криптосистемам.

Эта криптосистема стала первой системой, пригодной как для шифрования, так и для цифровой подписи. Принцип её работы можно разделить на три шага: первый – создание открытого (публичного) и закрытого (секретного) ключей на основе взаимно простых чисел (тех, которые делятся только на единицу или сами на себя), второй шаг – шифрование сообщения и третий шаг – расшифровка.

Как же создать эти самые ключи? Для создания открытого ключа нужно: выбрать два простых числа, вычислить модуль их произведения, вычислить функцию Эйлера, выбрать открытую экспоненту, которая также будет являться простым числом, при этом будет меньше числа, полученного при вычислении функции Эйлера и наконец будет взаимно простым для этой функции. В результате этих манипуляций с формулами мы получим пару чисел, это и есть наш публичный ключ. Закрытый ключ создаётся вычислением обратной открытой экспоненты по модулю функции Эйлера, при этом модуль должен быть равен единице.

Теперь нужно отдать полученный открытый ключ человеку, который с помощью него планирует отправлять вам зашифрованные сообщения. Допустим, что, выполнив все предыдущие операции мы получили числа 5 и 21 – это публичный ключ и числа 17 и 21 – это секретный ключ. Теперь допустим, что вы хотите зашифровать букву «С», в русском алфавите она располагается на 19 позиции. Для того чтобы зашифровать эту букву нужно возвести позицию нашей буквы в 5 степень и от полученного числа взять остаток от деления на 21. В результате получиться число 10 или буква «И» это и будут наши закодированные данные.

Шифрованные данные передаются владельцу секретного ключа. Тут следует обратить внимание на то, что открытый ключ не может расшифровать сообщение, а закрытый находится только у владельца (если

он никому его не говорил), так что передача может осуществляться по открытому каналу. Итак, чтобы дешифровать сообщение нужно провести те же действия, что и при шифровании сообщения только используя закрытый ключ. Возьмём нашу зашифрованную букву «И» расположенную на позиции 10, возведём её в 17 степень и от полученного числа возьмём остаток от деления на 21. Результатом вычислений будет число 19 или буква «С».

Плюсами этого метода можно считать удобство распространения ключей и высокую безопасность при передаче небольших сообщений.

Минусами являются: существенный размер ключа, низкая скорость шифрования, а также то, что шифрование происходит по буквам, то есть одна и та же буква будет шифроваться одним и тем же числом, если злоумышленник перехватит достаточно большое сообщение расшифровать его не составит никакого труда.

Ошибки и способы их исправления

Ошибки при вводе ключа

Ошибки при вводе ключа для метода транспозиции

Чтобы исправить ошибку в поле необходимо ввести необходимое количество числовых значений через пробел

Ошибки при вводе ключа для метода моноалфавит

Чтобы исправить ошибку в поле необходимо ввести числовое значение

Ошибки при вводе ключа для метода полиалфавит

Чтобы исправить ошибку в поле чаще всего необходимо ввести исходный текст

Ошибки при вводе ключа для метода XOR

Чтобы исправить ошибку в поле чаще всего необходимо ввести исходный текст

Ошибки при вводе ключа для метода одноразовый блокнот

Чтобы исправить ошибку в поле необходимо ввести ключ, который будет одной длины с исходным текстом или больше него

Ошибки при вводе ключа для метода RSA

Чтобы исправить ошибку в поле необходимо ввести два числовых значения через пробел, при этом значения должны быть сгенерированы на основе простых чисел

Также ошибка может возникнуть если пытаться расшифровать зашифрованный текст открытым ключом, или пытать зашифровать открытый текст закрытым ключом

Ошибки при генерации ключа

Ошибки при генерации ключа с вводом размера

Чтобы исправить ошибку в поле необходимо ввести числовое значение

Ошибки при генерации открытого и закрытого ключей

Чтобы исправить ошибку в поле P нужно ввести значение, соответствующее следующим критериям:

- P должно быть простым числом;
- P должно быть больше 10;
- P должно быть отличным от Q.

Чтобы исправить ошибку в поле Q нужно ввести значение, соответствующее следующим критериям:

- Q должно быть простым числом;
- Q должно быть больше 10;
- Q должно быть отличным от P.

Ошибка отсутствия файла справки

Чтобы исправить ошибку попробуйте установить программу заново, если после этого ошибка не исчезнет, обратитесь к администратору.