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

ЛАБОРАТОРНАЯ РАБОТА №1

по дисциплине «Криптография и защита информации»

Тема: Изучение классических шифров средствами RailFence, Scytale, Caesar

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

Санкт-Петербург
2019

Цель работы

Исследовать шифры Rail Fence, Scytale, Caesar и получить практические навыки работы с ними, в том числе и в программном продукте Cryptool 1 и 2.

1. Шифр Rail Fence

1.1. Описание шифра

Тип шифра — перестановка.

В шифре Изгороди открытый текст разбивается на определенное количество строк. В каждой строке поочередно записывается одна буква подобно изгороди, зашифрованный текст составляется при чтении строки за строкой. Например, при разбиении открытого текста “0123456789” на 3 строки шифрование выглядит следующим образом:

Разбиение на строки						Шифротекст
0		4		8		
	1	3	5	7	9	=> 0481357926
		2		6		

Для увеличения криптостойкости используют смещение. Пример для смещения 2:

Разбиение на строки						Шифротекст
—		3		7		
	—	2	4	6	8	=> 2613579048
		1	5		9	

Таким образом, ключ шифра — число строк (N_r) и смещение (O). Так как $O \leq N_r < l$, где l — длина сообщения, сложность атаки грубой силы:

$$N_{bf} < l^2 \tag{1.1}$$

1.2. 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 (транс-

литерация латиницей) вручную и с помощью шифра при Number of Rows>2, Offset≥2. Убедиться в совпадении результатов.

6. Создайте шифровку для варианта Offset=0 и Number of Rows≤ и передайте коллеге слева для расшифровки.
7. Определите ключ методом “грубой сил” и расшифруйте полученный от коллеги шифротекст.

1.3. Выполнение задания

1. В CrypTool найден шифр Rail Fence.

