

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

ОТЧЕТ
по лабораторной работе №1-2-3
по дисциплине «Криптография и защита информации»
Тема: Изучение классических шифров

Студент гр.8382

Нечепуренко Н.А.

Преподаватель

Племянников А.К.

Санкт-Петербург

2021

Цели работы.

Исследовать шифры Scytale, Substitution, Hill и получить практические навыки работы с ними, в том числе с использованием приложений Cryptool 1 и 2.

Шифр «Сцитала» (Scytale).

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 \geq 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.

Описание шифра.

В криптографии шифр «Сцитала», известный также, как шифр Древней Спарты, представляет собой прибор, используемый для осуществления перестановочного шифрования. Прибор состоит из гранёного цилиндра (жезла) и узкой полоски пергамента, которая обматывается вокруг цилиндра по спира-

ли. На гранях цилиндра записывалось сообщение. Иллюстрация, демонстрирующая работу данного шифра представлена на рисунке 1. Для расшифровки использовался гранёный цилиндр такого же диаметра, на который наматывался пергамент, чтобы прочесть сообщение.

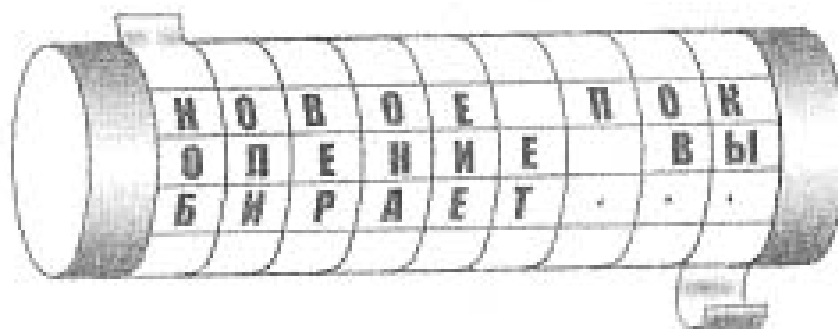


Рисунок 1 – Иллюстрация принципа работы шифра Сцитала

Тип шифра – перестановочный.

Введем обозначения: k – длина сообщения, m – «ключ», количество строк матрицы Сцитала (количество граней цилиндра), n – количество столбцов.

$$n = \left\lfloor \frac{k-1}{m} \right\rfloor + 1$$

Тогда положение буквы сообщения с индексом j в шифротексте будет

$$j = m \cdot (i \bmod n) + \frac{i}{n}$$

Реализация в Cryptool.

В инструменте Cryptool 1 имеется встроенная реализация алгоритма шифрования и дешифрования Сцитала (см. рис.2).

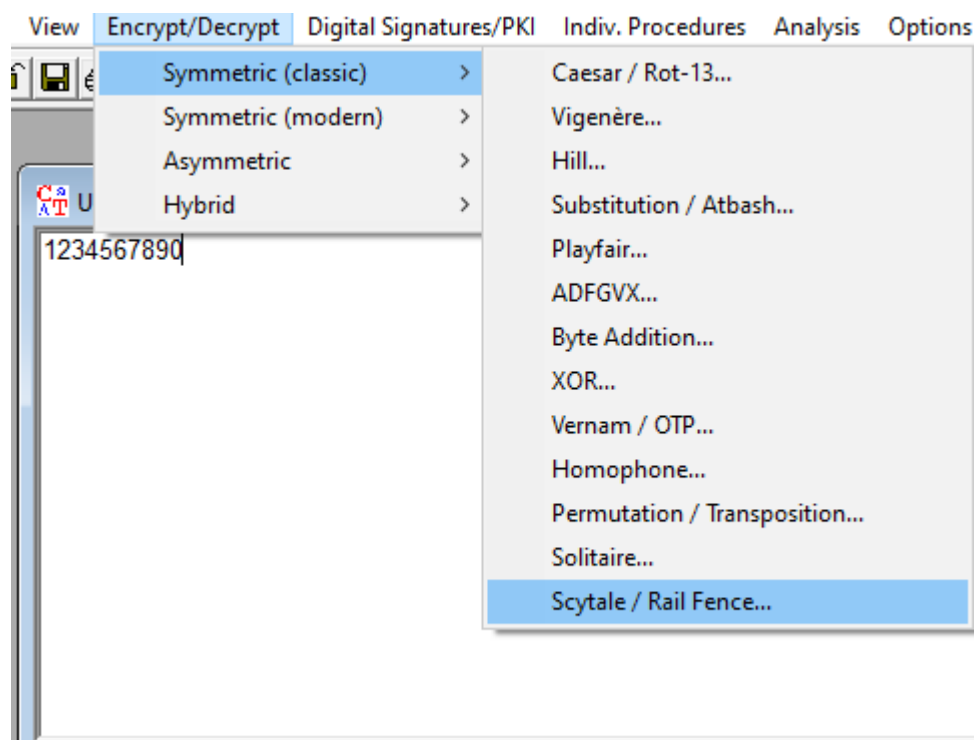


Рисунок 2 – Шифр Сцитала в Cryptool 1

Существует возможность изменить количество граней с помощью параметра Number of edges, а также задать смещение первого символа с помощью параметра Offset.

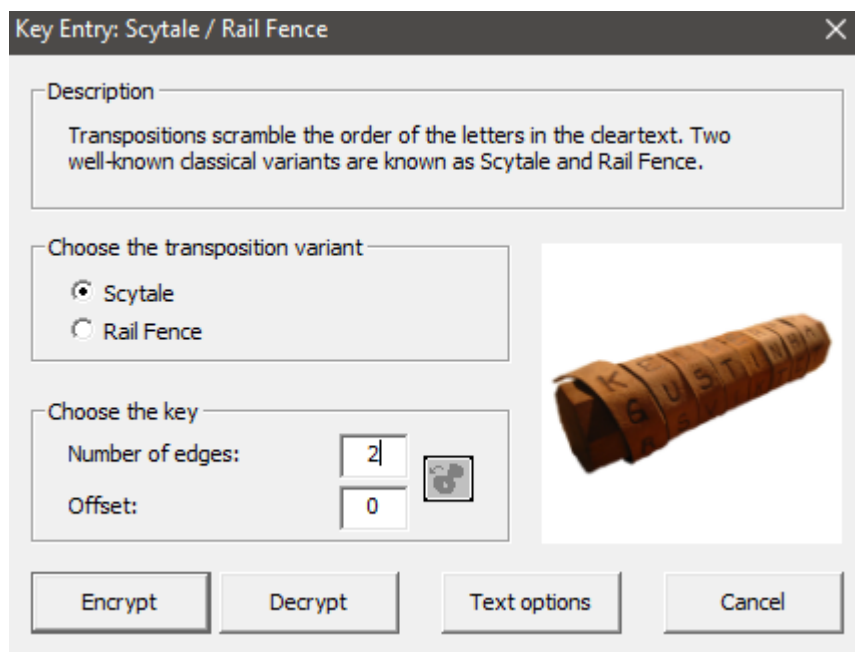


Рисунок 3 – Пользовательские параметры шифра Сцитала

Рассмотрим последовательность 1234567890, применим к ней шифр Сцитала с параметрами Number of edges равным 4 и параметром Offset равным 0. Результат представлен на рисунке 4.

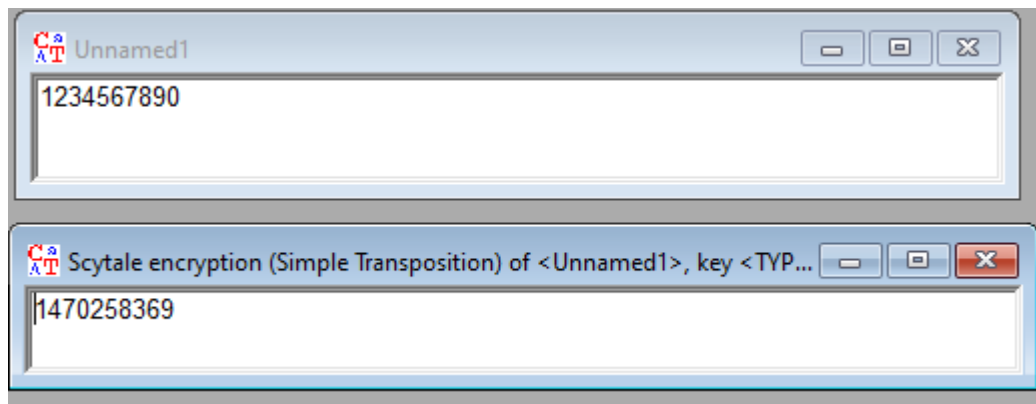


Рисунок 4 – Шифр Сцитала, 4 грани, смещение 0

Получаем последовательность 1470258369. Схематически сообщение было представлено в следующем виде:

1 2 3

4 5 6

7 8 9

0 * *

Зашифрованная последовательность была получена чтением сообщения по столбцам.

