МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И.УЛЬЯНОВА (ЛЕНИНА)
Кафедра ИБ

ЛАБОРАТОРНАЯ РАБОТА №2

по дисциплине «Криптография и защита информации»
Тема: Изучение классических шифров Substitution, Permutation/Transposition, Vigenere

Студент гр. 6304 _____ Корытов П.В.
Преподаватель _____ Племянников А.К.

Санкт-Петербург
2019

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

1.1. Описание шифра

Параметры — Key, Offset

1. Первый шаг:
   - Удаление всех элементов алфавита, которые присутствуют в кодовом слове
   - Удвоенные элементы кодового слова слова сливаются в один
2. Второй шаг
   - Задается значение смещение первого элемента кодовго слова (Offset)
   - По значению смещения определяется количество символов алфавита, полученного после удаления его элементов, которые будут предшествовать вставке когодового слова, после которого запись имеющегося алфавита

1.2. Формулировка задания

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 с выбранным ключом и смещением Offset≠ 0. 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 (пап-

ка 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.

1.3. Ход работы

1. Найден шифр в CrypTool 1.

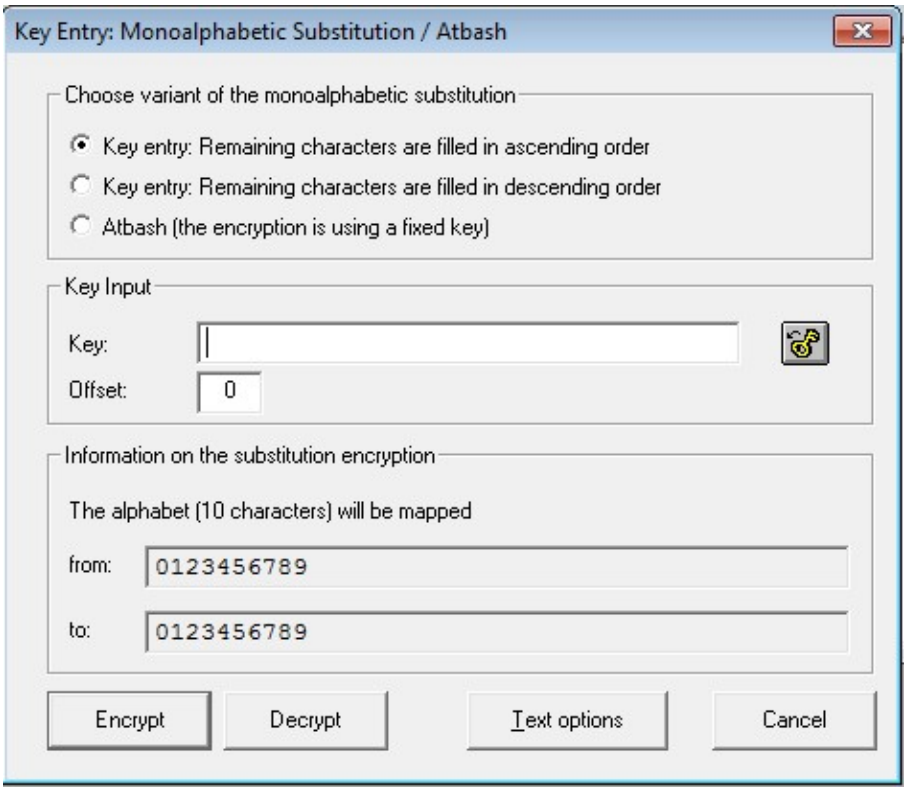


Рисунок 1. Параметры шифра моноалфавитной подстановки в CrypTool 1

2. Фамилия автора — KORYTOV, выбранный ключ — PAVEL. Offset = 5

Таблица 1. Таблица шифрования

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

- Результат шифрования фамилии: HMQYSMU

- Результат расшифрования: KORYTOV

Результаты совпадают.