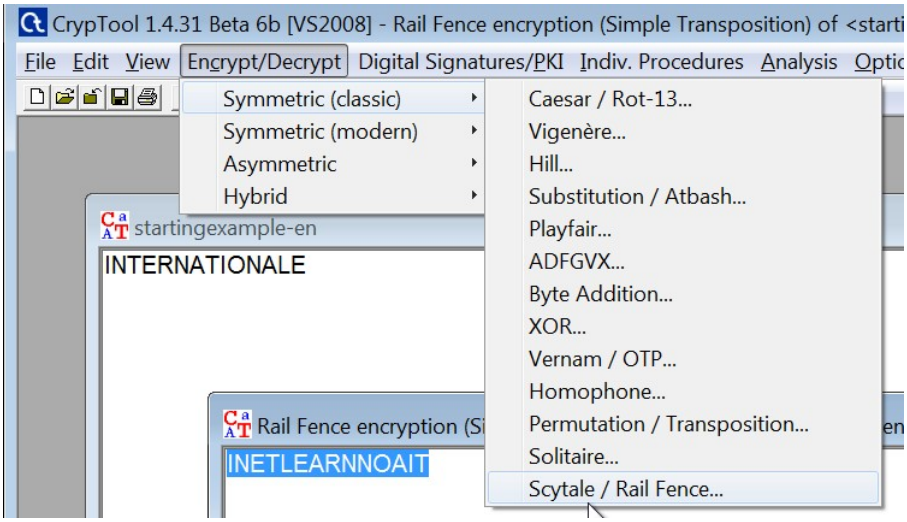

Рисунок 1. Шифр Rail Fence в CrypTool

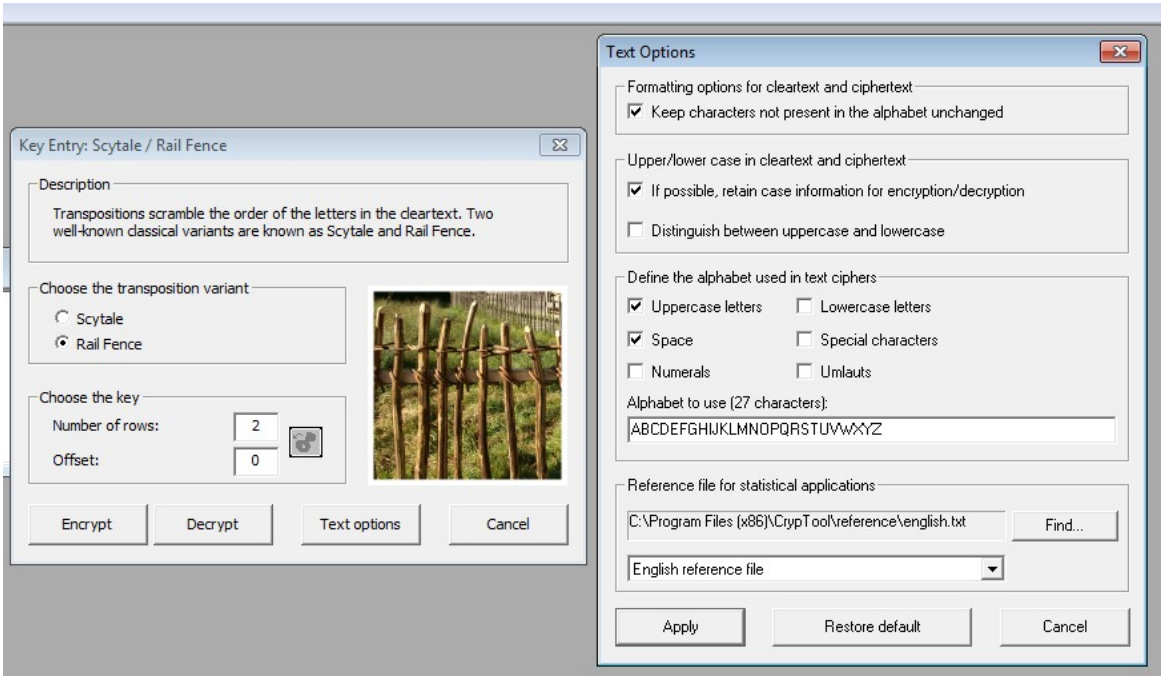

Рисунок 2. Опции шифровния в CrypTool 1

2. Создан файл с открытым текстом, содержащим последовательность цифр 12345678900987654321
3. Произведена зашифровка и расшифровка созданного текста. Результаты на рисунке 4

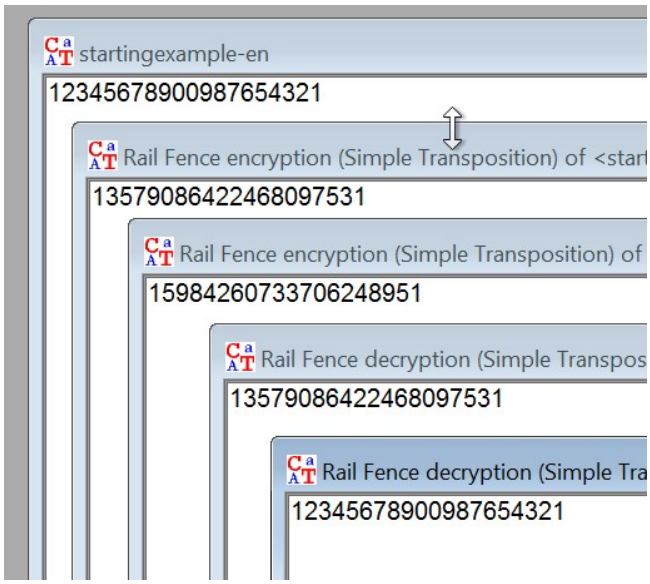

Рисунок 3. Зашифровка и расшифровка

4. Number of rows в шифре — число строк, Offset — смещение. Так, зашифровка 123456 с параметрами $(2, 0)$ превращает его в 135246 — сначала записываются четные цифры, затем — нечетные. Если поставить $(2, 1)$, то результат — 246135, т.к. в таком случае первая цифра — нечетная.
5. Зашифрована и расшифрована вручную фамилия автора — `KORYTOV` — с параметрами $(3, 2)$

— R V
— O Y O => RVOYOKT
K T

Смещение — 2, длина текста — 7 $\Rightarrow$ длина таблицы — 9:

— X X
— X X X
X X

Подстановка шифротекста в вышеуказанную таблицу дает ответ:

— R V
— O Y O
K T

$\Downarrow$

K O R Y T O V

Как видно на рисунке 4, Зашифровка в CrypTool с такими же параметрами дает такие же результаты.