Зашифруем полученную последовательность с помощью Cryptool, положив параметры Number of edges и Offset равными 3 и 2. Затем расшифруем сообщение в обратном порядке и убедимся в корректности данных.

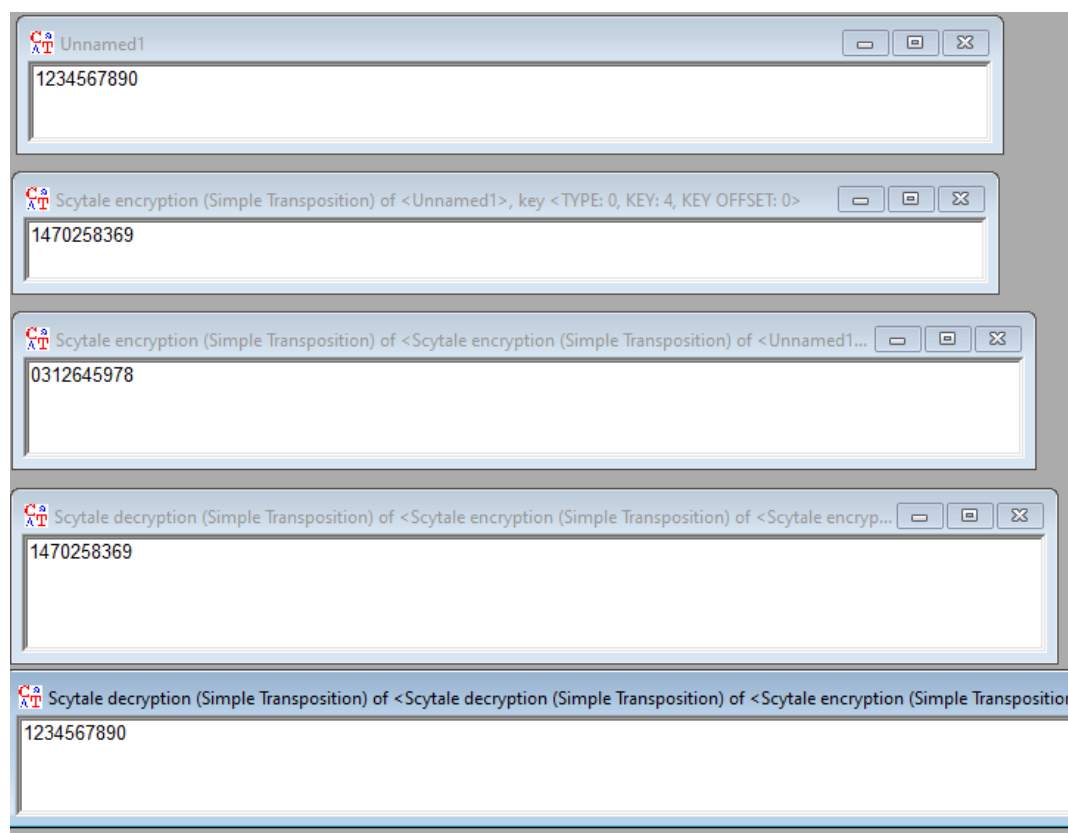


Рисунок 5 – Шифрование шифротекста с параметрами 3 и 1. Затем получение исходного сообщения

Так как шифр перестановочный, поэтому выполнив расшифровку в обратном порядке получаем исходный текст 1234567890.

Зашифруем и расшифруем фамилию NECHEPURENKO с помощью шифра Сцигала с параметром 4. Таблица будет иметь следующий вид:

N E C

H E P

U R E

N K O

Читая по столбцам, получаем шифротекст NHUNEERKCPEO.

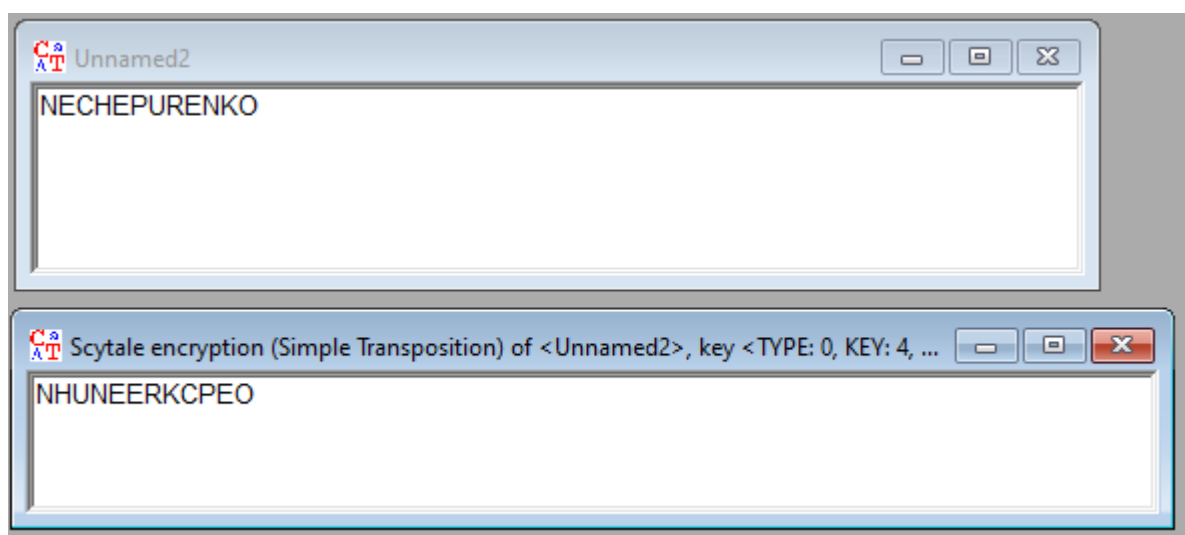


Рисунок 6 – Шифрование фамилии NECHEPURENKO в Cryptool

Шифротексты совпали. Расшифруем сообщение, заполним таблицу по рядам и прочитаем по строкам:

N E C

H E P

U R E

N K O

получаем NECHEPURENKO. Дешифруем сообщение с помощью Cryptool. Результат приведен на рисунке 7.

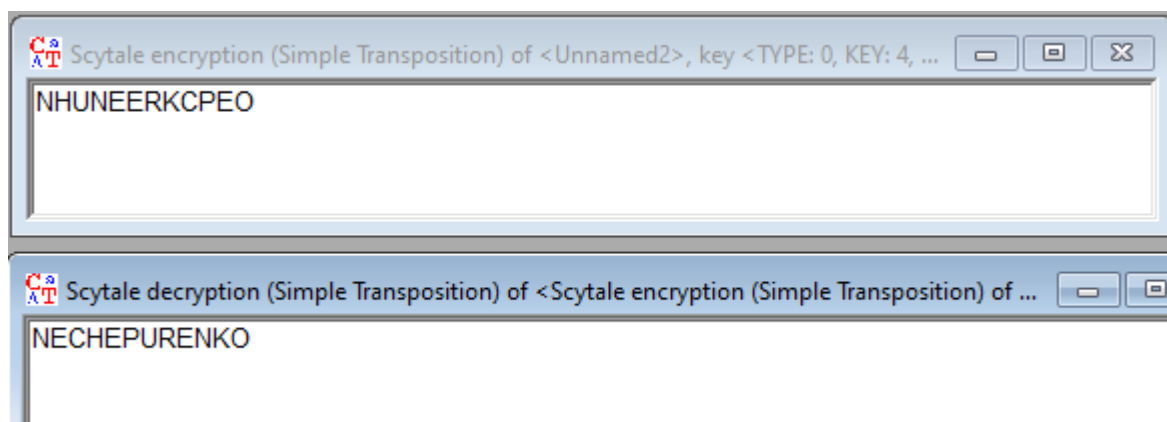


Рисунок 7 – Дешифрование фамилии NECHEPURENKO в Cryptool

Проведем атаку на шифр Сцитала методом грубой силы в Cryptool 2. Зашифруем открытый текст с параметром 5 (см. рис. 8).

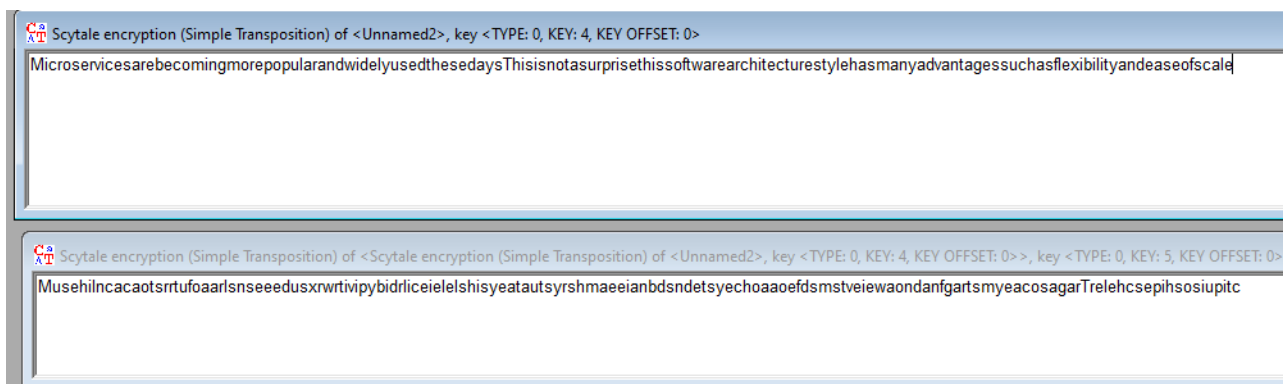


Рисунок 8 – Шифрование открытого текста шифром Сцитала с параметром 5

Проведем атаку методом грубой силы на этот текст (см. рис. 9).

