**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра ИБ**

**отчет**

**по лабораторной работе №2**

**по дисциплине «Криптографические методы защиты информации»**

**Тема: Изучение классических шифров Substitution, Permutation/Transposition, Vigenere**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 5381 |  | Кобылянский А.В. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2018

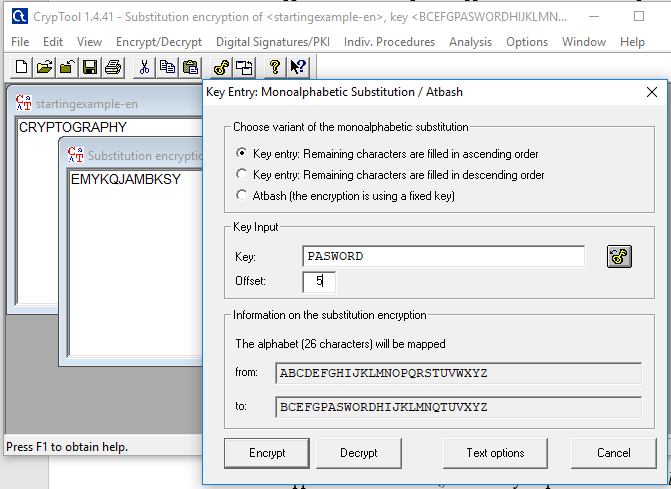
**Цель работы**

Исследовать шифры Substitution, Permutation/Transposition, Vigenere и получить практические навыки работы с ними, в том числе и в программном продукте Cryptool 1 и 2.

**1. Шифр моноалфавитной подстановки (Substitution)**

**1.1 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 и смещением *Offset* Убедиться в совпадении результатов.
3. Выполнить зашифрование и расшифрование с различными паролями и смещениями *Offset* и разобраться как формируется алфавит шифрограммы.
4. Выбрать абзац (примерно 600 символов) из файла *English.txt* (папка *CrypTool/reference*) и зашифровать его.
5. Выполнить атаку на шифротекст, используя приложение из *Analysis-> Symmetric Encryption(classic)-> Cipher Text Only.*
6. Повторить шифрование и атаку для тестов примерно в 300 и в 150 символов
7. Изучите ручное расшифрование для текстов менее 300 символов.
8. Выбрать новый абзац (примерно 600 символов) из файла *English.txt* (папка CrypTool/reference) и зашифровать его.
9. Расшифровать этот абзац, используя приложение *Analysis-> Tools for Analysis* и *Analysis-> Symmetric Encryption(classic)-> Manual Analysis.*
10. Зашифруйте текст из 200 символов, сохраните ключ, и передайте коллеге для расшифровки.
11. Самостоятельно изучите атаки, реализованные CrypTool 2, опираясь на Help и ссылки на статьи.

**1.2 Реализация в CrypTool 1.0 (скриншот, спецификация параметров).**

Key – ключ шифрования

Offset – смещение.

Можно выбрать в каком порядке будут идти символы, не вошедшие в ключ – A -> Z или Z -> A.

Так же можно переключиться на шифр Atbash, который является частным случаем Substitution (key = ZYXWVUTSRQPONMLKJIHGFEDCBA, offset = 0).

**1.3. Пример работы шифра для выбранных параметров.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Открытый текст** | **KEY** | **Offset** | **Результат шифрования** |
| ANIME | TEST | 0 | TLGKB |
| ANIME | TEST | 20 | AOJNF |
| ANIME | RUST | 20 | ANIME |

**1.4 Тип шифра**

Тип шифра – замена.

**1.5 Ключ шифра**

Ключ шифра – кодовое слово (key) и отступ (offset).

Так же в качестве ключа может выступать некоторая перестановка используемого алфавита.

**1.6 Оценка сложности атаки “грубой силы”**

Данным шифром можно задать любую перестановку выбранного алфавита, выбрав эту перестановку в качестве key, а offset положив 0. Обратно, данный шифр может задать только перестановку алфавита.

Тогда, при длине алфавита n, имеем

вариантов для перебора.

**1.7 Описание атаки на шифр с использованием утилит CrypTool 1.0.**

Cryptool-1 предлагает 2 метода автоматических атак.

Первый метод основан на анализе частотного распределения символов в сообщении. Подходит и для текстов без пробелов.

Второй метод основан на списке самых популярных слов в языке. Он пытается подставлять самые популярные слова вместо зашифрованных слов, постепенно восстанавливая ключ шифрования.

