**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

отчет

**по лабораторной работе №1**

**по дисциплине «Криптография и защита информации»**

Тема: Изучение классических шифров RailFence, Vigenere и ADFGVX

|  |  |  |
| --- | --- | --- |
| Студент гр. 8304 |  | Сергеев А.Д. |
| Преподаватель |  |  |

Санкт-Петербург

2021

**Цель работы.**

Исследовать шифры Rail Fence, Vigenere и ADFGVX, получить практические навыки работы с ними, в том числе с использованием приложений Cryptool 1 b 2.

**Основные теоретические положения.**

В шифре Изгороди открытый текст вписывается в таблицу-шаблон, содержащую заданное количество строк. В каждую строку поочередно записывается одна буква со смещением, подобно изгороди. Зашифрованный текст создается путем объединения наборов символов из строк таблицы шаблона.

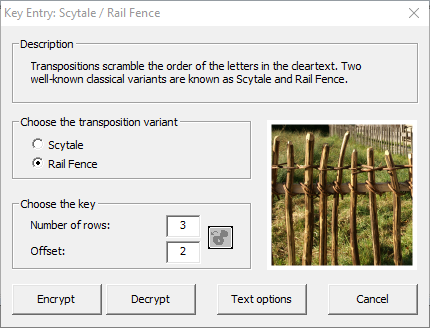
Шифр Виженера - метод полиалфавитного шифрования текста с использованием ключевого слова. Для зашифровывания выбирается кодовое слово длины n, которое делит открытый текст на отрезки данной длины. Далее составляется, так называемая, таблица Виженера (tabula recta). Горизонтально записывается алфавит, вертикально под первым символом алфавита записывается кодовое слово. Заполнение таблицы осуществляется символами алфавита, начинающегося с элемента кодового слова, и циклически замыкается. Элемент шифротекста выбирается на пересечении столбца, соответствующего букве открытого текста и строки, соответствующей букве кодового слова.

Шифр ADFGVX — один из самых известных шифров времён Первой мировой войны, который использовался немецкой армией. Шифрование осуществляется в два этапа. На первом этапе сначала задается матрица-ключ 6х6, заполненная символами алфавита, а также цифрами от 0 до 9. Индексами строк и столбцов этой матрицы являются буквы A,D,F,G,V,X. Далее каждый символ открытого текста кодируется парой буквенных индексов, на пересечении которых в матрице-ключе он находится. На втором этапе задаётся кодовое слово производится перестановка столбцов, и ранее закодированный открытый текст переписывается построчно в матрицу с числом столбцов равным длине ключевого слова. В завершении столбцы этой матрицы переставляются в соответствии с лексикографическим порядком букв ключевого слова и шифротекст образуется конкатенацией строк этой матрицы

**Шифр изгороди.**

Задание:

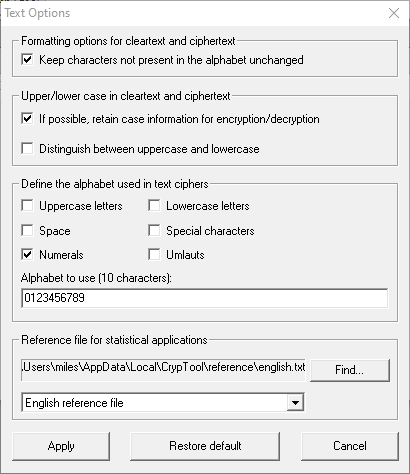
1. Найти шифр в CrypTool 1: *Encrypt/Decrypt -> Symmetric (Classis)*.
2. Создать файл с открытым текстом, содержащим последовательность цифр.
3. Запустить шифр и выполнить зашифровку и расшифровку созданного текста несколько раз.
4. Установить, как влияют на шифрование параметры *Number of Rows* и *Offset*.
5. Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра при *Number of Rows*>2, *Offset*≥2. Убедиться в совпадении результатов.



Реализация в CrypTool 1.0:

Интерфейс CrypTool для работы с шифром изгороди

На данном экране можно настроить параметры *Number of Rows* (количество строк таблицы) и *Offset* (смещение при записи текста в таблицу).

Экран для настройки параметров шифрования

На данном можно задать дополнительные параметры, такие как алфавит, используемый при шифровании, обработка заглавных и строчных букв, а также поведение по отношению к символам, не входящим в заданный алфавит.

Схема, поясняющая работу шифра:

Для шифрования используется специальная таблица, число столбцов в которой представляет из себя сумму числа букв в исходном тексте и параметра *Offset*, который определяет отступ при записи букв в таблицу, а число строк задается параметром *Number of Rows*:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| - | \* | \* | \* | \* | \* | E | \* | \* |
| \* | - | \* | \* | \* | G | \* | E | \* |
| \* | \* | S | \* | R | \* | \* | \* | V |
| \* | \* | \* | E | \* | \* | \* | \* | \* |

Таблица для зашифровки сообщения “SERGEEV” с 4 рядами и отступом, равным 2

Пример работы шифра для выбранных параметров:

При использовании стандартного латинского алфавита заглавных букв, числа рядов равного 4 и отступа равного 2, пользуясь приведенной выше таблицей, сообщение “SERGEEV” может быть преобразовано в “EGESRVE”.