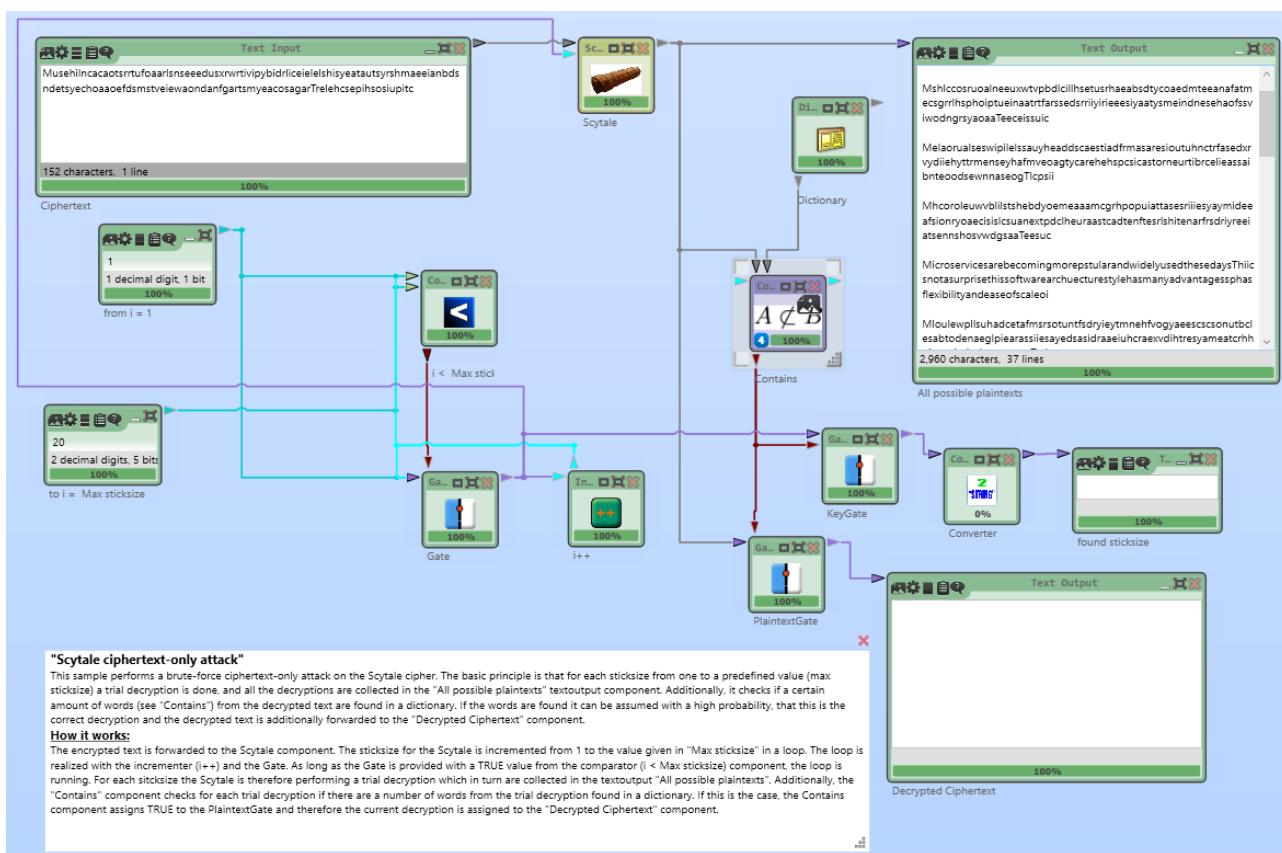


Рисунок 9 – Атака грубой силы на шифр Сцитала

Среди всех возможных текстов можно найти изначально зашифрованное сообщение. Анализатор не нашел окончательный ответ из-за отсутствия разбиения на слова. Если провестки атаку на зашифрованный с тем же параметром разбитый на слова текст, то атака сможет найти изначально сообщение (см. рис. 10).

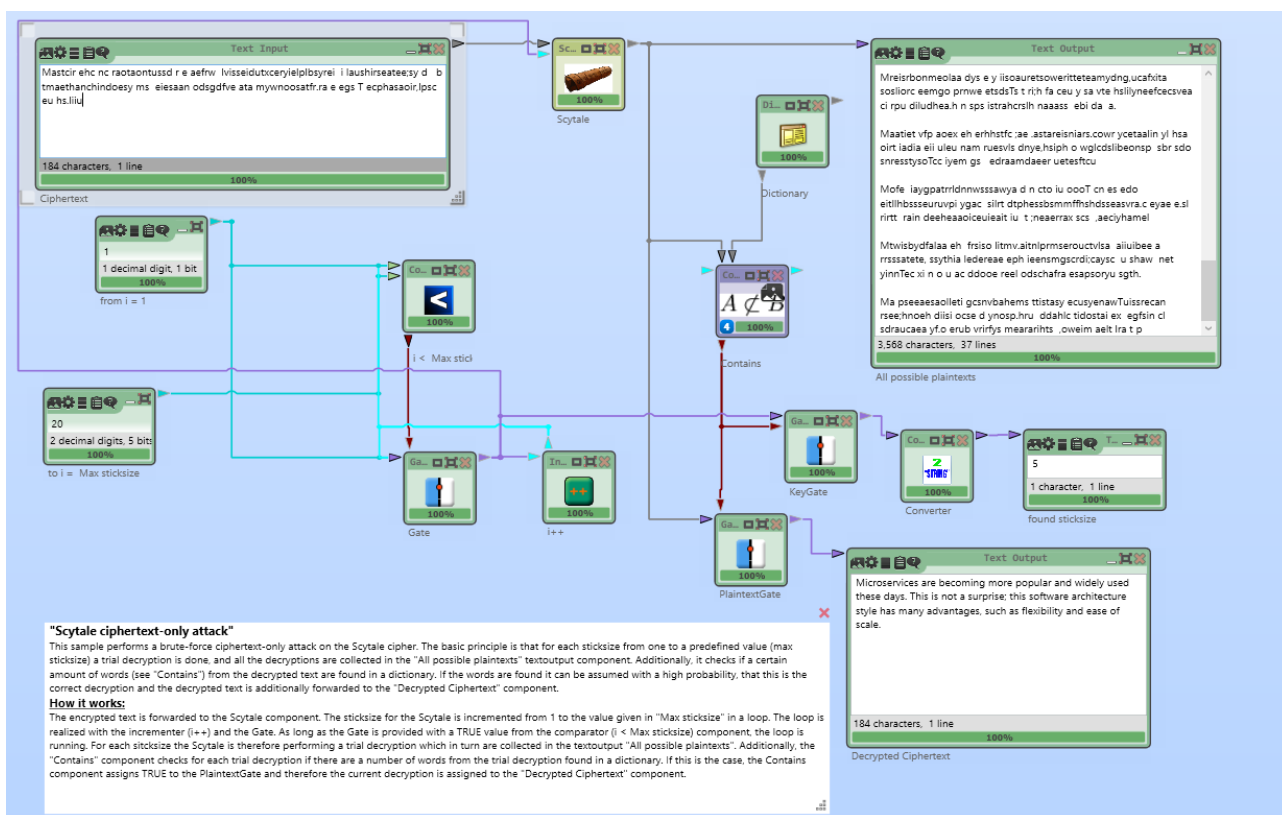


Рисунок 10 – Успешный результат атаки

Заменим блок с шифротекстом на блок с открытым текстом и блок с шифром. Получаем аналогичный и вполне ожидаемый результат (см. рис. 11).