3. Offset сдвигает позицию Key в полученном алфавите
4. Выбран абзац из текста и зашифрован

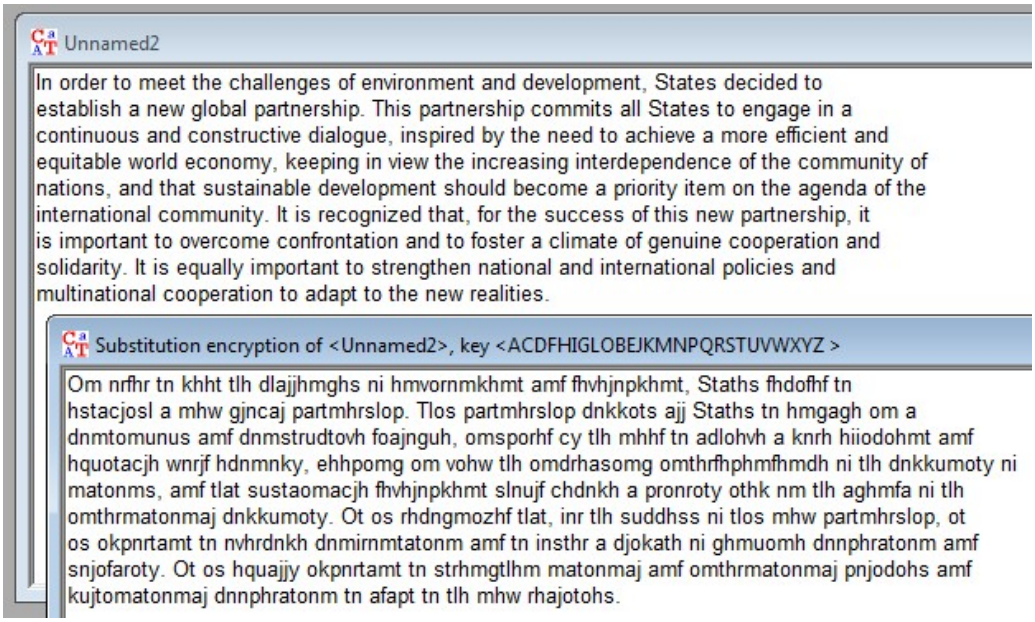


Рисунок 2. Шифрование текста подстановкой

5. Успешно выполнена атака на текст. Результаты на рисунке 3
6. Выполнены атаки на более короткие тексты:
    - Для текста длиной в 300 символов неправильно определена одна буква
    - Для текста длиной 150 символов около трети букв определено неверно
7. Ручное расшифрование текста длиной менее 300 символов возможно с помощью частотного анализа и знания слов языка, но является непростой задачей. Подробности в пункте 9.
8. Зашифрован новый абзац текста
9. Проведена ручная расшифровка:
    - Определена точка расхождения гистограмм частоты букв оригинала и шифротекста. Это смещение — 3. Буква ключа — “D”
    - С другой стороны алфавита расхождение начинается с “U”, значит, это часть ключа
    - После этого поиском корелляций между диаграммами можно установитьещё

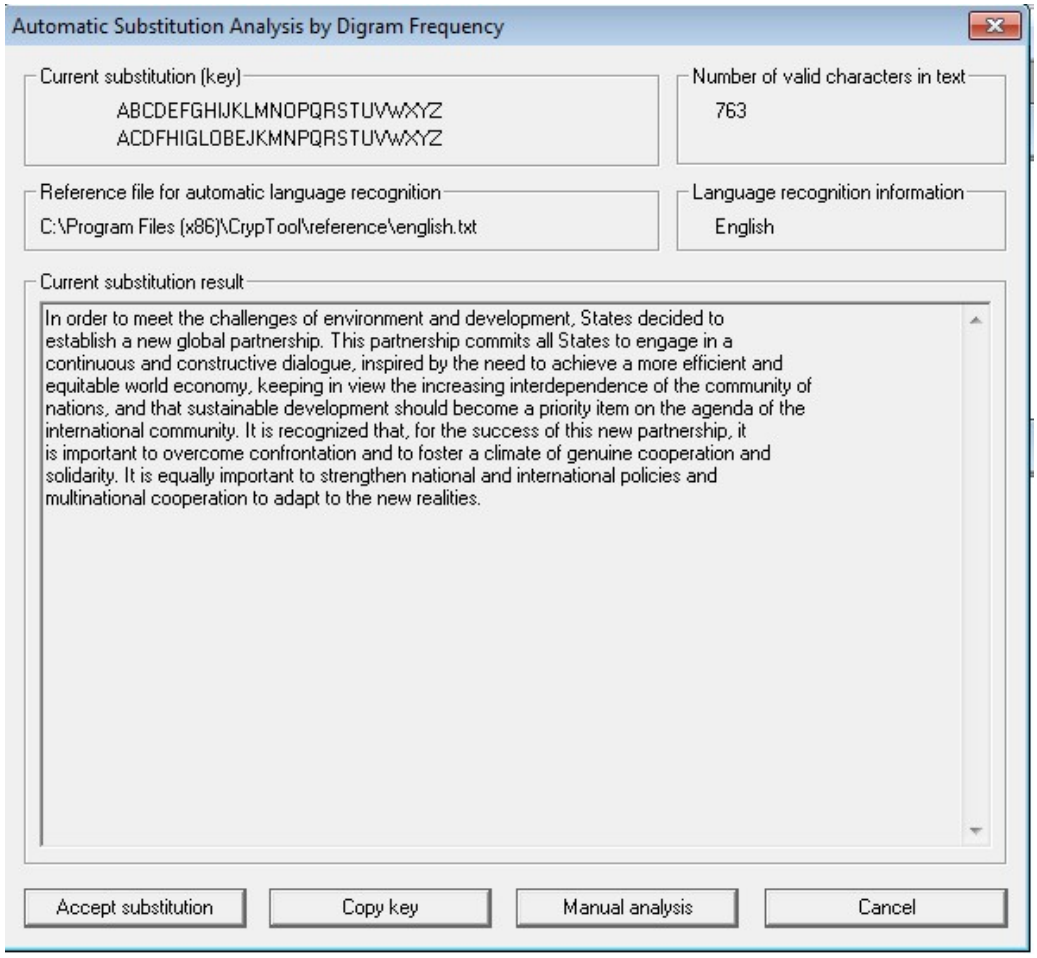


Рисунок 3. Результаты атаки на зашифрованный текст

- После того, как известна большая часть букв, расшифровка оставшихся — простая задача, т.к. слова становсятся различимы.