Так же можно пытаться расшифровать вручную.

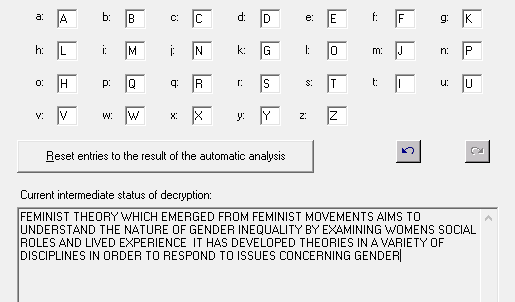
**1.8 Результат расшифровки перехваченного от коллеги текста.**

Перехваченный текст:

Feitjtrs soelqy, wotco eieqked fqli feitjtrs ilveiejsr, atir sl ujdeqrsajd soe jasuqe lf kejdeq tjepuahtsy by exaitjtjk wliej'r rlctah qlher ajd htved exneqtejce;

ts oar devehlned soelqter tj a vaqtesy lf dtrctnhtjer tj lqdeq sl qernljd sl trruer cljceqjtjk kejdeq

Расшифровка и ключ:



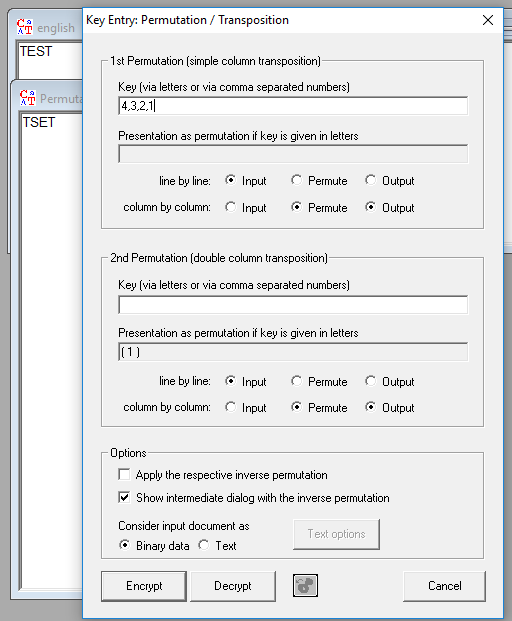
**1.9 Описание атаки на шифр реализованной в CrypTool 2.0.**

В CrypTool 2.0 ключ ищется алгоритмом hill climbing-а. Мы генерируем случайную перестановку алфавита и пытаемся последовательными маленькими изменениями этой перестановки дойти до перестановки, расшифровывающий данный текст. Если маленькое изменение приблизило текст к расшифрованному, то оставляем полученную перестановку как текущую, если ухудшило, то отбрасываем её и пытаемся сделать другое изменение. Близость текста к нормальному (fitness) определяется как логарифм среднего арифметического вероятностей появления n-грам в нормальном тексте на предполагаемом языке.

**2. Шифр двойной перестановки (Permutation/Transposition)**

**2.1 Задание**

1. Найти шифр в CrypTool 1: *Encrypt/Decrypt-> Symmetric(Classic).*
2. Зашифровать и расшифровать текст, содержащий ФамилиюИмяОтчество (транслитерация латиницей) вручную и с помощью шифра c ключами для перестановки столбцов и строк.Убедиться в совпадении результатов.
3. Выполнить зашифрование и расшифрование с различными ключами и с различными вариантами перестановки матрицы с текстом по строкам и столбцам. Разобраться с параметрами утилиты.
4. Зашифровать текст, содержащий ФамилиюИмяОтчество и провести атаку, основанную на знании исходного текста *Analysis-> Symmetric Encryption(classic)-> Known Plaintext.*
5. Зашифровать текст с произвольным сообщением в формате «DEAR messagе THANKS», используя только одинарную перестановку.
6. Передайте шифровку соседу, для расшифрования при условии, что формы обращения и завершения письма известны.
7. Самостоятельно изучите атаки, реализованные в CrypTool 2, опираясь на Help и ссылки на статьи.

**2.2. Реализация в CrypTool 1.0**

key – перестановка. Номера переставляемых столбцов (строк) через запятую. Если перестановка равна , то это означает, что мы записываем текст в таблицу с количеством столбцов (строк) равным и затем первый столбец (строку) переставляем на позицию , второй на позицию и т.д.

Ниже можно выбрать, как мы заносим текст в таблицу, как переставляем, как читаем результат - по строкам или по столбцам.