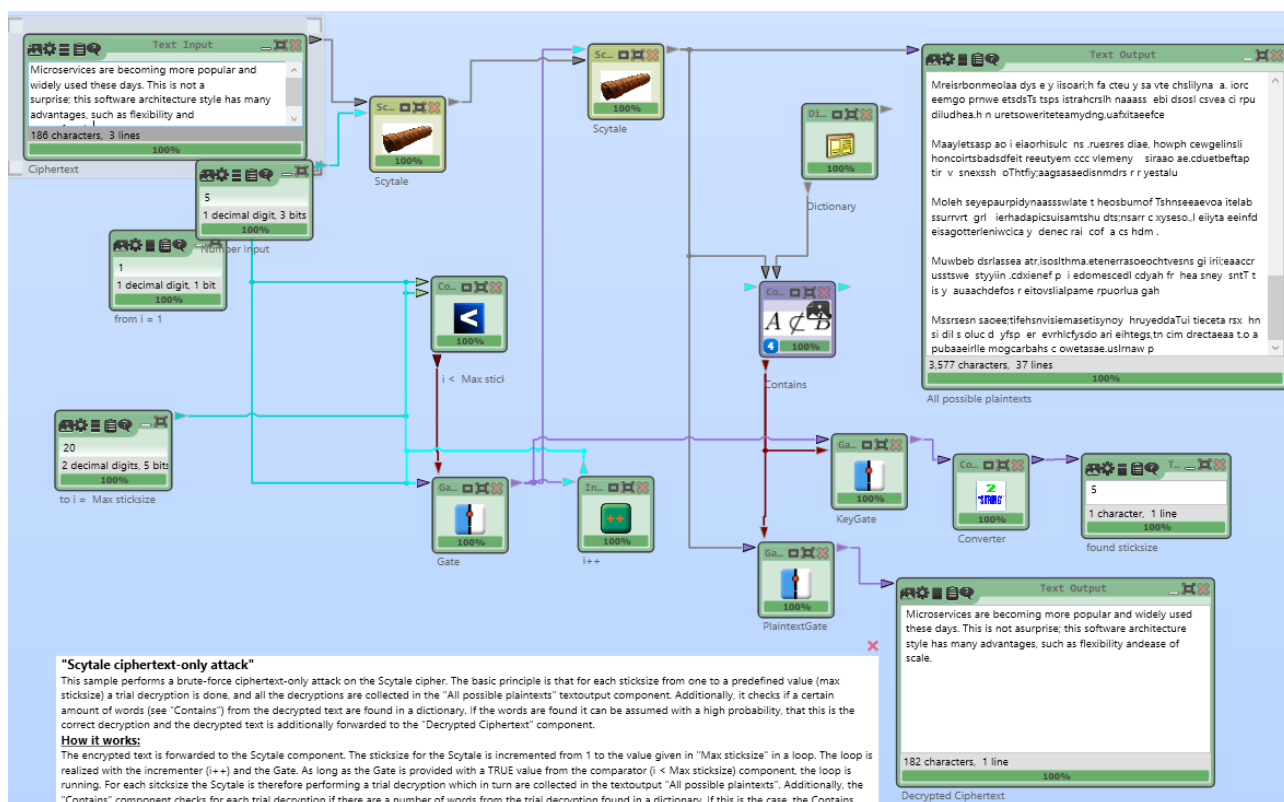


Рисунок 11 – Успешный результат атаки на зашифрованный текст

В схеме содержится словарь английских слов, а также элемент, который отвечает за подсчет слов. Схема перебирает все возможные варианты количества граней цилиндра, по-умолчанию максимальное значение параметра равно 20.

Сложность алгоритма $O(\text{maxsticksized})$.

Вывод.

Был изучен принцип работы шифра Сцигала. С помощью программы Cryptool 1 некоторый исходный текст был зашифрован и расшифрован несколько раз. С помощью программы Cryptool 2 была проведена атака методом грубой силы на полученный данным алгоритмом шифрования шифротекст.

Шифр моноалфавитной подстановки(Substitution).

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 выбранным ключом и смещением Offset \neq 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. Изучить, как в CrypTool 1 позволяет выполнить ручное дешифрование 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. Зашифровать текст из 200 символов, сохранить ключ, и передать коллеге по учебной группе для расшифровки.
11. Самостоятельно изучите одну атаку, реализованную в CrypTool 2, опираясь на Help и ссылки на статьи.

Описание шифра.

В шифре моноалфавитной подстановки для задания ключа используются два параметра Key и Offset. Key – это кодовое слово, на основе которого формируется алфавит шифрограммы. Первым шагом создания нового алфавита служит удаление всех повторяющихся букв, которые присутствуют в кодовом слове. Затем из алфавита удаляются все буквы кодового слова. На заключительном шаге кодовое слово внедряется в алфавит со смещением первого элемента кодового слова на величину параметра Offset. Тип шифра – шифр замены.

Реализация в Cryptool.


Шифр моноалфавитной подстановки представлен в Cryptool 1 (см. рис. 12).

Key Entry: Monoalphabetic Substitution / Atbash

Choose variant of the monoalphabetic substitution

- ☒ Key entry: Remaining characters are filled in ascending order
- ☐ Key entry: Remaining characters are filled in descending order
- ☐ Atbash (the encryption is using a fixed key)

Key Input

Key: 

Offset:

Information on the substitution encryption

The alphabet (26 characters) will be mapped

from:

to:

Encrypt Decrypt Text options Cancel

Рисунок 12 – Параметры шифра моноалфавитной подстановки

Можно выбрать ключ, сдвиг и порядок, в котором невычеркнутые буквы исходного алфавита будут в новом алфавите. В том же окне можно увидеть полученный по данным параметрам алфавит.

Зашифруем фамилию NECHEPURENKO с ключом KEY и сдвигом 2 (см. рис. 13).

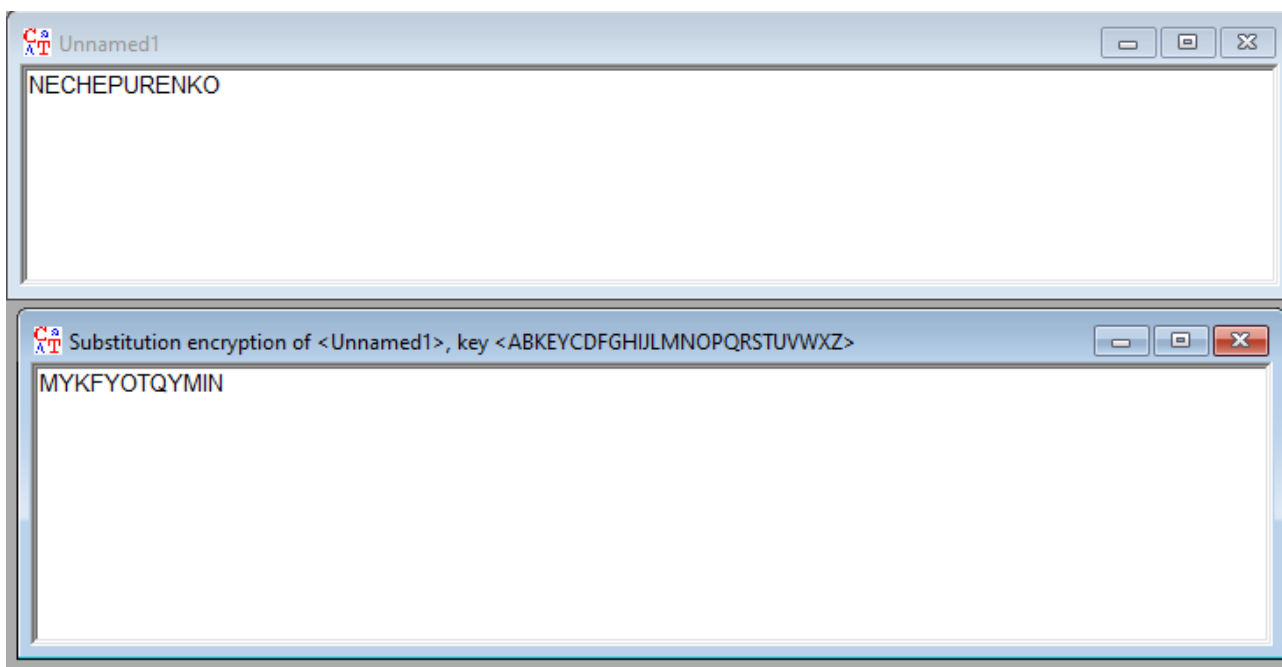


Рисунок 13 – Шифрование фамилии NECHEPURENKO шифром моноалфавитной подстановки в Cryptool

Вручную это выглядит следующим образом (см. рис. 14):

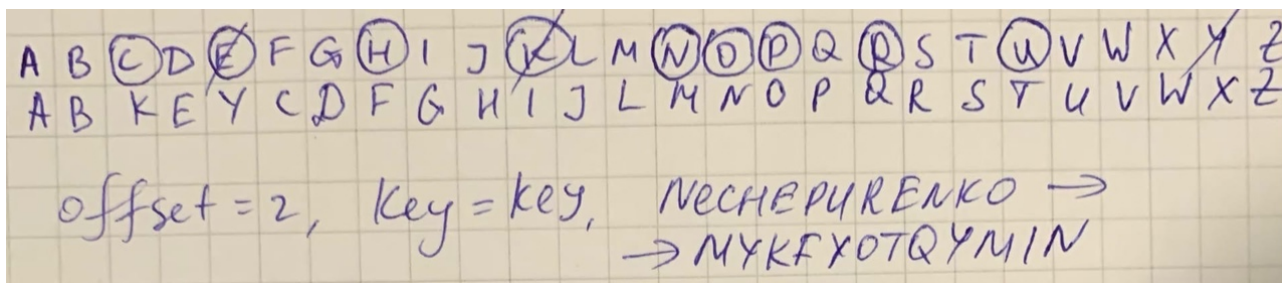


Рисунок 14 – Шифрование фамилии NECHEPURENKO шифром моноалфавитной подстановки вручную

Зашифруем текст из файла english.txt ~600 символов с ключом FORMIDABLE и сдвигом 13. Результат приведен на рисунке 15.