10. Коллеге зашифрована следующая циатата Ричарда Докинза из книги “Delusion God”:
    “There is something infantile in the presumption that somebody else (parents in the case of children, God in the case of adults) has a responsibility to give your life meaning and point Richard Dawkins”
    Ключ — “ATHEISM”, смещение — 13
11. От коллеги получена следующая шифровка:
    “Wf fxnudjrf yns, fvfuy joasuf rajujq fvfuy rbqbpjd anwfu, fvfuy jpdsurjnp ng qif jpgfupbm bevfurbuy, fvfuy mfhjnp fvfuy dnphufhbqjnp bpe ejbcnmjdbm rfdq. Qisr dsurfe efonp bpe fvfuy ejbcnmjdbm mfhjnp wf beksuf yns. Dfbrf qn efdfjvf isobp dufbqsufr bpe qn hjvf qn qifo qif anjrnp ng fqfupbm Afuejqjnp.”
    Автоматическая расшифровка дает не очень хороший результат, как видно на рисунке 4
    С помощью ручной расшифровки удалось восстановить текст. Результаты

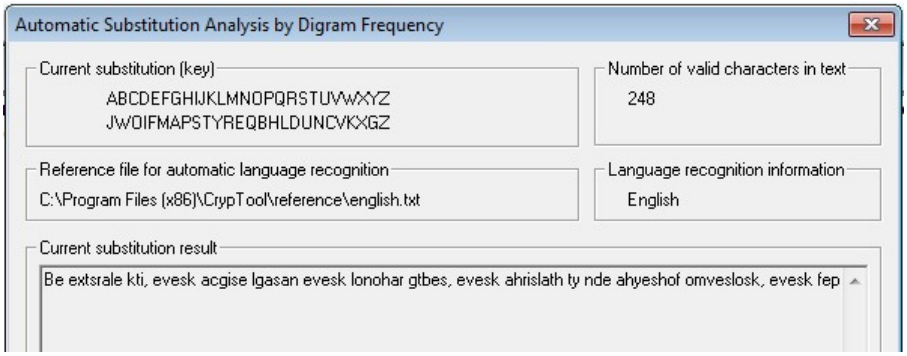


Рисунок 4. Автоматическая расшифровка полученного текста

на рисунке 5

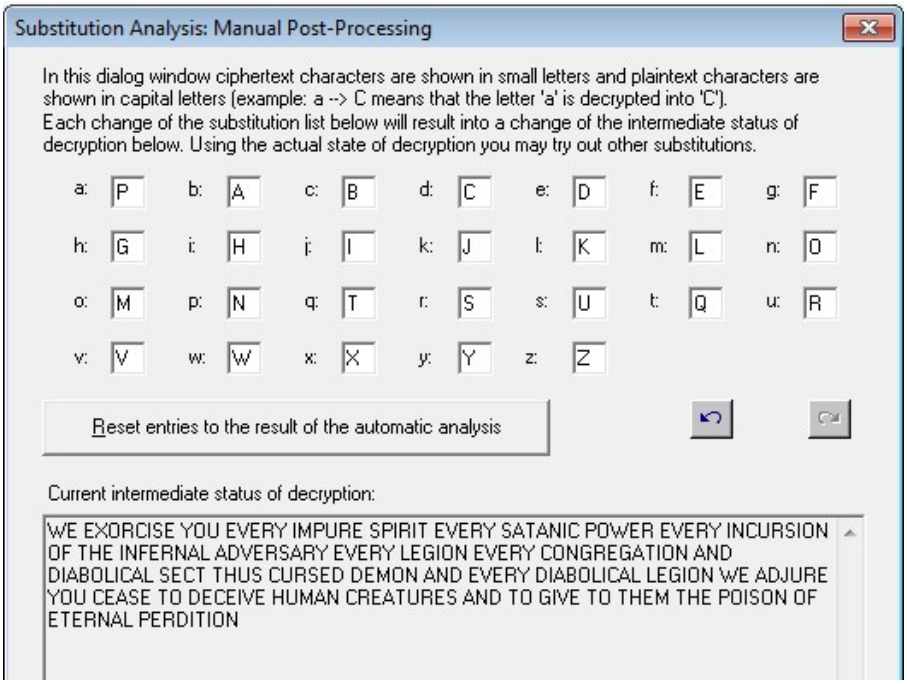


Рисунок 5. Результаты расшифровки

Как видно, содержание текста — молитва, изгоняющая демонов. Предположительно, смещение распределения из-за церковных терминов осложнило расшифровку текста.

12. В CrypTool 2 реализована атака на шифр путем частотного анализа с восхождением к вершине. Т.е.