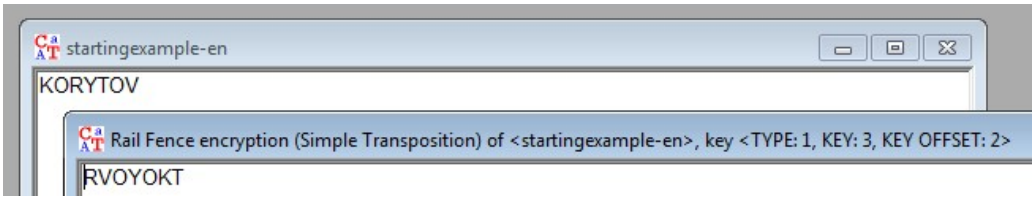

Рисунок 4. Проверка зашифровки

6. Коллеге слева сгенерирована последовательность INTERNATIONALE и зашифрована с числом строк 8: INETLEARNNOAIT.
   Коллега расшифровывала последовательность меньше нескольких минут путём перебора числа строк.
7. Полученная от коллеги слева последовательность: BKLIOINVNA. Ход расшифровки представлен на рис. 5 С 4-й попытки выяснено, что после-

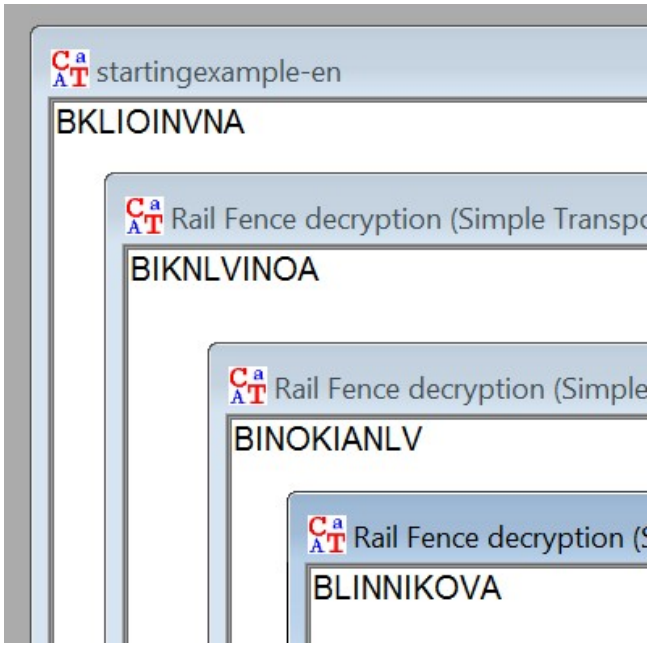

Рисунок 5. Ход расшифровки последовательности

довательность зашифрована с числом строк 4. Соответственно, это ключ.

2. Шифр “Сцитала” (Scytale)

2.1. Описание шифра

Тип шифра — перестановка.

В криптографии сцитала, известный также как шифр Древней Спарты, представляет собой прибор, используемый для осуществления перестановочного шифрования. Прибор состоит из цилиндра и узкой полоски пергамента,

обматывавшейся вокруг него по спирали, на которой писалось сообщение. Иллюстрация, демонстрирующая работу данного шифра представлена на рисунке 6.

Рисунок 6. Иллюстрация шифра Сцитала

Для расшифровки использовался цилиндр такого же диаметра, на который наматывался пергамент, чтобы прочитать сообщение.

Сложность атаки грубой силы в таком случае такая же, как и у шифра Rail Fence. Если убрать смещение (вряд ли оно применялось в Древней Греции) и учесть физические ограничения, число перебираемых вариантов едва ли превосходит несколько десятков.

2.2. Задание

1. Найти шифр в CrypTool 1: Encrypt/Decrypt-> Symmetric (Classic).
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 Edges и Offset.
5. Зашифровать и расшифровать текст содержащий только фамилию (транслитерация латиницей) вручную и с помощью шифра при Number of Edges > 2, Offset ≥ 2. Убедиться в совпадении результатов.
6. Взять в CrypTool 2 шаблон атаки на шифр методом “грубой силы” и модифицировать этот шаблон, заменив блок с шифротекстом на блок ввода открытого текста и блок зашифрования. Изучить принципы этой автоматической атаки.