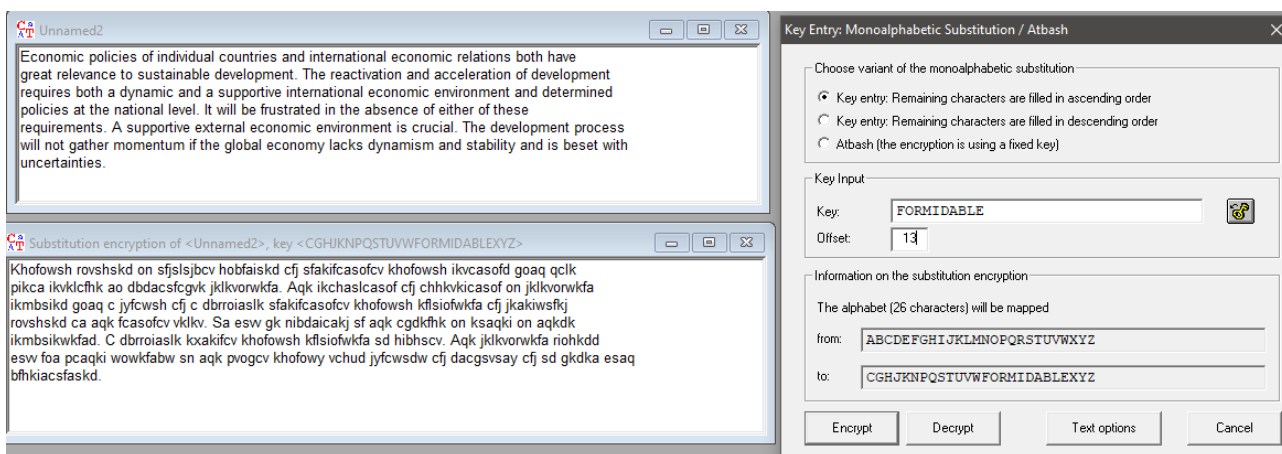


Рисунок 15 – Шифрование английского текста ~600 символов

Выполним атаку на шифротекст, результат приведен на рисунке 16.

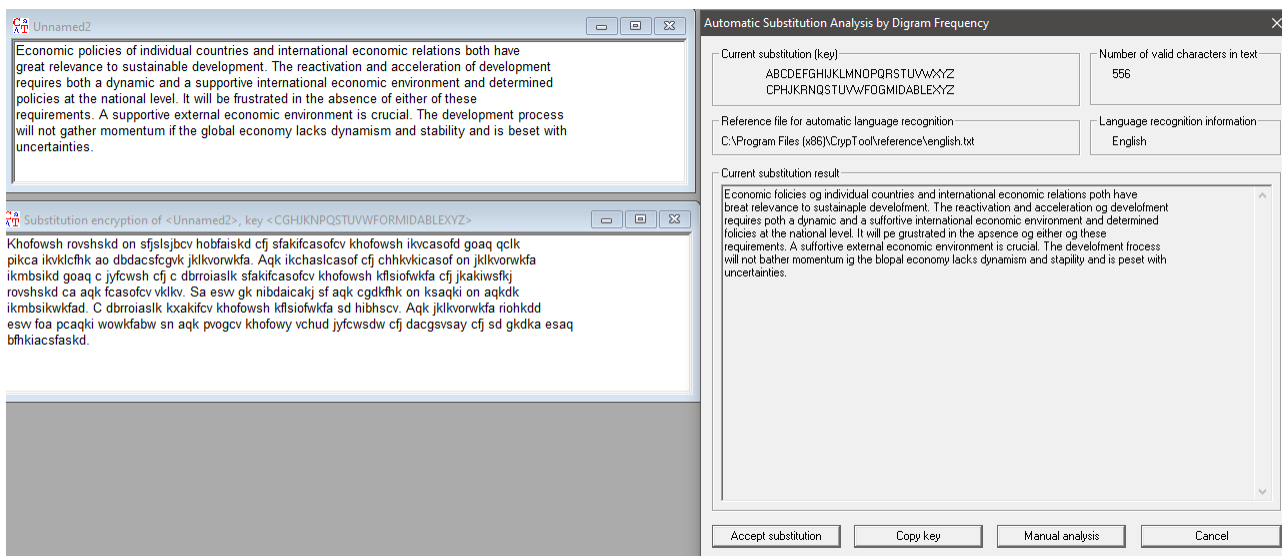


Рисунок 16 – Атака на шифротекст ~600 символов

За исключением нескольких символов можно считать атаку успешной, человек может понять смысл полученного текста.

Повторим процедуру для текстов в ~300 и 150 символов. Ключ и смещения оставим теми же.

Результат шифрования и атаки на текст в ~300 символов приведен на рисунке 17.

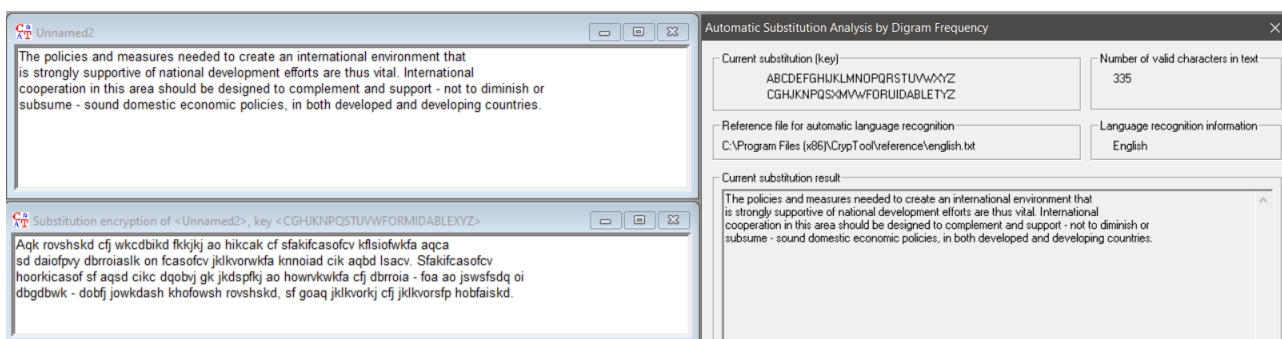


Рисунок 17 – Атака на шифротекст ~300 символов

Текст был полностью дешифрован, полученное сообщение полностью корректно.

При попытке провести атаку на текст с меньшим количеством символов, например, ~150, получаем предупреждение (см. рис. 18).

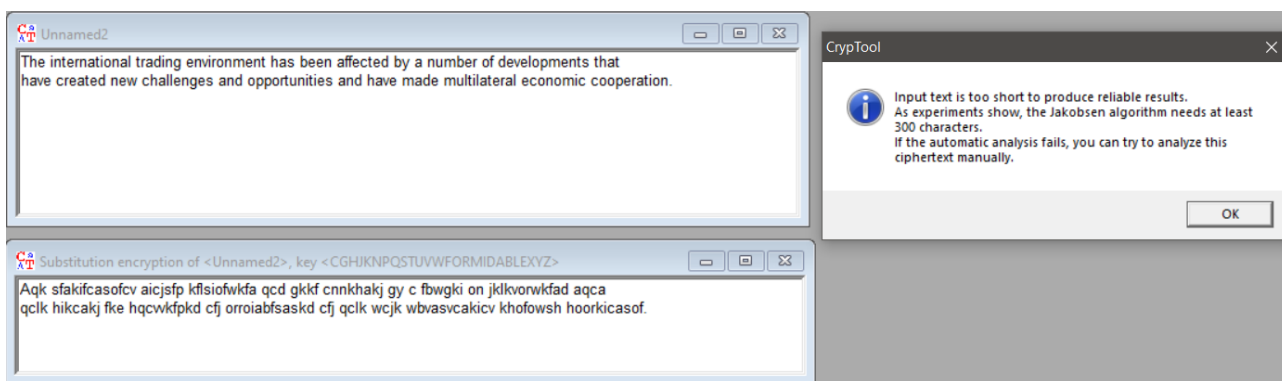


Рисунок 18 – Предупреждение о потенциальной ненадежности результатов

Принимая условия программы, получаем следующие результаты атаки (см. рис. 19).