Для того, чтобы это сделать, необходимо начертить таблицу, как показано в предыдущем пункте, после чего записать в нее сообщение, начав с верхней левой клетки и после каждой буквы сдвигаясь на одну клетку вправо и на одну клетку вниз. Достигнув нижнего края таблицы, следует начать сдвигаться на одну клетку вправо и на одну клетку вверх, достигнув верхнего края – сдвигаться в изначальном направлении. После чего следует выписать буквы из всех заполненных ячеек, читая их слева направо и сверху вниз.

Тип шифра:

Данный шифр является симметричным, в нем используется исключительно перестановка символов.

Ключ шифра:

Ключом шифра являются два числа (*Number of Rows* и *Offset*).

Оценка сложности атаки «грубой силы»:

Сложность перебора ключей для текста, зашифрованного этим алгоритмом, можно оценить как *((n - 2)^2)/2*, где *n* – это количество букв в исходном тексте. Это происходит потому, что для текста длины *n* имеет смысл проверять количество строк от *2* до *n-1*, а для каждого количества строк *k* необходимо проверить смещение от *1* до *k*.

**Шифр Виженера.**

Задание:

1. Найти шифр в CrypTool 1: *Encrypt/Decrypt-> Symmetric(Classic)*.
2. Зашифровать и расшифровать текст, содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра c выбранным ключом. Убедиться в совпадении результатов.
3. Произвести атаку на шифротекст, используя приложение *Analysis -> Symmetric Encryption (Classic) -> Cipher Text Only -> Vigenere*.
4. Повторить атаку для фрагмента текста из файла English.txt (папка CrypTool/reference). Размер текста не менее 1000 символов.
5. Воспроизведите эту атаку в автоматизированном режиме:
   1. Определите размер ключа с помощью приложения *Analysis -> Tools for Analysis -> Autocorrelation*
   2. Выполните перестановку текста с размером столбца равным размеру ключа приложением *Permutation/Transposition*
   3. Определите очередную букву ключа приложением *Analysis -> Symmetric Encryption (Classic) -> Cipher Text Only -> Caesar*.
6. Самостоятельно изучить атаку, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

Схема и формулы, поясняющие работу шифра:

Пусть даны текст T и ключ K. Представим буквы в виде их порядковых номеров в алфавите. Тогда буквы шифротекста C можно будет вычислить по следующей формуле: *C[i] = (T[i] + K[i mod lK]) mod n*, где *lK* – длина ключа, а *n* – количество символов в алфавите (при условии, что буквы в тексте и в алфавите нумеруются с нуля). Для облегчения использования формулы применяется специальная таблица (tabula recta):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |

Таблица для зашифровки сообщений ключом “MYKEY”

Пример работы шифра для выбранных параметров:

При использовании стандартного латинского алфавита заглавных букв и ключом “MYKEY”, пользуясь приведенной выше таблицей, сообщение “SERGEEV” может быть преобразовано в “ECBKCQT”.

Для того, чтобы это сделать, необходимо разделить текст на отрезки, равные по длине ключу. После этого для каждой буквы каждого отрезка в таблице выбирается элемент, стоящий на пересечении столбца, начинающегося с этой буквы и строки, начинающейся с буквы, стоящей в ключе на той же позиции, что и эта буква в своем отрезке.

Тип шифра:

Данный шифр является симметричным, в нем используется исключительно перестановка символов.

Ключ шифра:

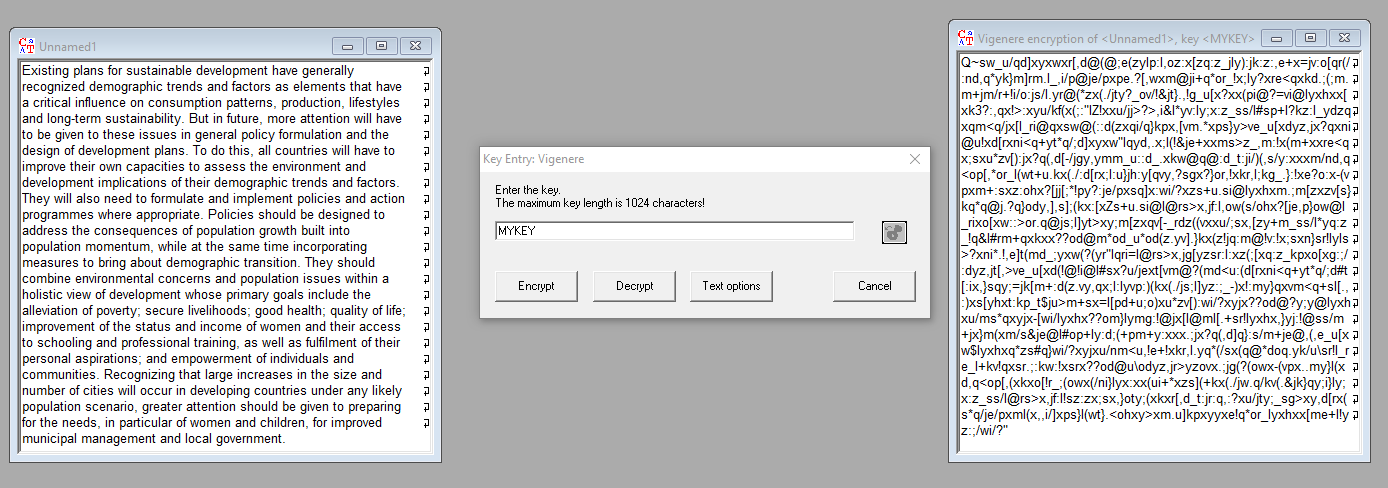
Ключом шифра является строка-ключ, по которой было произведено шифрование.

Оценка сложности атаки «грубой силы»:

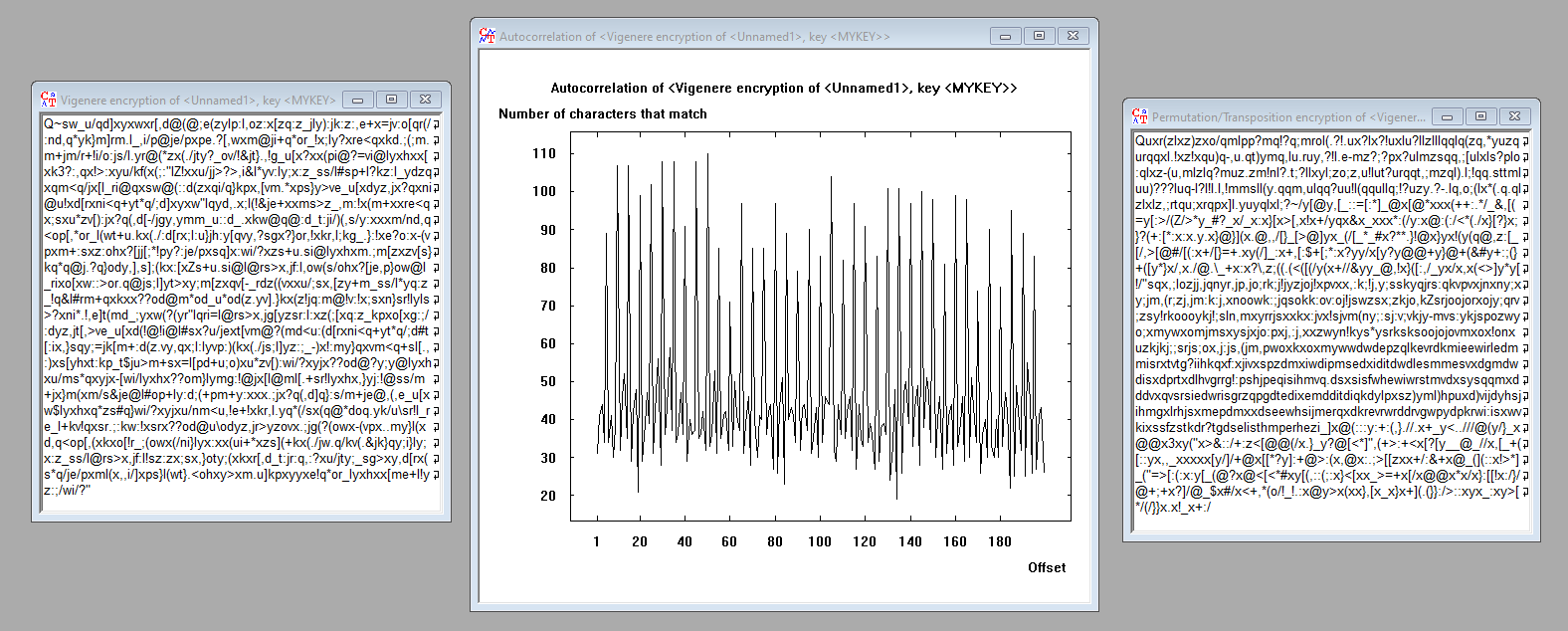
Сложность перебора ключей для текста, зашифрованного этим алгоритмом, можно оценить как*n! / (n-m)!* – количество всевозможных слов-ключей длины *m* (длина ключа), которые могут быть составлены из данного алфавита (длины *n*). При неизвестной длине ключа, имеет смысл перебирать возможные длины от 1 до длины шифротекста.