2. Шифр двойной перестановки (Permutation / Transposition)

2.1. Принцип работы шифра

Текст записывается в матрицу, производится перестановка строк и столбцов

2.2. Формулировка задания

1. Найти шифр в CrypTool 1: Encrypt/Decrypt-> Symmetric (Classic).
2. Зашифровать и расшифровать текст, содержащий ФамилиюИмяОтчество (транслитерация латиницей) вручную и с помощью шифра с 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 message 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.

2.3. Ход работы

1. Найден шифр в CrypTool 1. Параметры шифра на рисунке 6
2. Текст — KORYTOVPAVELVALERIEVICH. Ключ — DACB, DEFBAC.

	D	**A**	**C**	**B**
D	K	O	R	Y
E	T	O	V	P
F	A	V	E	L
B	V	A	L	E
A	R	I	E	V
C	I	C	H	

	A	**B**	**C**	**D**
D	O	Y	R	K
E	O	P	V	T
F	V	L	E	A
B	A	E	L	V
A	I	V	E	R
C	C		H	I

	D	**E**	**F**	**B**	**A**	**C**
A	O	O	V	A	I	C
B	Y	P	L	E	V	R
C	V	E	L	E	H	K
D	T	A	V	R	I	

	A	**B**	**C**	**D**	**E**	**F**
A	I	A	C	O	O	V
B	V	E	R	Y	P	L
C	H	E	K	V	E	L
D	I	R		T	A	V

Поскольку длина текста — 23, число операций немного больше. Результат — IVHIAEERCRKOYVTOPEAVLLV.

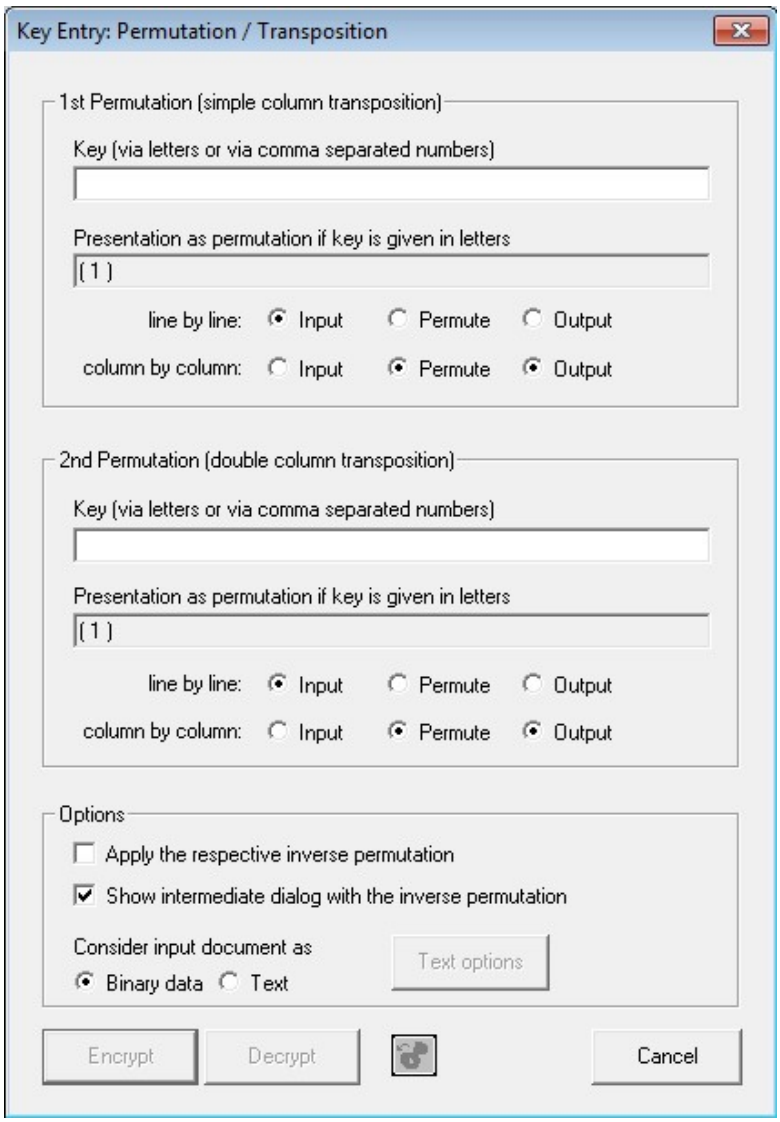


Рисунок 6. Параметры шифра Permutation / Transposition

CrypTool дает тот же результат — см. рисунок 7

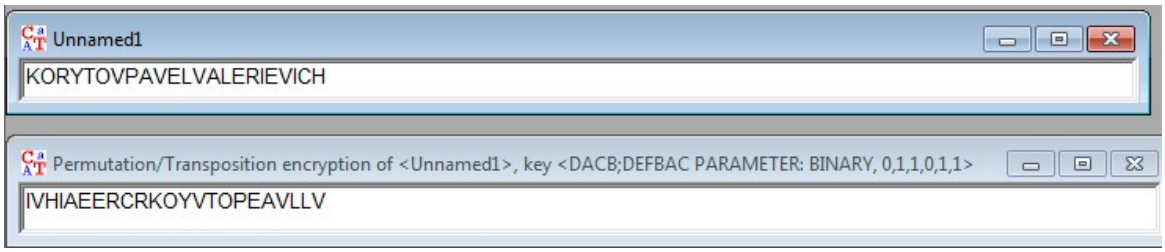


Рисунок 7. Результат CrypTool

Для расшифрования нужно получить обратную перестановку для ключей. Это несложно сделать:

D	**A**	**C**	**B**
A	*B*	*C*	*D*
A	**B**	**C**	**D**
B	*D*	*C*	*A*

D	**E**	**F**	**B**	**A**	**C**
A	*B*	*C*	*D*	*E*	*F*
A	**B**	**C**	**D**	**E**	**F**
E	*D*	*F*	*A*	*B*	*C*

Обратная перестановка — BDCA, EDFABC. В столбце с “C” будет на один символ меньше, т.к. этот столбец соответствует последнему символу ключа.

	E	**D**	**F**	**A**	**B**	**C**
B	I	A	C	O	O	V
D	V	E	R	Y	P	L
C	H	E	K	V	E	L
A	I	R		T	A	V

	A	**B**	**C**	**D**	**E**	**F**
B	O	O	V	A	I	C
D	Y	P	L	E	V	R
C	V	E	L	E	H	K
A	T	A	V	R	I	

Теперт пустое место переедет в столбец с “B”, т.к. это последний символ первой перестановки.

	B	**D**	**C**	**A**
A	O	Y	R	K
B	O	P	V	T
C	V	L	E	A
D	A	E	L	V
E	I	V	E	R
F	C		H	I

	A	**B**	**C**	**D**
A	K	O	R	Y
B	T	O	V	P
C	A	V	E	L
D	V	A	L	E
E	R	I	E	V
F	I	C	H	

Расшифрованный текст — KORYTOVPAVELVALERIEVICH — совпадает с исходным

3. Проведена проверка различных параметров утилиты. В целом в утилите для каждого шага настраиваются следующие параметры:
    - Перестановка. Длина перестановки определяет число строк/столбцов на данном шаге
    - Как читать — по строкам / по столбцам
    - Как переставлять — по строка / по столбцам
    - Как выводить

Вывод с первого трансформируется в строку и подставляется во второй. Как видно, утилита проводит не транпозицию матрицы, а чтение по столб-

цам и запись по строкам (или наоборот, или нет — в зависимости от настроек).

Подобная операция не идентична транспозиции, если в матрице есть пустые места (не пробелы).Этим обусловлены операции предыдущего пункта.

4. Зашифрован текст KORYTOVPAVELVALERIEVICH с ключом FCK. Проведена атака для выяснения ключа по исходному тексту. Результаты на рисунке 8