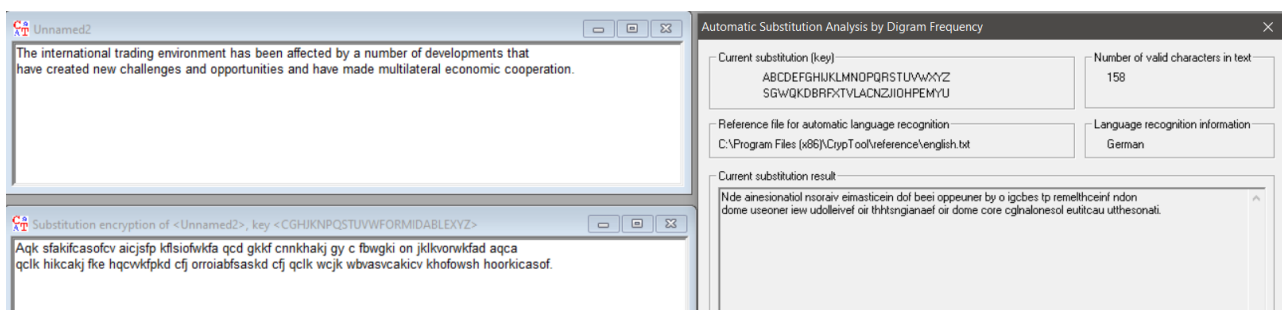


Рисунок 19 – Атака на шифротекст ~150 символов

Как и ожидалось, сообщение не получилось дешифровать автоматическими алгоритмами.

В Cryptool 1 существует возможность ручного анализа, интерфейс которого представлен на рисунке 20.

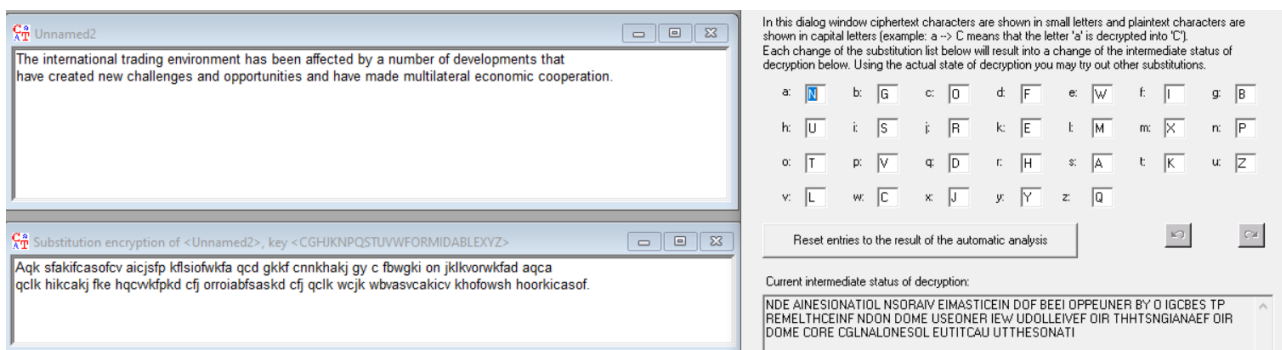


Рисунок 20 – Интерфейс ручного анализа

Зная минимальную информацию об исходном сообщении можно попытаться идентифицировать такие служебные слова английского языка, как «the», «that», «has», «been». Заменяя вручную буквы этих слов (после семантического анализа) можно частично восстановить алфавит и делать предположения относительно других букв (см. рис. 21).

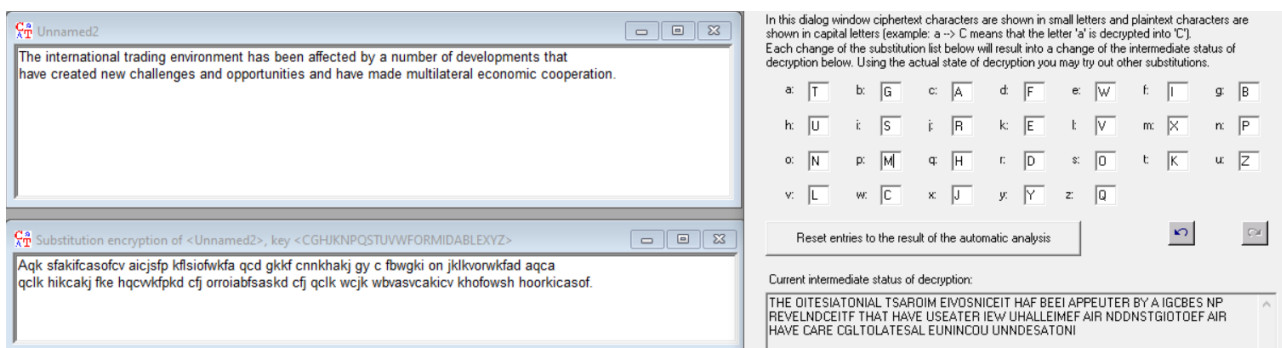


Рисунок 21 – Процесс ручного анализа с применением семантических эвристик

Попробуем вручную расшифровать текст ~600 символов, зашифрованный с ключом MANUAL и смещением 5. Предположим, что мы не знаем ключ шифра.

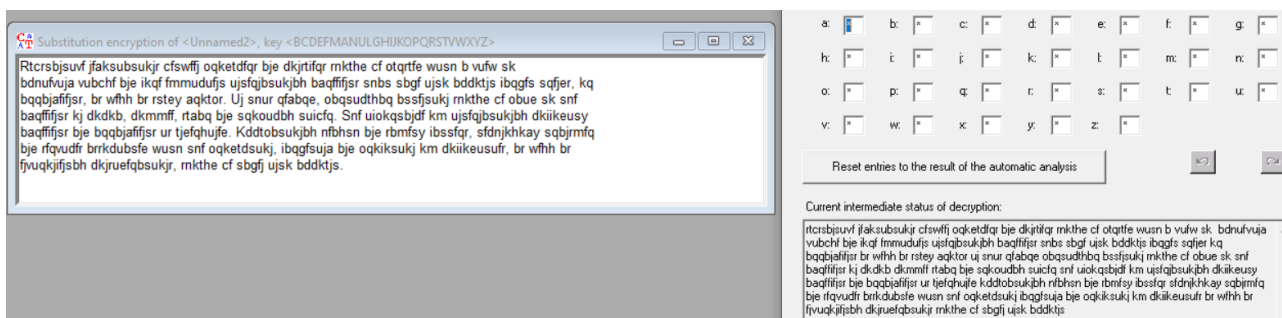


Рисунок 22 – Перехваченный текст и средства ручного анализа

Попробуем начать с коротких слов длины 2-3. Зачастую это союзы, предлоги и местоимения. Первое такое слово – «bje» не может быть вопросительным местоимением. Скорее всего, это либо предлог «for», либо союз «and». Примем гипотезу, что это союз. Результат приведен на рисунке 23.

ной вероятностью «SHOULD BE TAKEN».

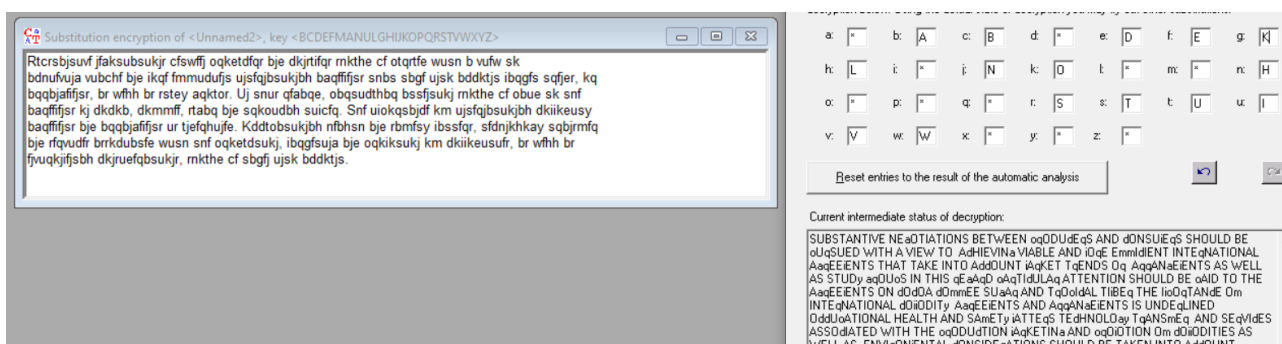


Рисунок 25 – Промежуточный результат ручной атаки

Когда угадана большая часть алфавита, слова уже интуитивно узнаются носителем языка. Результат успешной ручной атаки представлен на рисунке 26.