Описание выполненной процедуры атаки на шифротекст:

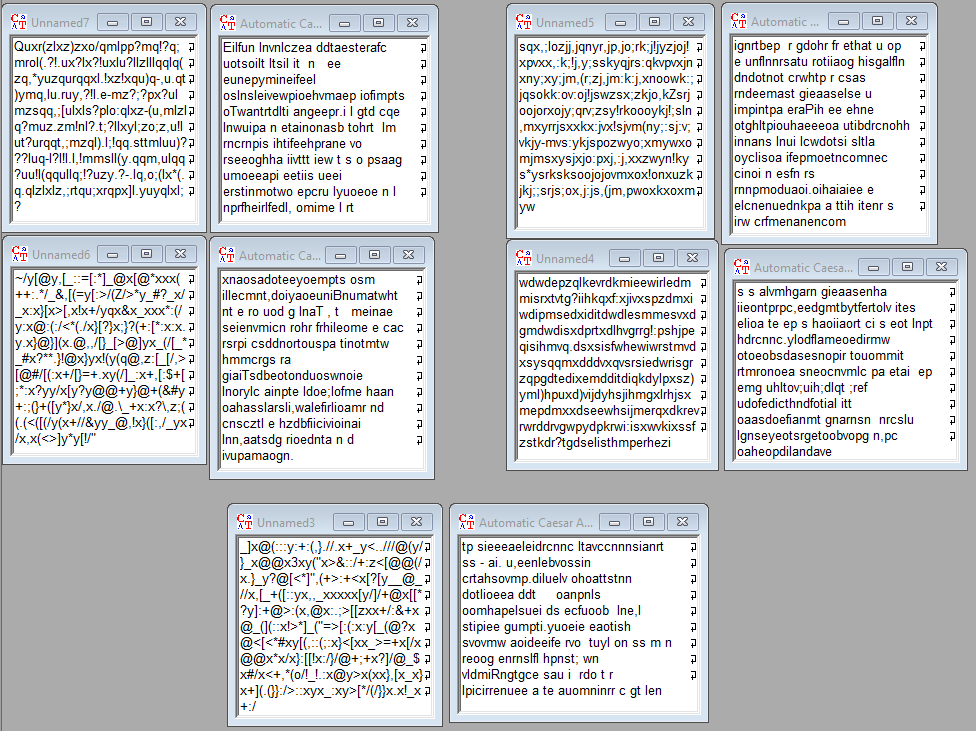
При помощи шифра Виженера был зашифрован один из параграфов текста *english.txt*:

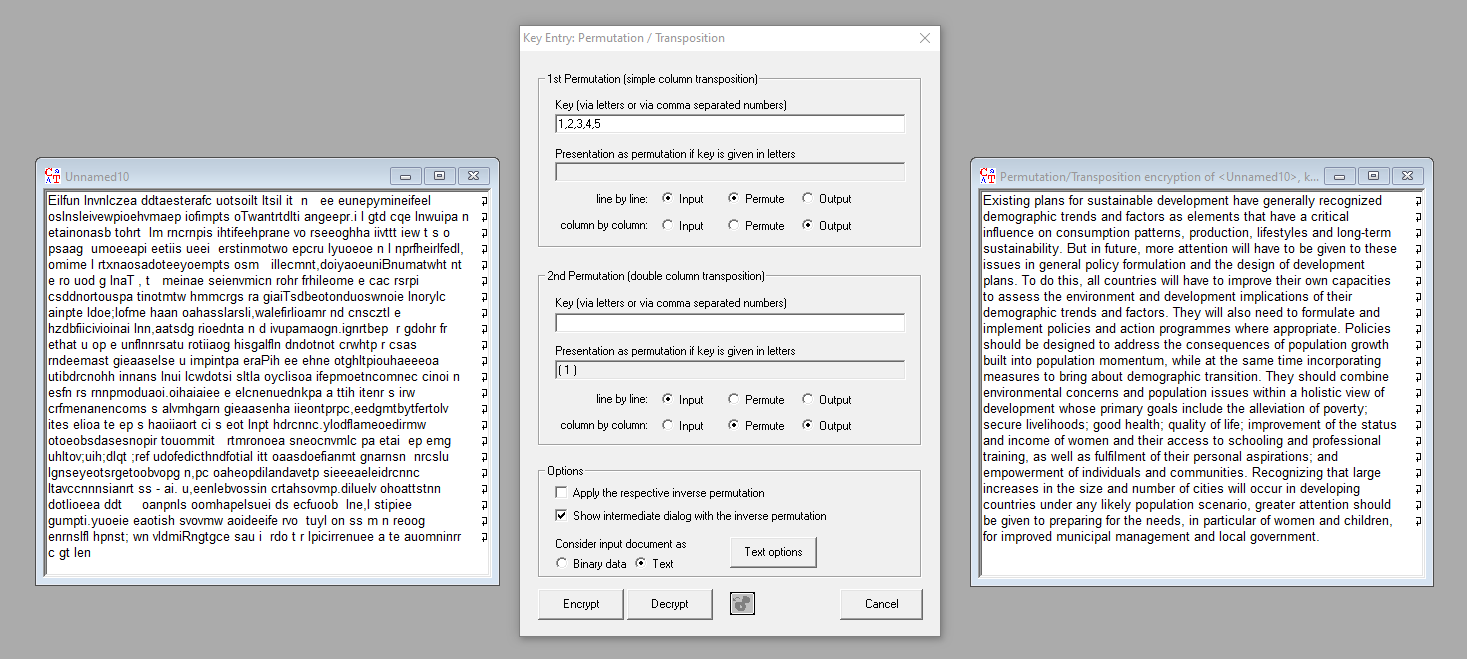
Зашифрованный шифром Виженера текст

При помощи инструмента autocorrelation был выполнен поиск длины ключа, а при помощи инструмента *Permutation/Transposition* – перестановка букв в соответствии с найденной длиной:

Зашифрованный текст с переставленными буквами

Шифротекст был разделен на пять частей, после чего к каждой был применен инструмент расшифровки шифра Цезаря:

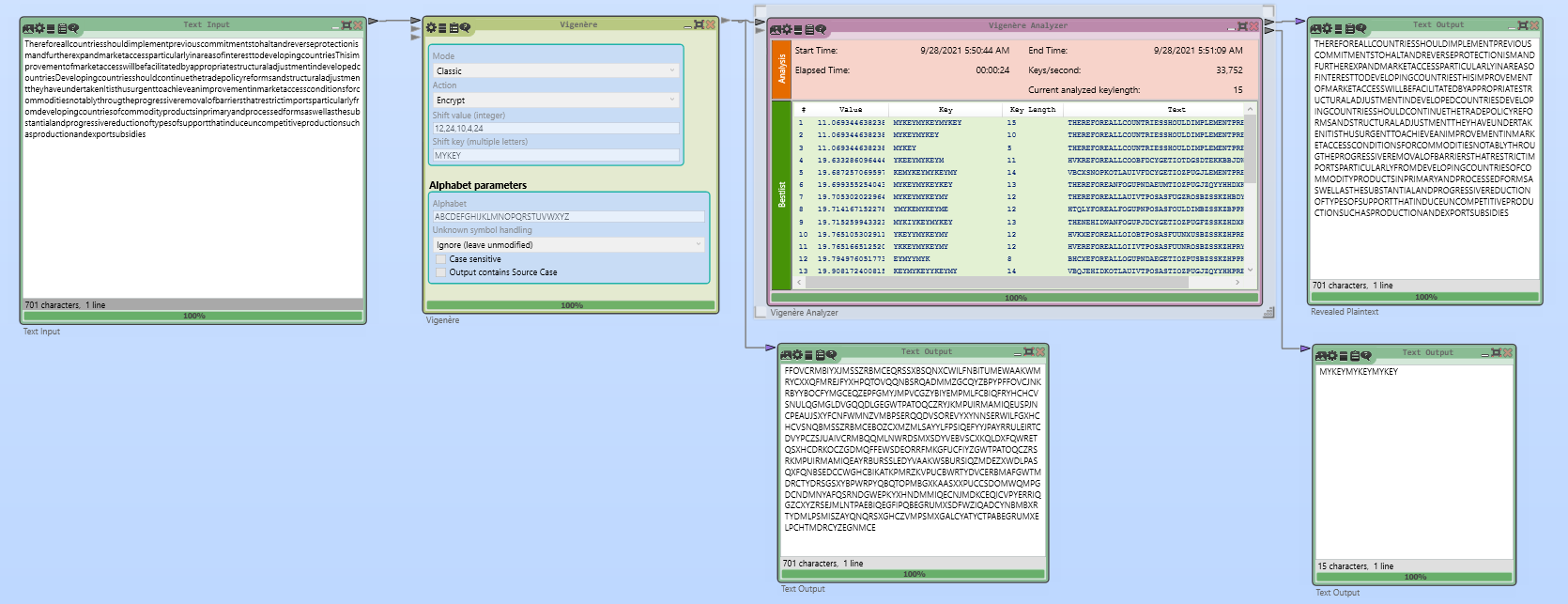
Части дешифрованного текста

После этого части текста были объединены, и в них были обратно переставлены буквы:

Дешифрованный текст

Описание атаки на шифр реализованной в CrypTool 2.0:

Атака на шифр в CrypTool 2.0 реализована так же, как и в CrypTool 1, за исключением того, что виджет дешифровки поддерживает исключительно латинский алфавит заглавных букв, а также, если ключ, представляющий из себя конкатенацию нескольких исходных ключей по какой-то причине показывает лучший результат, чем исходный ключ, в качестве ответа используется конкатенация (в то время как алгоритм из CrypTool 1 удаляет повторы из найденного ключа).