Можно выполнить 2 перестановки последовательно.

В блоке options можно выбрать, как рассматривать зашифровываемые данные – как набор байт или как текст (не переставлять пробелы, не делать различий между регистрами и т.д.). Здесь же настраивается, применить прямую перестановку или обратную (как пр расшифровывании).

**2.3 Пример работы шифра для выбранных параметров.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Открытый текст** | **1st permutation****(столбцы)** | **2nd permutation****(строки)** | **Результат шифрования** |
| ABCD | (2, 1) | (1) | BDAC |
| ABCD | (1) | (2, 1) | CADB |
| ABCD | (2, 1) | (2, 1) | DBCA |
| ABCD | (4,3,2,1) | (1) | DCBA |

**2.4 Тип шифра**

Тип шифра – перестановка.

**2.5 Ключ шифра**

Ключ шифра – 2 перестановки и к чему они применяются – к столбцам или к строкам.

**2.6 Оценка сложности атаки “грубой силы”**

Данный алгоритм шифрования может реализовать любую перестановку исходного текста. Обратно, всякое действие данного шифра – это некоторая перестановка исходного текста.

Значит, сложность перебора будет

где n – длина текста.

**2.7 Описание атаки на шифр с использованием утилит CrypTool 1.0.**

В CrypTool 1.0 для шифра с одинарной перестановкой можно найти потенциальные ключи шифрования, зная открытый текст и его зашифрованную версию. После получения потенциальных ключей, можно попытаться применить их для расшифровки другого текста, зашифрованного тем же алгоритмом с тем же ключом.

**2.8 Результат расшифровки перехваченного от коллеги текста.**

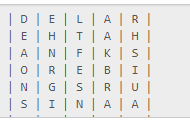
Зашифрованный текст:

DELA REHT AHANFK SOR EBING SRUSINA ANIPM ERORGAMMSER ONO EF THE EBST NI THIA SPRT FO OUR VUIERISTY MBAYE TAHNKS

Параметры шифрования:

https://pp.userapi.com/c846019/v846019551/edce3/brhV71ObeJE.jpg

Попытка расшифровать текст при длине ключа 5:



Попробуем перестановку (1, 2, 5, 3, 4)

DEAR LEHA HTANKS FOR BIENG RUSSIAA NNIME PROGARMMERS ONE FO THE BEST IT NHIS PART OO FUR UIVERSTIY MAYBE THNAKS

Текст почти расшифрован, но не до конца. При длине ключа 5 его невозможно корректно расшифровать. То, что текст почти расшифрован говорит нам, что длина ключа кратна 5. Попробуем ключ длиной 10 и перестановку (1, 2, 5, 3, 4, 6, 7, 9, 8, 10)

Результат:

DEAR LEHA THANKS FOR BEING RUSSIAN ANIME PROGRAMMERS ONE OF THE BEST IN THIS PART OF OUR UIVERSITY MAYBE THANKS

**2.9 Описание атаки на шифр реализованной в CrypTool 2.0.**

CrypTool 2.0 позволяет расшифровывать тексты, зашифрованные двумя перестановками по методу разработанному George Lasry в 2013 году.

**3. Шифр Виженера (Vigenere)3.1. 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.

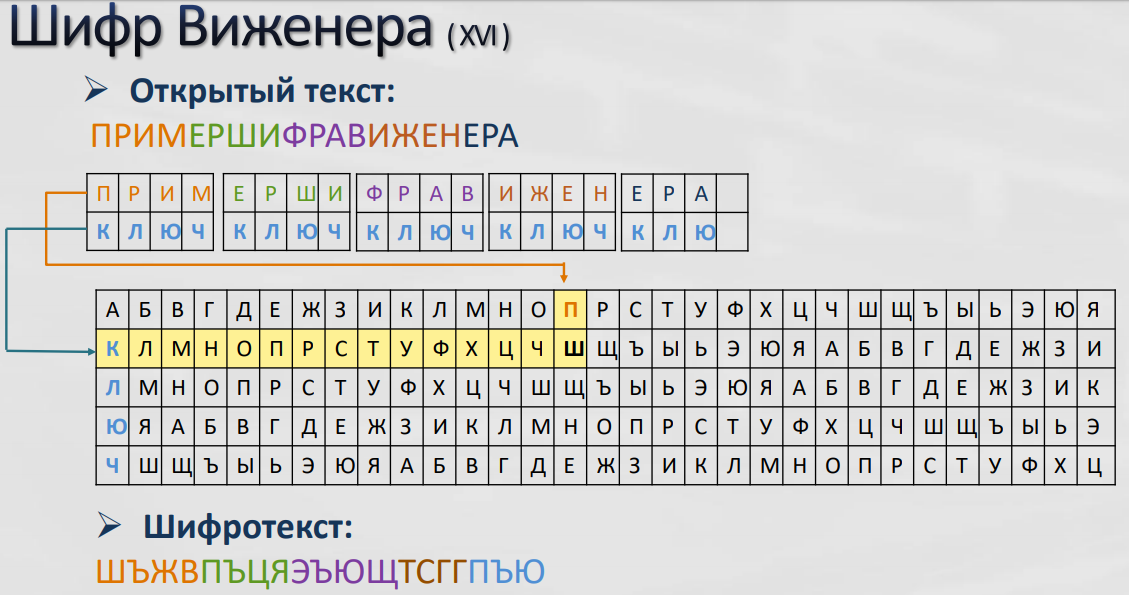
5. Воспроизведите эту атаку в автоматизированном режиме:

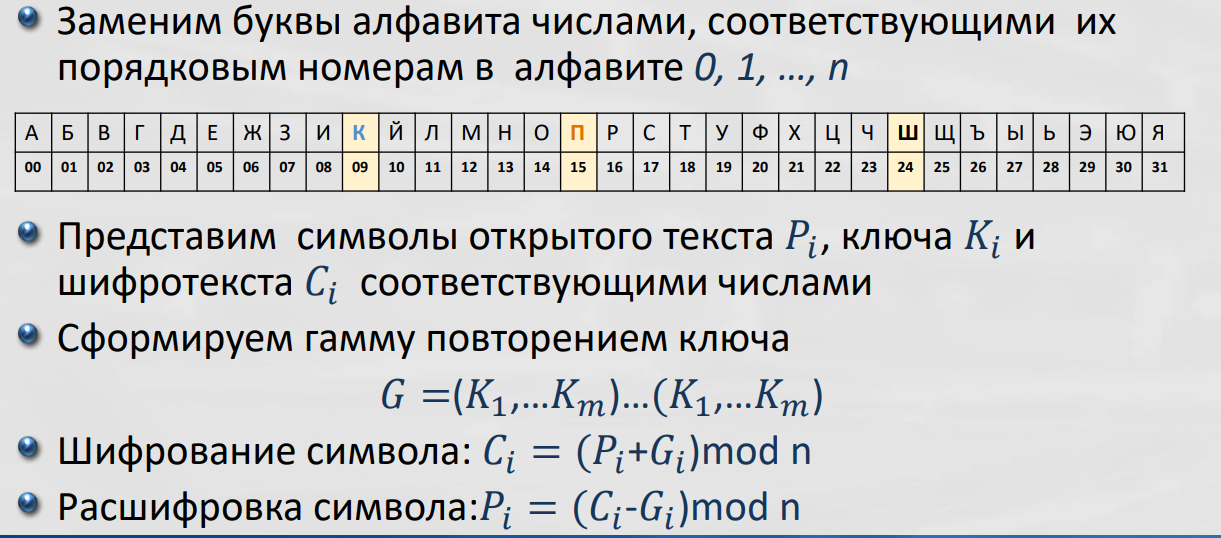
a. Определите размер ключа с помощью приложения Analysis-> Tools for Analysis-> Autocorrelation

b. Выполните перестановку текста с размером столбца равным размеру ключа приложением Permutation/Transposition

c. Определите очередную букву ключа приложением Analysis-> Symmetric Encryption(Classic)-> Cipher Text Only->Caesar.

6. Самостоятельно изучите атаки, реализованные CrypTool 2, опираясь на Help и ссылки на статьи.

**3.2 Схема и формулы, поясняющие работу шифра.**



**3.3 Пример работы шифра для выбранных параметров.**

|  |  |  |
| --- | --- | --- |
| **Открытый текст** | **Key** | **Результат шифрования** |
| TEST | TEST | MIKM |
| TEST | OK | HOGD |
| TEST | AA | TEST |
| TEST | KWVR | DANK |

**3.4 Тип шифра**

Тип шифра – замена.

**3.5 Ключ шифра**

Ключ шифра – кодовое слово.