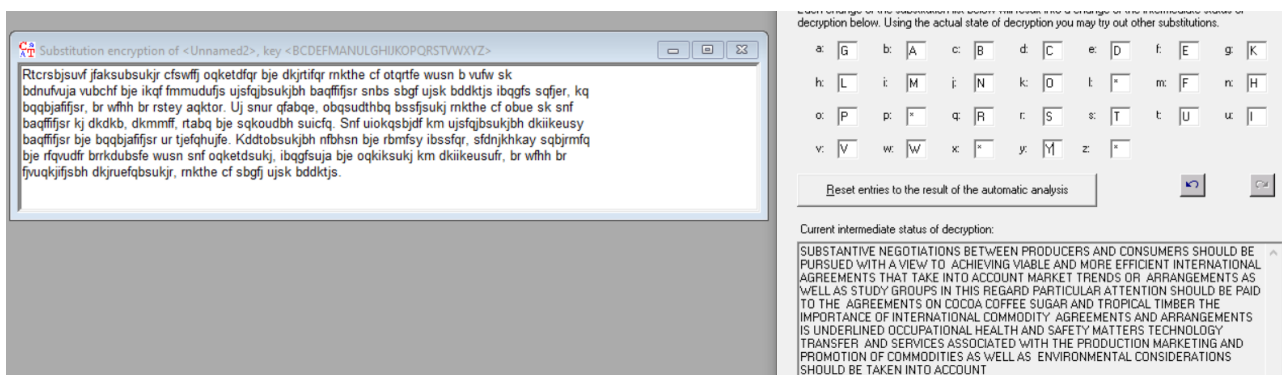


Рисунок 26 – Успешная ручная атака на шифр моноалфавитной подстановки

Сложность атаки на шифр – 26!. Именно столько существует различных отображений английского алфавита в самого себя.

В Cryptool 1 используются эвристики нахождения частотных слов или биграмм (двубуквенных сочетаний). Интерфейс атаки на данный шифр в Cryptool 2 приведен на рисунке ниже.



Рисунок 27 – Атака на шифр моноалфавитной подстановки в Cryptool 2

Атака практически восстановила исходное сообщение за исключением нескольких букв. Существует возможность настройки параметров атаки, например алгоритма и эвристик (см. рис. 28).

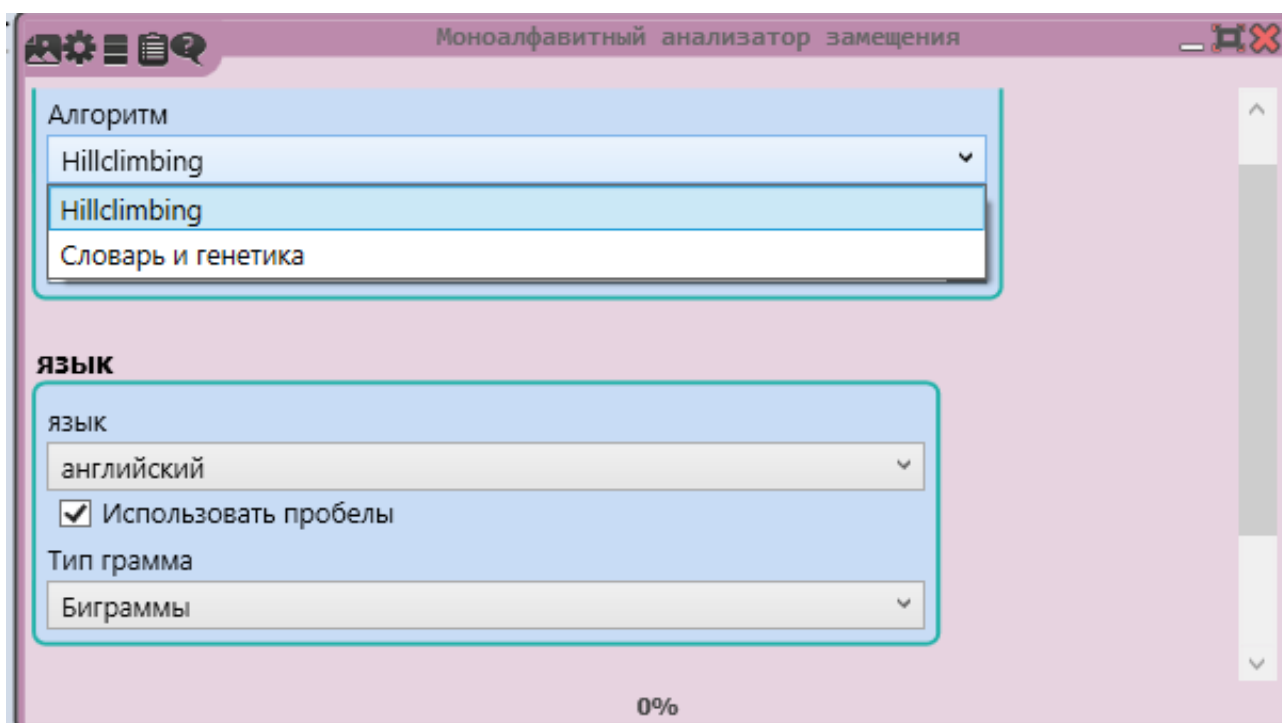


Рисунок 28 – Параметры атаки на шифр моноалфавитной подстановки в Cryptool 2

В основе работы атаки лежит статья «Olson, E.: Robust Dictionary Attack of Short Simple Substitution Ciphers». Из документации к Cryptool 2: «Этот компонент использует два разных подхода для поиска открытого текста и соответствующего ключа. Сначала выполняется атака словаря. В словарном словаре слова предполагаемого языка открытого текста отображаются на слова в данном зашифрованном тексте. Если будет найдено допустимое сопоставление, будет указан соответствующий ключ. Помимо атаки словаря, выполняется эвристический поиск на основе генетического алгоритма и частот буквенных групп. Этот подход основан на пошаговом режиме и создает случайным образом новые ключевые кандидаты, которые оцениваются в соответствии со стоимостью.»

Атака на шифротекст коллеги.

Для коллеги по учебной группе был сгенерирован следующий шифротекст с известными параметрами (см. рис. 29):

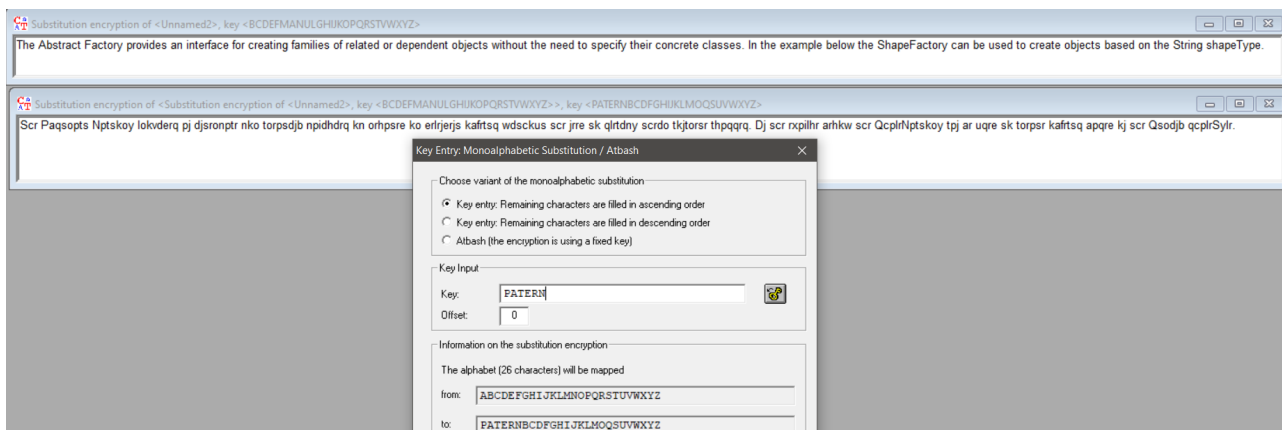


Рисунок 29 – Генерация шифротекста для коллеги

От коллеги был получен следующий шифротекст:

«G iave kls iad aky exneqsgre gk lqhakgzgkh ruci sigkhr, akd iad sl hl siqluhi gs app flq sie fgqrs sgje. Ieqe gr a jlqe lq perr desagped dercqngsglk lf sie tluqkey. Feep fqee sl peaql fqlj gs akd jame a besseq clkfeqekce yluqrepf. We wgpp sqy sl jame a besseq lke kexs yeaq.».

Исходное сообщение было зашифровано не очень хорошо, узнаются выражения «Feel free», «We will» и слова «have» (iave) и «year» (yeaq).

Результат ручной дешифровки приведен на рисунке 30.