Схема атаки на шифр в CrypTool 2.0

**Шифр ADFGVX.**

Исходное описание шифра:

Шифр ADFGVX состоит из двух стадий: стадии замены и стадии перестановки. Сначала буквы исходного текста заменяются при помощи следующей матрицы:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | A | D | F | G | V | X |
| A | A | B | C | D | E | F |
| D | G | H | I | J | K | L |
| F | M | N | O | P | Q | R |
| G | S | T | U | X | W | X |
| V | Y | Z | 0 | 1 | 2 | 3 |
| X | 4 | 5 | 6 | 7 | 8 | 9 |

Это стандартная матрица для этого шифра, но также буквы и цифры в ней могут быть расположены любым другим образом. Каждая буква исходного текста находится в этой матрице заменяется на пару букв: букву в начале соответствующей ей строки и букву в начале соответствующего ей столбца.

После этого полученный текст записывается в таблицу, первыми буквами столбцов которой являются буквы ключа перестановки:

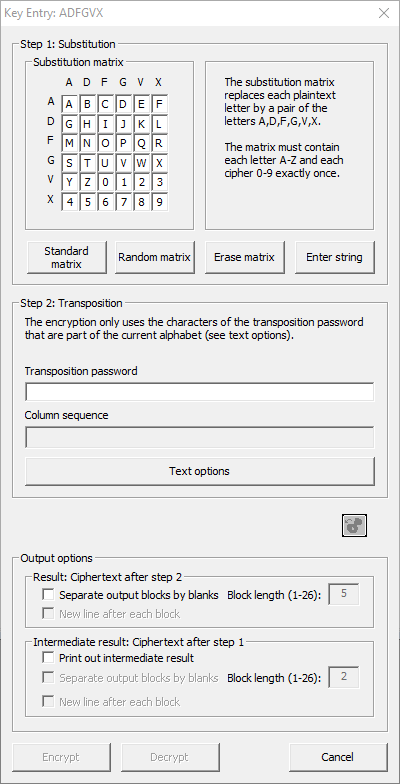
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| M | Y | K | E | Y |
| A | B | C | D | E |
| F | G | H | I | J |
| K | L |  |  |  |

Далее столбцы сортируются в соответствии с лексикографическим порядком букв ключа и получившийся шифротекст выписывается из таблицы слева направо и сверху вниз:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| E | K | M | Y | Y |
| D | C | A | B | E |
| I | H | F | G | J |
|  |  | K | L |  |

Результат: DCABEIHFGJKL

Реализация в CrypTool 1:

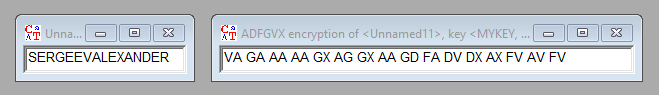
Интерфейс CrypTool для работы с шифром ADFGVX

На данном экране можно настроить матрицу подстановки (*Substitution matrix*) для первого шага алгоритма, ключ перестановки (*Transposition password*), а также результаты вывода (*Output options*).

Пример работы шифра для выбранных параметров:

При использовании стандартного латинского алфавита заглавных букв и ключом “MYKEY”, пользуясь приведенной выше таблицей, сообщение “SERGEEVALEXANDER” может быть преобразовано в “VAGAAAAAGXAGGXAAGDFADVDXAXFVAVFV”.

Для того, чтобы это сделать, необходимо сначала заменить буквы исходного текста на биграммы, как показано в таблице выше, после чего переставить эти биграммы, воспользовавшись отсортированным ключом, как описано выше.

Результат работы шифра в CrypTool 1

Тип шифра:

Данный шифр является симметричным, в нем используется как перестановка, так и замена символов, он - комбинированный.

Ключ шифра:

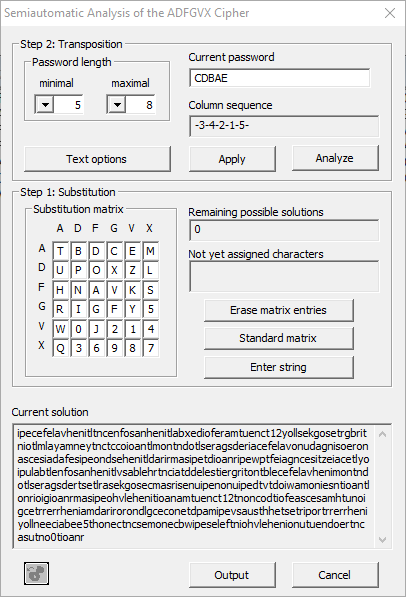
Ключом шифра является строка-ключ, по которой было произведено шифрование. Также частью ключа может являться матрица замены, если была использована не стандартная.