2.3. Выполнение задания

1. В CrypTool 1 найден исследуемый шифр. Он находится в том же пункте, какой выбран на рисунке 1. Спецификация параметров такая же, как и на рисунке 2.
2. Создан файл с открытым текстом: 0987654321123456789

3. Произведена его зашифровка и расшифровка несколько раз. Результаты на рис. 7

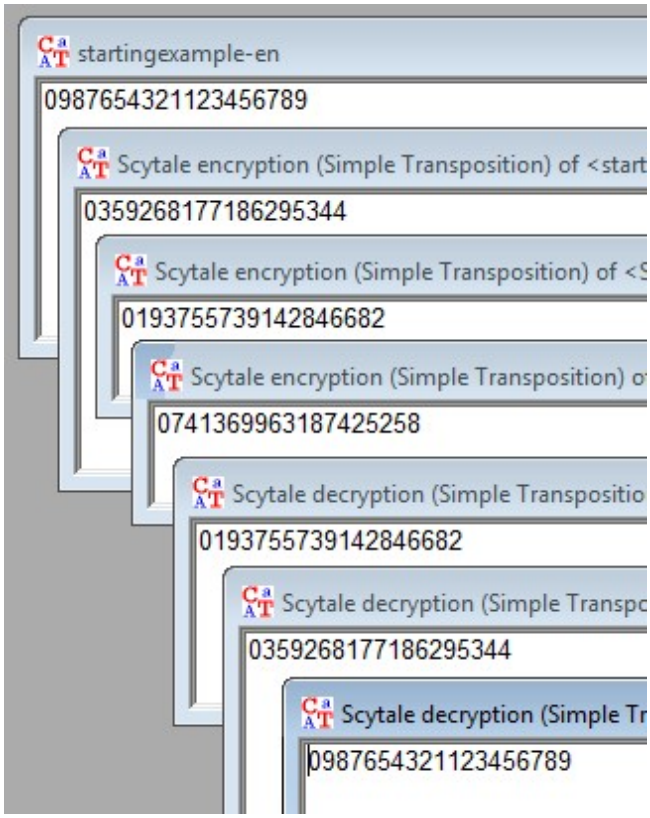

Рисунок 7. Зашифровка и расшифровка шифром Сцитала

4. Number of Rows в CrypTool — количество граней цилиндра, Offset — смещение от начальной грани.
5. Фамилия автора — KORYTOV — зашифрована с параметрами $(3, 2)$.

   — — K
   O R Y
   T O V
   ⇓
   OTROKYV

   Расшифровка не составляет труда:

   — — K
   O R Y => KORYTOV
   T O V

   CrypTool дает те же результаты.
6. Проведена указанная модификация шаблона в CrypTool 2. В качестве текста взят первый куплет “Интернационала” в адаптации Билли Брэгга. Принцип работы автоматической атаки заключается в переборе количества строк в указанном диапазоне (смещение не поддерживается) и в по-

иске известных слов в расшифровке.

Скриншот workspace CrypTool 2 в приложении А.

3. Шифр Цезаря (Caesar)

3.1. Описание шифра

Шифр Цезаря — один из древнейших шифров. Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки.

Тип шифра — замена.

- Заменим буквы алфавита числами соответствующими их порядковым номерам в алфавите $0, 1, \ldots, n-1$.
- Представим символы открытого текста P_i и шифротекста C_i
- Выбираем в качестве ключа числа k
- Шифрование: $C_i = (P_i + k) \bmod n$
- Расшифровка: $P_i = (C_i - k) \bmod n$

Сложность атаки грубой силы — $N_{bf} < n$

3.2. 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 с ключом, отличным от 0. Убедиться в совпадении результатов.
3. Построить гистограмму частот букв английского языка по эталонному файлу English.txt (папка CrypTool/reference), используя утилиту из Analysis -> Tools for Analysis.
4. Зашифровать ключом отличным от 0 файл CrypTool-en.txt (папка CrypTool / Examples).
5. Построить гистограмму частот букв в зашифрованном тексте, сравнить визуально гистограммы и подтвердить ключ зашифрования.
6. Проверить гипотезу о значении ключа утилитой Analysis -> Symmetric Encryption (Classic)->Cipher Text Only->Caesar.
7. Передать шифровку соседу слева для проведения подобной атаки.