**3.6 Оценка сложности атаки “грубой силы”**

Т.к. кодовое слово может быть произвольной длины и состоять из произвольных символов, то мы можем из любого текста получить любой другой, подобрав подходящее кодовое слово длиной с шифруемый текст.

Полный перебор в таких условиях выглядит бессмысленно и потребует

попыток, где – длина алфавита, – количество символов в сообщении.

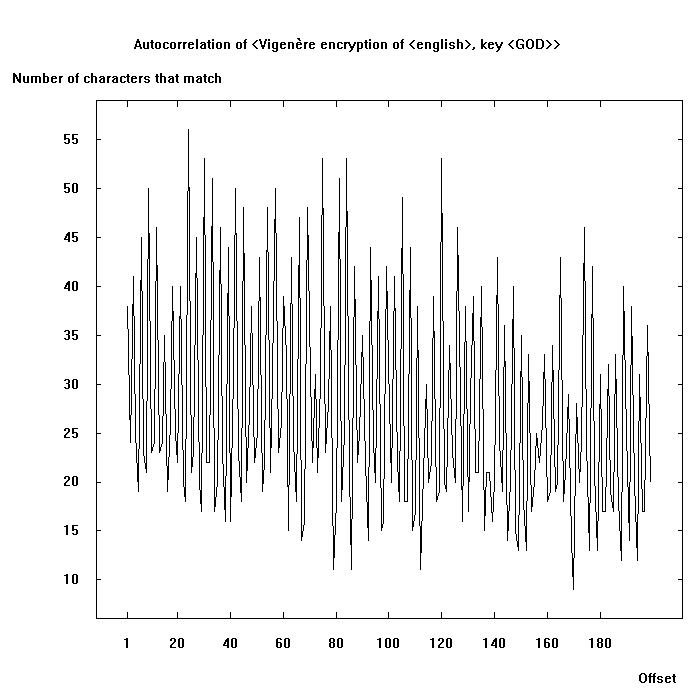
При ограничении на ключ, при котором символы в ключе не повторяются, перебор потребует:

шагов.

**3.7 Описание выполненной процедуры атаки на шифротекст и результат (ключ) этой атаки.**

Зашифруем отрывок из English.txt длиной ~900 символов шифром vigenere с ключом “GOD”.

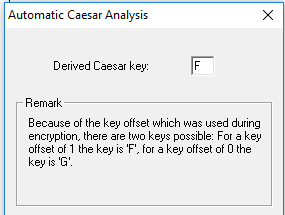
Воспользуемся инструментом Analysis/Tools for analysis/Autocorrelation.



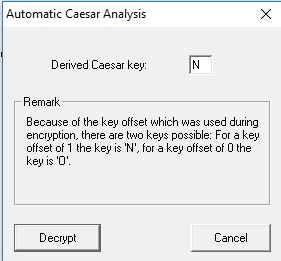
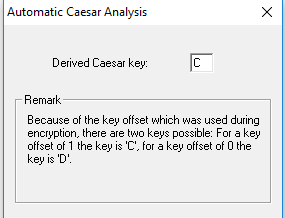
Локальные максимумы всегда на отступах кратных 3.

Зашифруем наш зашифрованный текст шифром Permutation/Transposition с одиночной перестановкой столбцов (1,2,3), чтобы разбить текст на три части, зашифрованные с одним и тем же сдвигом.

Скопируем первые 300 символов полученного текста и применим автоматическую расшифровку кода цезаря к этому фрагменту. Получим первую букву шифра – “G”



Аналогично получим 2 и 3 буквы шифра “O” и “D”.

**3.8 Описание атаки на шифр реализованной в CrypTool 2.0.**

В CrypTool 2.0 перебираются различные длины ключей и для каждой длины пытаются найти ключ методом hill climbing-а – оптимизируя fitness для четверок букв (4-grams) в предполагаемом языке.

**Вывод**

* Шифр “Substitution”

Тип шифра – замена.

Ключ шифра – кодовое слово (key) и отступ (offset).

При длине алфавита n сложность равна

* Шифр “Permutation/Transposition”

Тип шифра – перестановка.

Ключ шифра – 2 перестановки и к чему они применяются – к столбцам или к строкам.

При длине теста k сложность расшифровки равна

* Шифр “Vigenere”

Тип шифра – замена.

Ключ шифра – кодовое слово.

При длине алфавита n, длине текста k полный перебор потребует шагов.

При ограничении на ключ, при котором символы в ключе не повторяются, перебор потребует шагов.