Оценка сложности атаки «грубой силы»:

Сложность перебора ключей для текста, зашифрованного этим алгоритмом, можно оценить как*m!* – количество всевозможных перестановок *m* (длина ключа) столбцов. При неизвестной длине ключа, имеет смысл перебирать возможные длины от 1 до длины шифротекста. При использовании нестандартной матрицы замены, необходимо перебрать *n!* вариантов заполнения матрицы, где *n* – длина алфавита.

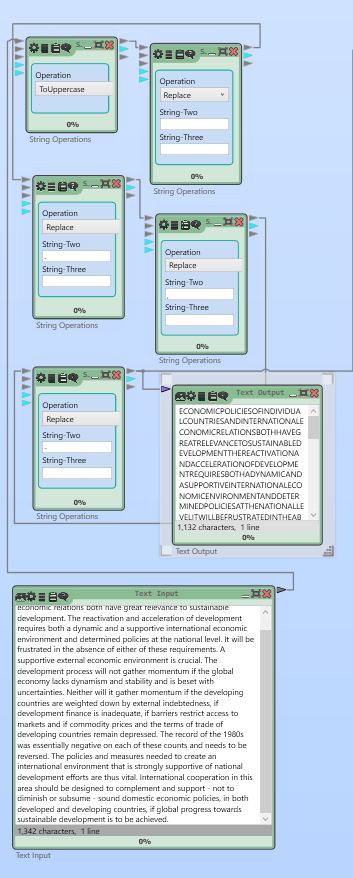
Описание атаки на шифр с использованием утилит CrypTool 1:

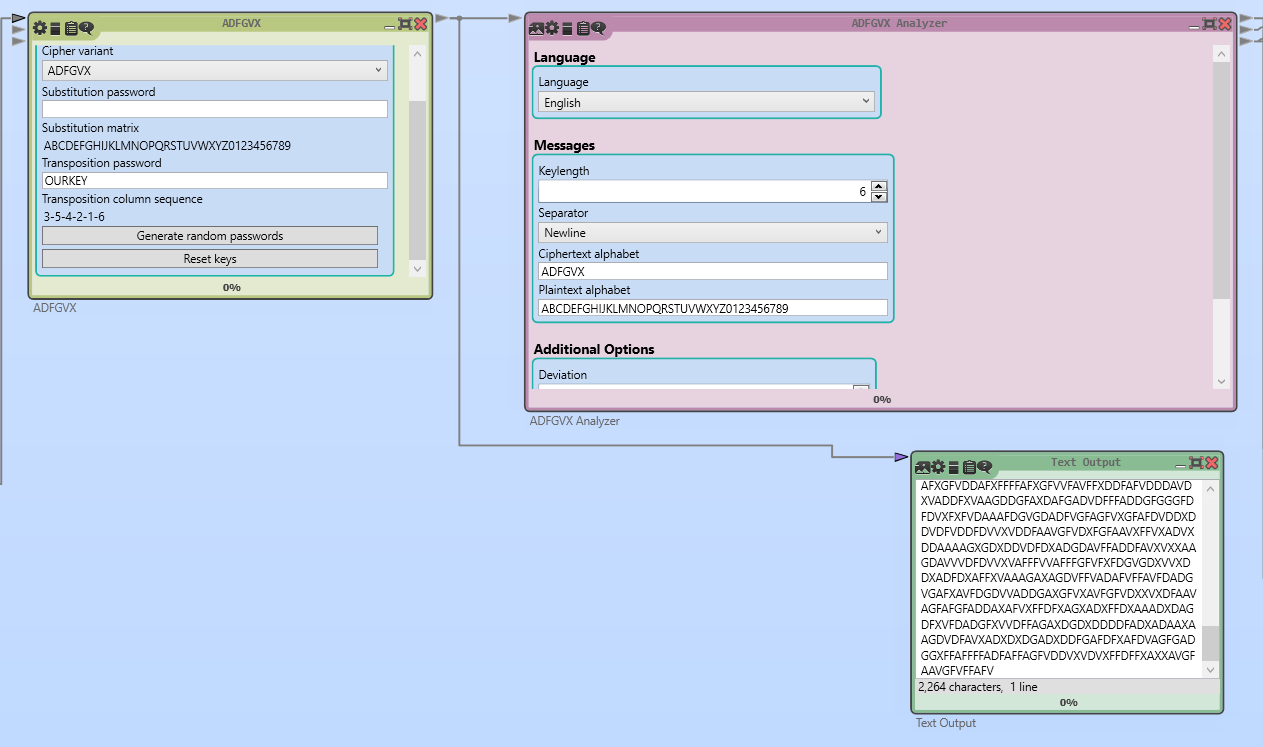
Утилита CrypTool чаще всего не может найти верный ключ для дешифровки шифротекста. По моему мнению это связано с невозможностью задать единую (стандартную) матрицу замены, которая генерируется для каждого ключа автоматически, что вызывает ошибки при частотном анализе текста. Успешно атаковать шифр получилось только с изначально заданным ключом перестановки.