3.3. Выполнение задания

1. Шифр найден в CrypTool 1. Параметры шифра указаны на рисунке 8

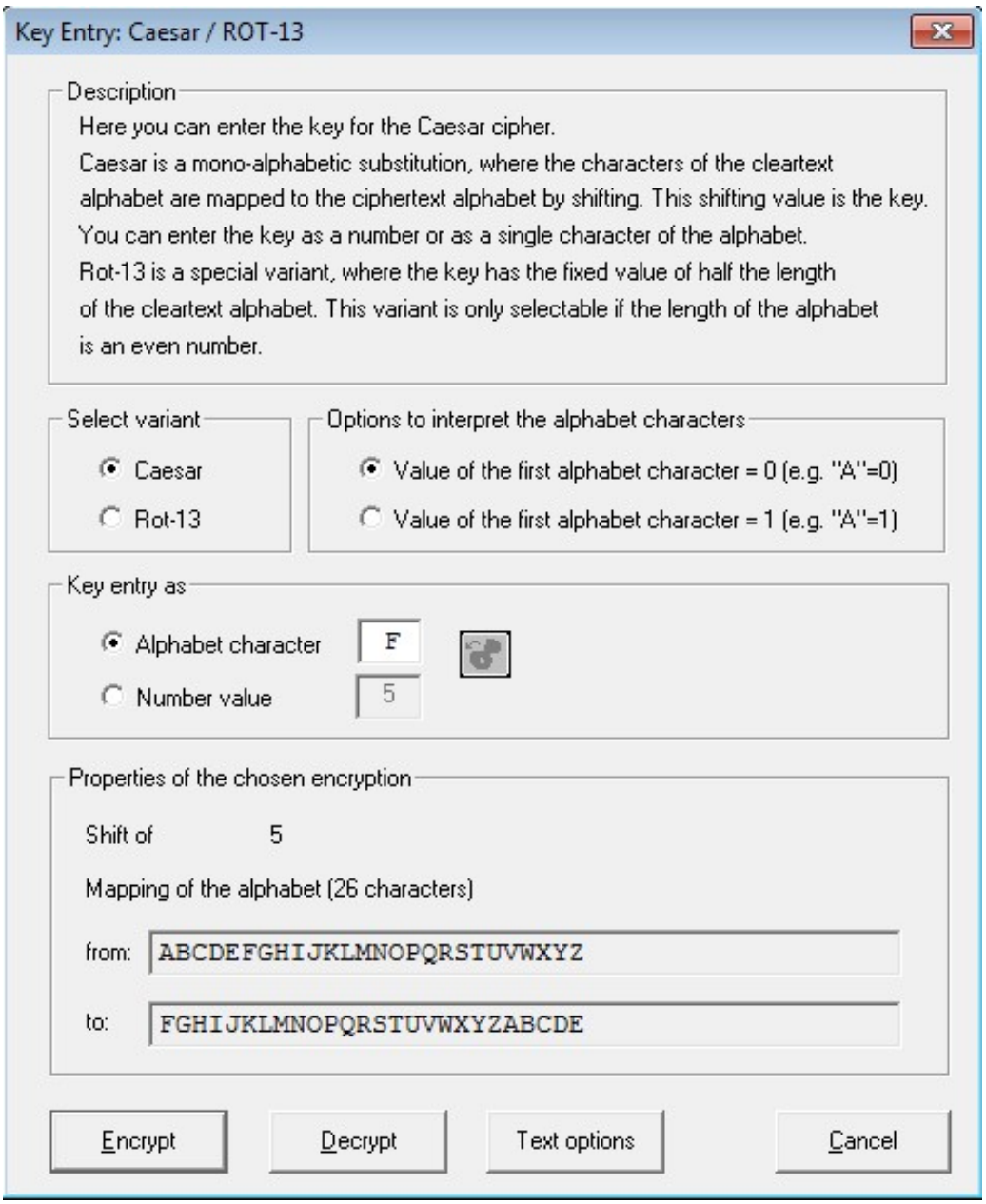

Рисунок 8. Спецификация параметров для шифра Цезаря

2. Фамилия автора “KORYTOV” зашифрована вручную с ключом 5:

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

Результат шифрования: “FJMTOJQ”. Расшифровка дает исходный результат

3. Построена гистограмма для указанного файла — “Повестки дня на XXI век”, “Agenda 21”. Результат на рисунке 9
4. Предлагаемый файл зашифрован шифром Цезаря с ключом F.