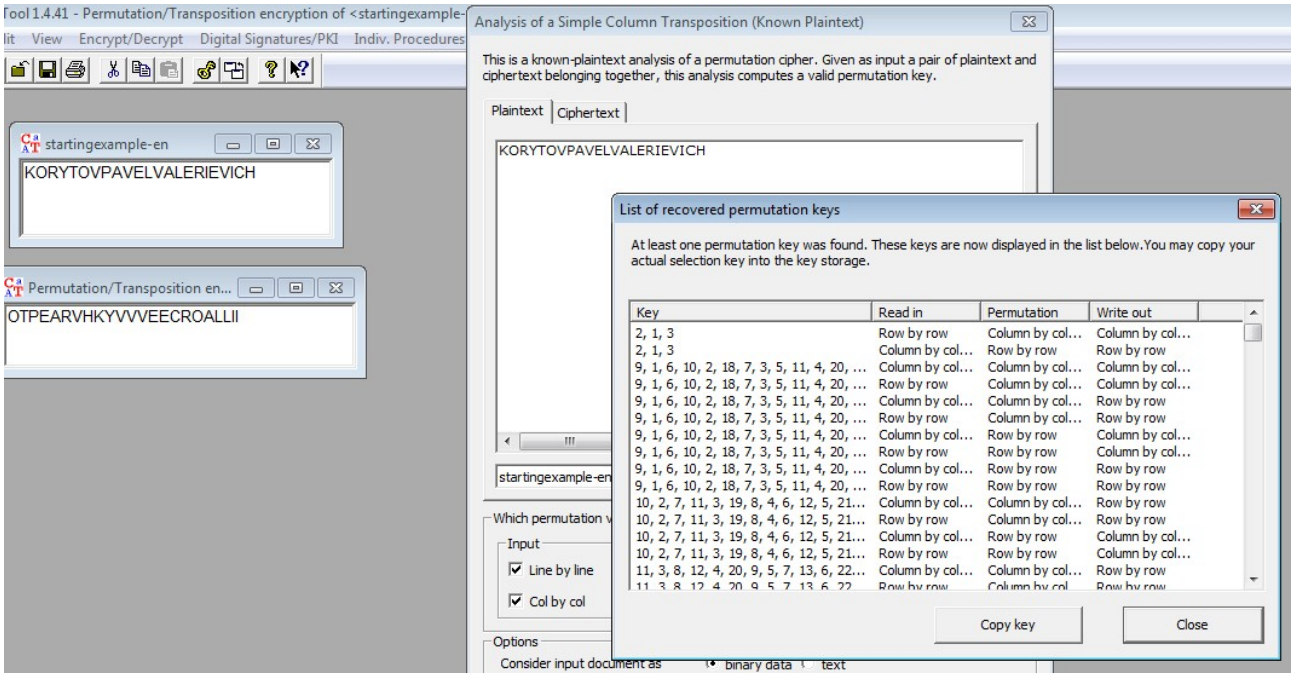


Рисунок 8. Результаты расшифровки ключа

5. Зашифровано сообщение: “DEAR GOD WAR IS HELL THANKS.” Шифротекст — “RDR LAAOASLHSEGWIETKD H N”

3. Шифр Виженера (Vigenere)

3.1. Описание шифра

- Заменим буквы алфавита числами соответствующими их порядковым номерам в алфавите $0, 1, \ldots, n-1$.
- Представим символы открытого текста P_i, ключа K_i и шифротекста C_i
- Сформируем *гамму* повторением ключа: $G = (K_1, \ldots, K_M) \ldots (K_1, \ldots, K_m)$
- Шифрование символа: $C_i = (P_i + G_i) \bmod n$
- Расшифровка символа: $P_i = (C_i - G_i) \bmod n$

3.2. Формулировка задания

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 с 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:
   - Определите размер ключа с помощью приложения Analysis-> Tools for Analysis-> Autocorrelation
   - Выполните перестановку текста с размером столбца равным размеру ключа приложением Permutation/Transposition
   - 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.

3.3. Ход работы

1. Найден шифр в CrypTool 1. Параметры шифра на рисунке 9.

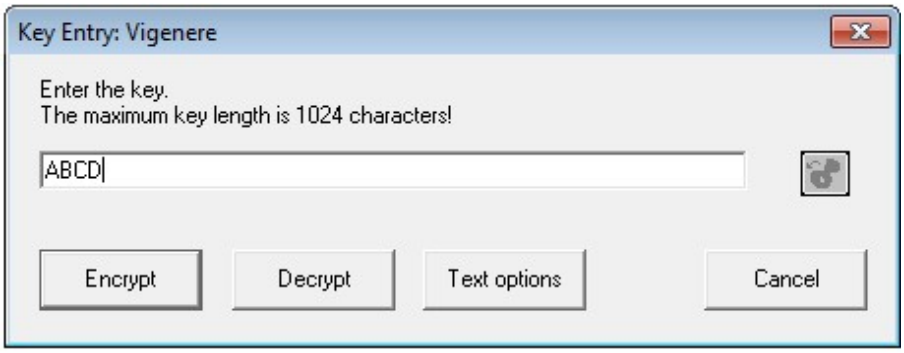


Рисунок 9. Параметры шифра Виженера

2. Текст — KORYTOV, ключ — PAVEL. Таблица соответствия букв и цифр для английского языка:

   Шифрование:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*

Текст	**K**	**O**	**R**	**Y**	**T**	**O**	**V**
Ключ	*P*	*A*	*V*	*E*	*L*	*P*	*A*
P_i	**10**	**14**	**17**	**24**	**19**	**14**	**21**
G_i	*15*	*0*	*21*	*4*	*11*	*15*	*0*
$C_i = (P_i + G_i) \bmod 26$	25	14	12	2	4	3	21
Шифротекст	Z	O	M	C	E	D	V

Расшифрование:

Шифротекст	Z	O	M	C	E	D	V
Ключ	*P*	*A*	*V*	*E*	*L*	*P*	*A*
C_i	25	14	12	2	4	3	21
G_i	*15*	*0*	*21*	*4*	*11*	*15*	*0*
$P_i = (C_i - G_i) \bmod 26$	**10**	**14**	**17**	**24**	**19**	**14**	**21**
Текст	**K**	**O**	**R**	**Y**	**T**	**O**	**V**

3. Для короткого шифротекста атака не выходит, т.к. мало данных для частотного анализа. Тем не менее, длина ключевого слова была установлена верно
4. Повторена атака для 1000 символов из English.txt. Атака выполнена успешно. Результаты на рисунке 10
5. Проведена атака на шифр.
    - Получена функция автокорелляции. Результат — на рисунке 11
      Как видно, функция больше в числах, кратных 5. Значит 5 — длина ключа
    - Выполнена Permutation / Transposition с ключом ABCDE. Таким образом, сгруппированы части текста, зашифрованные одной буквой. Результаты на рисунке 12