Интерфейс анализатора шифра ADFGVX в программе CrypTool 1

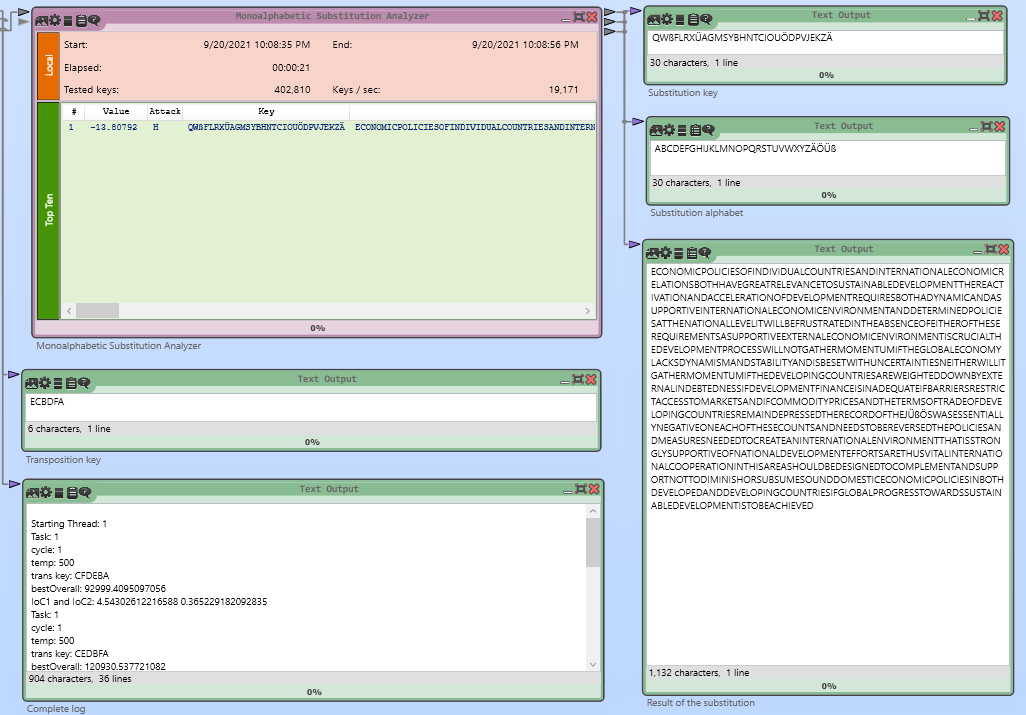
Описание атаки на шифр реализованной в CrypTool 2.0:

Стандартный анализатор шифра в программе CrypTool 2.0работает так же, как в программе CrypTool 1, но, вследствие возможности более гибкой настройки, успешно дешифрует шифротекст.

Схема, подготавливающая текст к шифрованию путем удаления неверно обрабатываемых символов

Схема, выполняющая шифрование текста

Схема, выполняющая стандартную атаку на шифр

Атака на шифр ADFGVX по словарюреализована в программе CrypTool 2.0 похожим образом. Предполагается, что ключом шифра является некое слово, содержащееся в полном словаре английского языка. Произведя перестановку шифротекста при помощи этого предполагаемого ключа можно, используя метод частотного анализа биграмм на получившемся тексте, понять, насколько правдоподобно предположение относительно ключа. Если результат сильно превышает 1/26 (результат для случайного набора букв), скорее всего, ключ угадан правильно, и осталось только расшифровать матрицу замен.**Выводы.**

В ходе выполнения лабораторной работы были исследованы следующие шифры: RailFence, Vigenere и ADFGVX, а также получены навыки работы с ними вручную и с помощью специальных программ CrypTool 1 и CrypTool 2.

Шифр RailFence:

Это шифр перестановочного типа, его ключом являются два числа: количество строк в шифровальной таблице и смещение относительно ее начала. Шифр уязвим к атаке перебором, так как его ключом являются два числа, вариантов для подбора которых сравнительно не много. Вследствие этого не является криптографически стойким.

Шифр Vigenere:

Это шифр перестановочного типа, его ключом является строка-ключ (по сути представляющая из себя набор чисел – ключей шифра Цезаря). Шифр уязвим к атаке автокорреляционным методом с последующим статистическим и/или частотным анализом или простым перебором. Не является стойким, если для задачи взлома использовать описанные выше методы вместо полного перебора.

Шифр ADFGVX:

Это шифр комбинированного типа, его ключом является строка-ключ на стадии перестановки и (опционально) матрица подстановки на стадии замены. Шифр уязвим к атаке на основе знания части открытого текста (2х и более сообщений с одинаковыми частями или сообщений одинакового размера), заключающимся в определении перестановки биграмм и частотному анализу шифрующей матрицы. Без знания частей открытого текста является достаточно криптостойким за счет использования биграмм и перестановок.