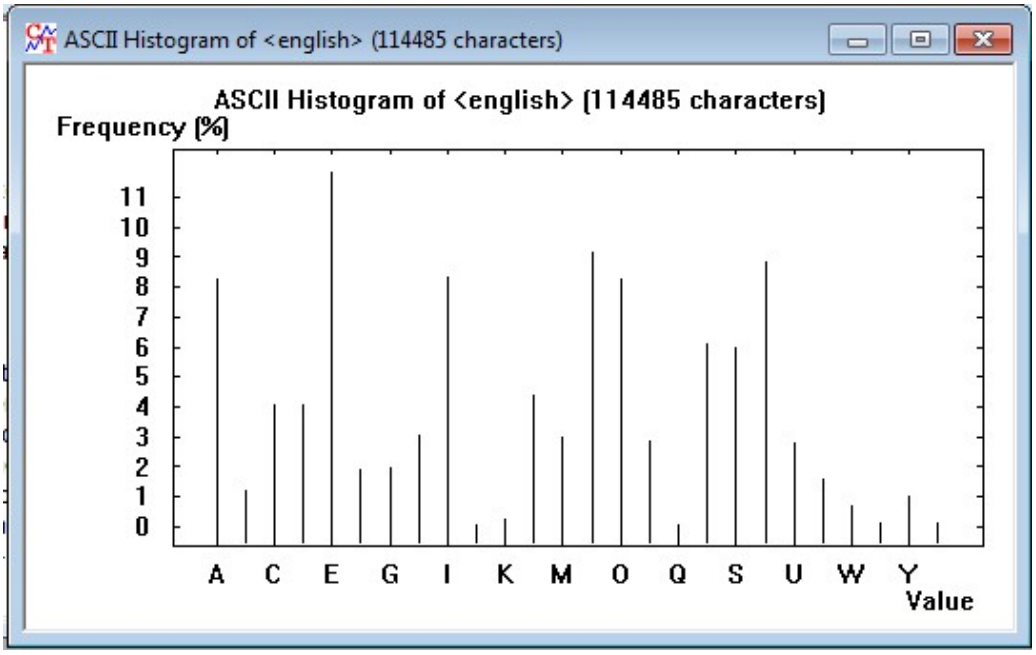

Рисунок 9. Распределение символов для Agenda 21

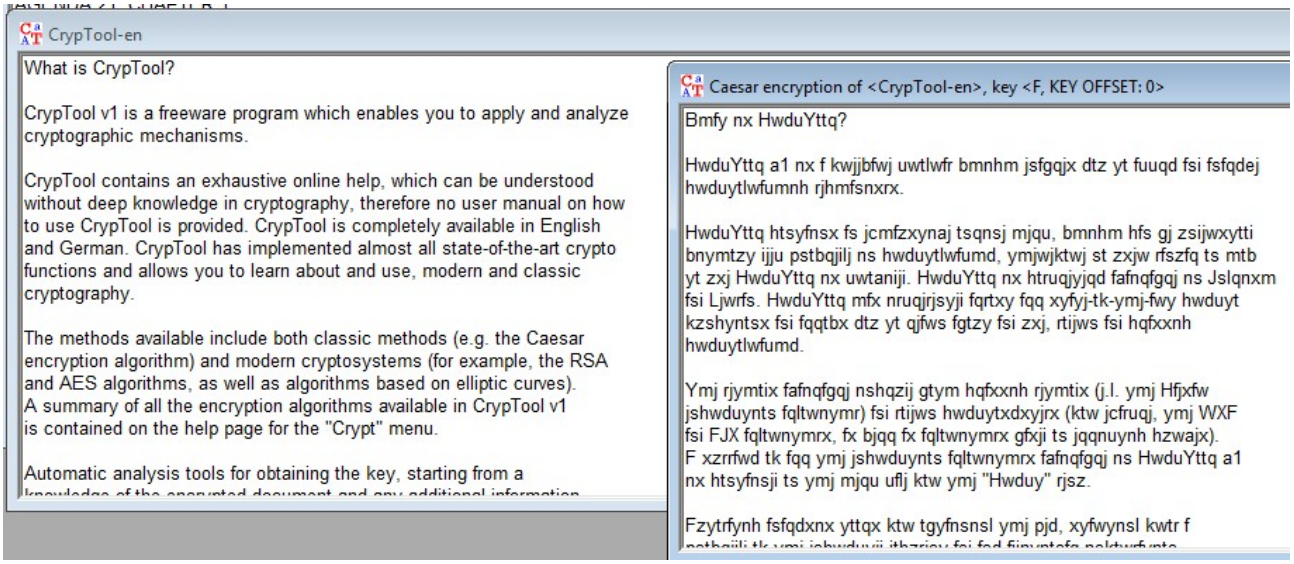

Рисунок 10. Шифр Цезаря

5. Проверено визуальное совпадение диаграмм. Диаграммы на рисунках 9 и 11 действительно похожи, однако из-за меньшего размера второго файла имеются расхождения.
6. CrypTool 1, как и ожидалось, успешно подобрал ключ — F.

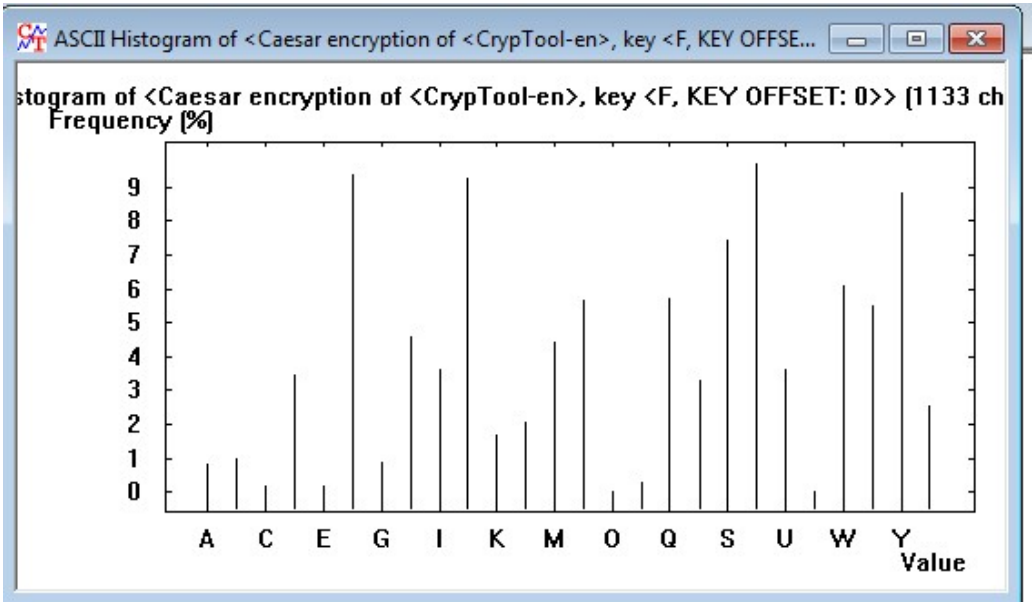

Рисунок 11. Диаграмма для зашифрованного текста

Выводы

- Рассмотренные шифры — симметричные, т.е. для шифрования и расшифрования используется один и тот же ключ
- Шифры Rail Fence и Scytale — шифры перестановки, шифр Цезаря — шифр замены
- Преимущество этих шифров — возможность легкого использования без какого-либо вычислительного оборудования. Это сделало возможным их применение в Древнем Мире.
- Атака “грубой силы” на рассмотренные шифры не составляет труда и не намного сложнее, чем зашифровка сообщения.
- Наличие вычислительного оборудования делает взлом рассмотренных шифров тривиальной задачей.
- Частотный анализ позволяет провести эффективную атаку на шифр Цезаря; для Rail Fence и Scytale этот метод неприменим

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

ПРИЛОЖЕНИЕ А
Среда CrypTool 2