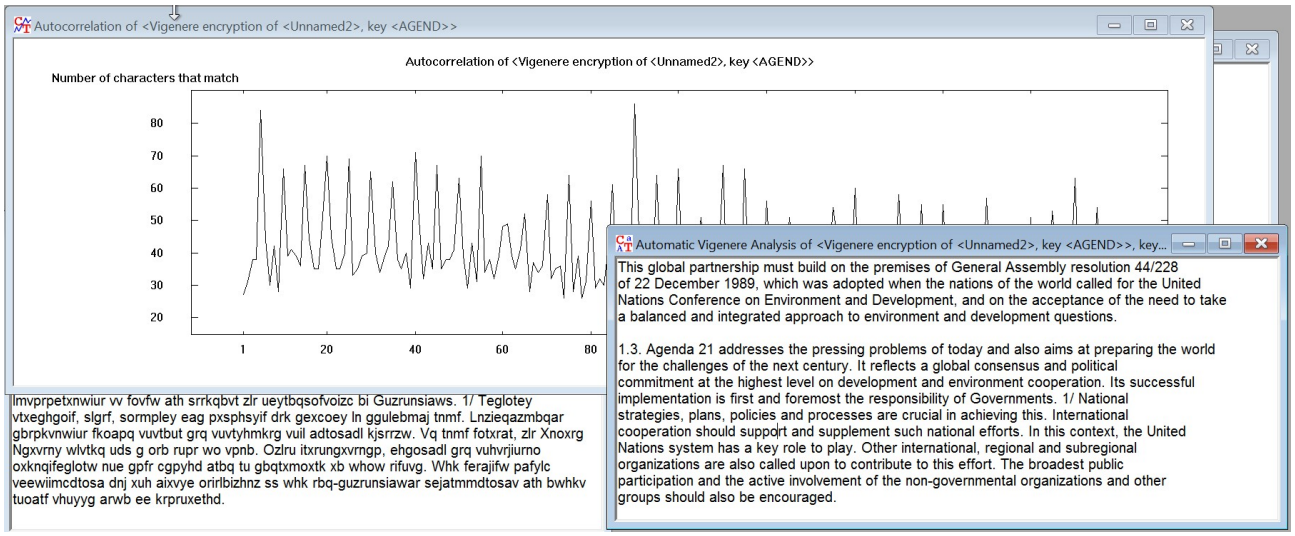


Рисунок 10. Атака на шифр Виженера

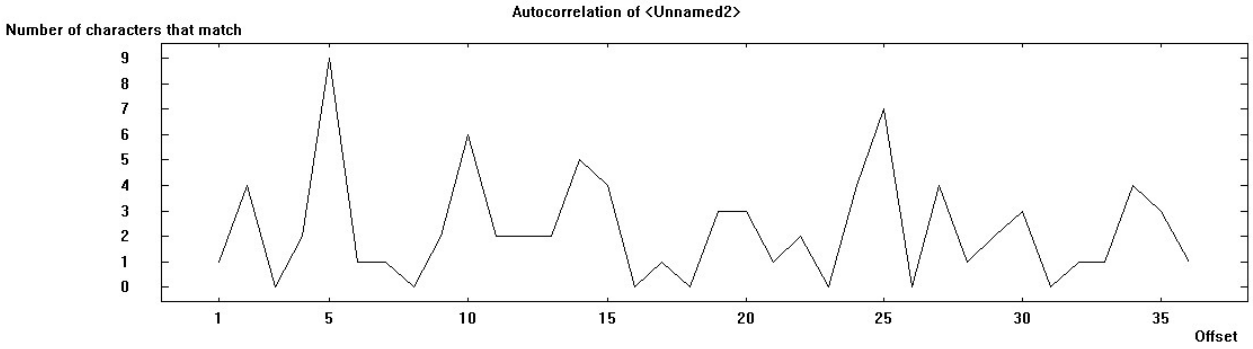


Рисунок 11. Функция автокорреляции

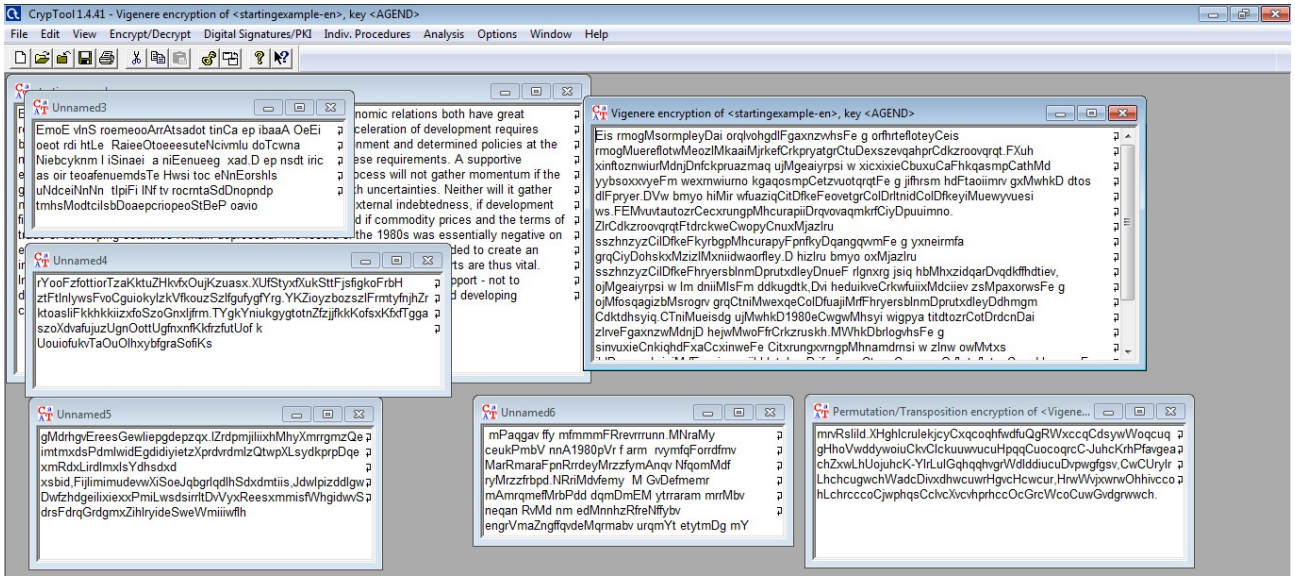
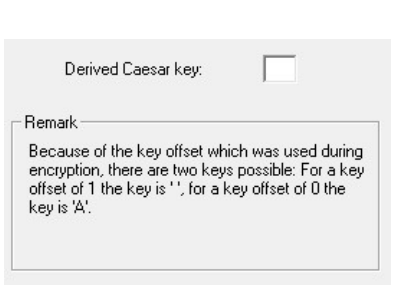
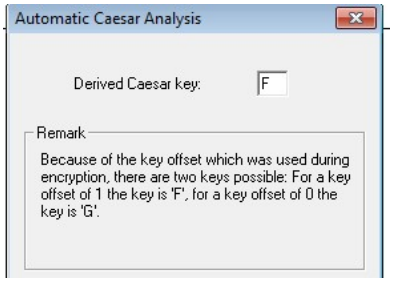


Рисунок 12. Разбиение шифротекста. Против часовой стрелки — фрагменты текста, зашифрованные одной частью ключа

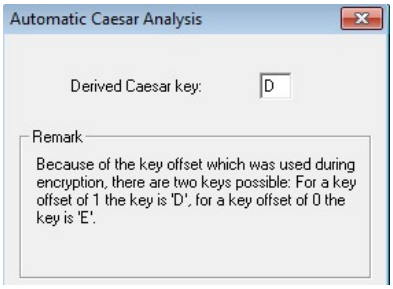
- На каждую часть шифротекста проведена атака, аналогичная атаке на шифр Цезаря. Результаты на рисунке 13



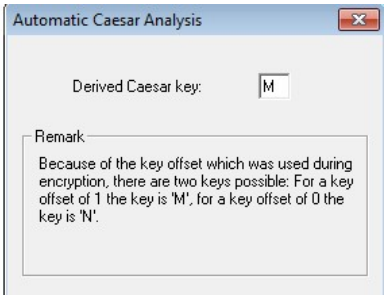
(a) Первый символ ключа



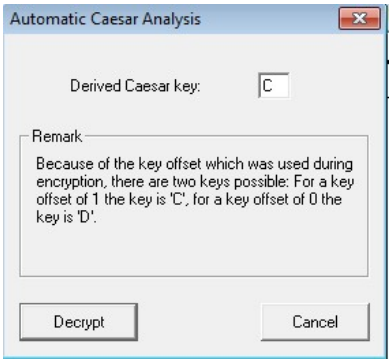
(b) Второй символ ключа



(c) Третий символ ключа



(d) Четвертый символ ключа



(e) Пятый символ ключа

Рисунок 13. Атака Цезарей

Полученный ключ — “ FDMC”. С поправкой на смещение в реализации шифра Цезаря, принятой в CrypTool, ключ — “AGEND”. Это совпадает с исходным ключом

Выводы

Название шифра	**Тип шифра**	**Ключ**
Substitution	Замена	Кодовое слово, смещение
Permutation / Transposition	Перестановка	Перестановки
Vigenere	Замена	Кодовое слово

Название шифра	**Сложность brute force**
Substitution	$o(n!)$, где n — мощность алфавита
Permutation / Transposition	$o(m! \times n!)$, где m, n — количество строк и столбцов матрицы
Vigenere	$o(n^m)$, где n — мощность алфавита, m — длина ключа. Если последняя неизвестна, то длина сообщения.

Изучены и проведены атаки на шифры Substitution, Permutation / Transposition и Vigenere.

Шифр Substitution — простой шифр на основе замены алфавита; взлом его с помощью частотного анализа не составляет труда.

Шифры Permutation / Transposition и Vigenere — более криптостойкие. Тем не менее, в современных условия их эффективный взлом возможен — с помощью поиска запретных биграмм и функции автокорреляции соответственно.

С развитием формальной криптографии изученные шифры потеряли эффективность; уже в ходе Гражданской Войны в США шифр Виженера регулярно расшифровывался, а Permutation / Transposition стал быстро взламываться в начале Первой Мировой.

Использованное ПО — CrypTool 1 / CrypTool 2 в VirtualBox, neovim и XeLaTeX для написания отчета.