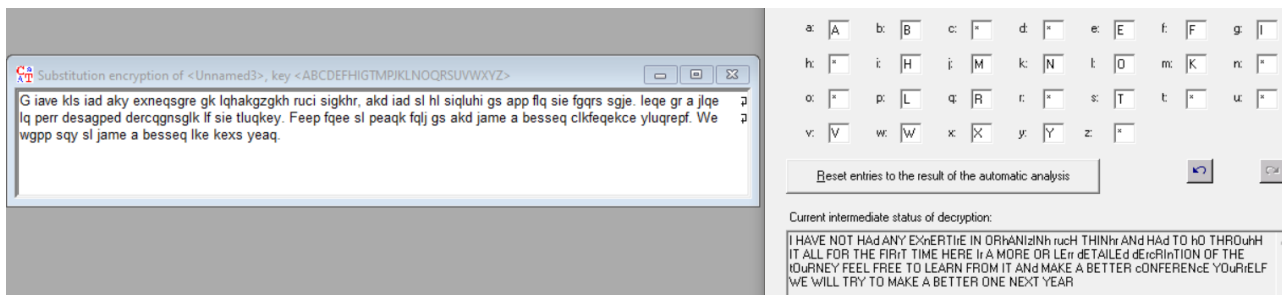


Рисунок 30 – Атака на шифротекст коллеги

Окончательный результат имеет вид:

«I have not had any expertise in organizing such things, and had to go through it all for the first time. Here is a more or less detailed description of the journey. Feel free to learn from it and make a better conference yourself. We will try to make a better one next year».

Вывод.

Был изучен шифр моноалфавитной подстановки. С помощью программы Cryptool 1 был зашифрован открытый текст для отправки коллеге. Также был проведен автоматический и ручной анализ шифротекстов с помощью встроенный в программу инструментов. Был изучен принцип атаки на данный шифр в программе Cryptool 2.

Шифр Хилла (Hill).

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 выбранным ключом 2×2 . Убедиться в совпадении результатов. Проверить обратимость шифрующей матрицы (ключа).
3. Зашифровать текст с произвольным сообщением в формате «DEAR MR ФАМИЛИЯ ИМЯ ОТЧЕСТВО THANK YOU VERY MUCH», используя транслитерацию латиницей и шифрующую матрицу 3×3 .
4. Выполнить атаку на основе знания открытого текста, используя приложение из Analysis-> Symmetric Encryption(classic)-> Known Plaintext.
5. Удалить из сообщения и шифротекста фрагменты с ФАМИЛИЯ ИМЯ ОТЧЕСТВО и повторить атаку. Убедиться, что полученный ключ (матрица) совпадает с исходным.
6. Передать произвольную шифровку коллеге по учебной группе для расшифрования при условии, что формы обращения и завершения сообщения известны. Размер использованного ключа держать в секрете.

Описание шифра.

Шифр Хилла основан на матричном преобразовании текста. Перед шифрованием необходимо каждому символу алфавита следует сопоставить код равный порядковому номеру символа в алфавите. Затем коды символов открытого текста записываются в матрицу размера $n \times m$ и создается шифрующая матрица $n \times n$. Для шифрования производится умножение матрицы открытого текста на шифрующую матрицу и вычисляется остаток от деления значения элементов матрицы-произведения на число символов выбранного

алфавита. Для расшифровки необходимо шифротекст умножить на матрицу, которая является мультипликативной инверсией по отношению к шифрующей для выбранного алфавита. В качестве примера шифрования, зашифруем текст «HILLCIPHEREXAMPLES»:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|----------|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| a | b | c | d | e | f | g | h | <u>i</u> | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

| | | |
|----|----|----|
| 7 | 8 | 11 |
| 11 | 2 | 8 |
| 15 | 7 | 4 |
| 17 | 4 | 23 |
| 0 | 12 | 15 |
| 11 | 4 | 18 |

 \times

| | | |
|----|----|----|
| 6 | 24 | 1 |
| 13 | 16 | 10 |
| 20 | 17 | 15 |

 $=$

| | | |
|-----|-----|-----|
| 366 | 483 | 552 |
| 252 | 432 | 151 |
| 261 | 540 | 145 |
| 614 | 863 | 402 |
| 456 | 447 | 345 |
| 478 | 634 | 321 |

 \equiv

| | | |
|----|----|----|
| 2 | 15 | 18 |
| 18 | 16 | 21 |
| 1 | 20 | 15 |
| 16 | 5 | 12 |
| 14 | 5 | 7 |
| 10 | 10 | 9 |

 $(mod 26)$

Шифрующая матрица

Рисунок 31 – Пример шифрования

Шифротекст: CPSSQVBUPQFMOFHKKJ Для демонстрации дешифровки, расшифруем полученный шифротекст «CPSSQVBUPQFMOFHKKJ»:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|----------|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| a | b | c | d | e | f | g | h | <u>i</u> | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

| | | |
|----|----|----|
| 2 | 15 | 18 |
| 18 | 16 | 21 |
| 1 | 20 | 15 |
| 16 | 5 | 12 |
| 14 | 5 | 7 |
| 10 | 10 | 9 |

 \times

| | | |
|----|----|----|
| 8 | 5 | 10 |
| 21 | 8 | 21 |
| 21 | 12 | 8 |

 $=$

| | | |
|-----|-----|-----|
| 709 | 346 | 479 |
| 921 | 470 | 684 |
| 743 | 345 | 550 |
| 485 | 264 | 361 |
| 364 | 194 | 301 |
| 479 | 238 | 382 |

 \equiv

| | | |
|----|----|----|
| 7 | 8 | 11 |
| 11 | 2 | 8 |
| 15 | 7 | 4 |
| 17 | 4 | 23 |
| 0 | 12 | 15 |
| 11 | 4 | 18 |

 $(mod 26)$

Дешифрующая матрица (обратная)

Рисунок 32 – Пример дешифровки

Получаем открытый текст: HILLCIPHEREXAMPLES.

Ключ: элементы шифрующей матрицы и размер алфавита. Тип шифра: блочный, шифр замены.

Реализация в Cryptool.

Зашифруем фамилию Nечеруренко с помощью шифра Hill. Интерфейс шифра Hill в программе Cryptool приведен на рисунке 33.

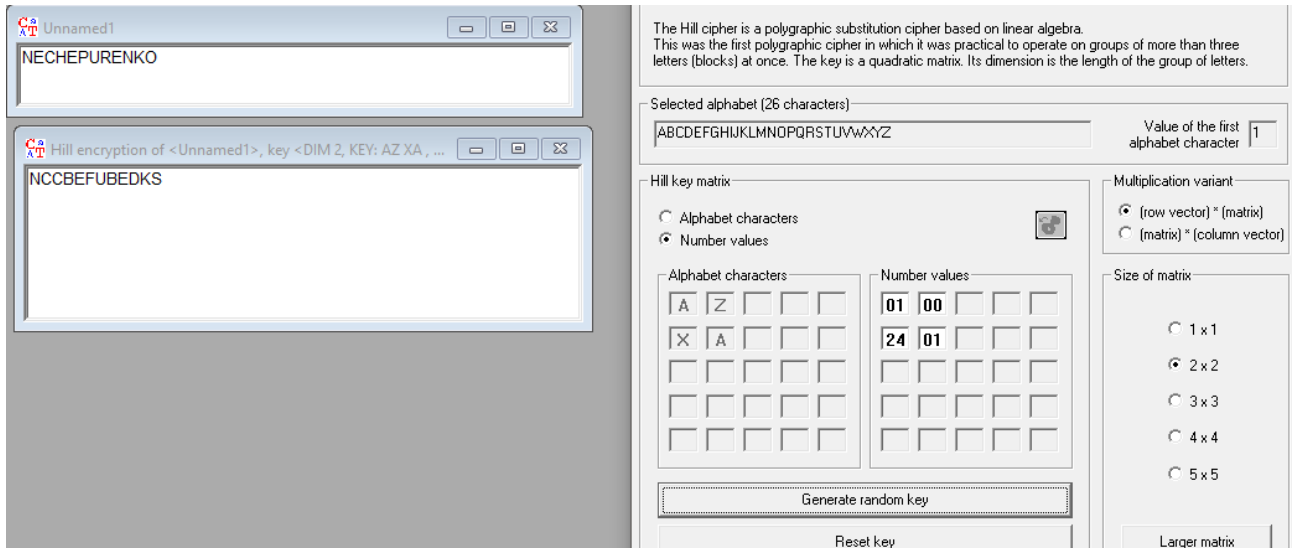


Рисунок 33 – Параметры шифра Hill

Выберем в интерфейсе для шифрования матрицу

$$\begin{pmatrix} 1 & 0 \\ 24 & 1 \end{pmatrix}$$

Вручную шифровка будет иметь следующий вид:

$$\begin{pmatrix} 14 & 5 \\ 3 & 8 \\ 5 & 16 \\ 21 & 18 \\ 5 & 14 \\ 11 & 15 \end{pmatrix} \cdot \begin{pmatrix} 1 & 26 \\ 24 & 1 \end{pmatrix}^T = \begin{pmatrix} 14 & 3 \\ 3 & 2 \\ 5 & 6 \\ 21 & 2 \\ 5 & 4 \\ 11 & 19 \end{pmatrix} \pmod{26}$$

26 неотлично от 0 в кольце вычетов по модулю 26, транспонирование матрицы выполнено для соответствия алгоритму перемножения в Cryptool.

Для дешифровки необходимо найти обратную матрицу. Имеем:

$$\begin{pmatrix} 1 & 26 \\ 24 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 26 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}$$

Результат дешифрации в Cryptool приведен на рисунке 34.

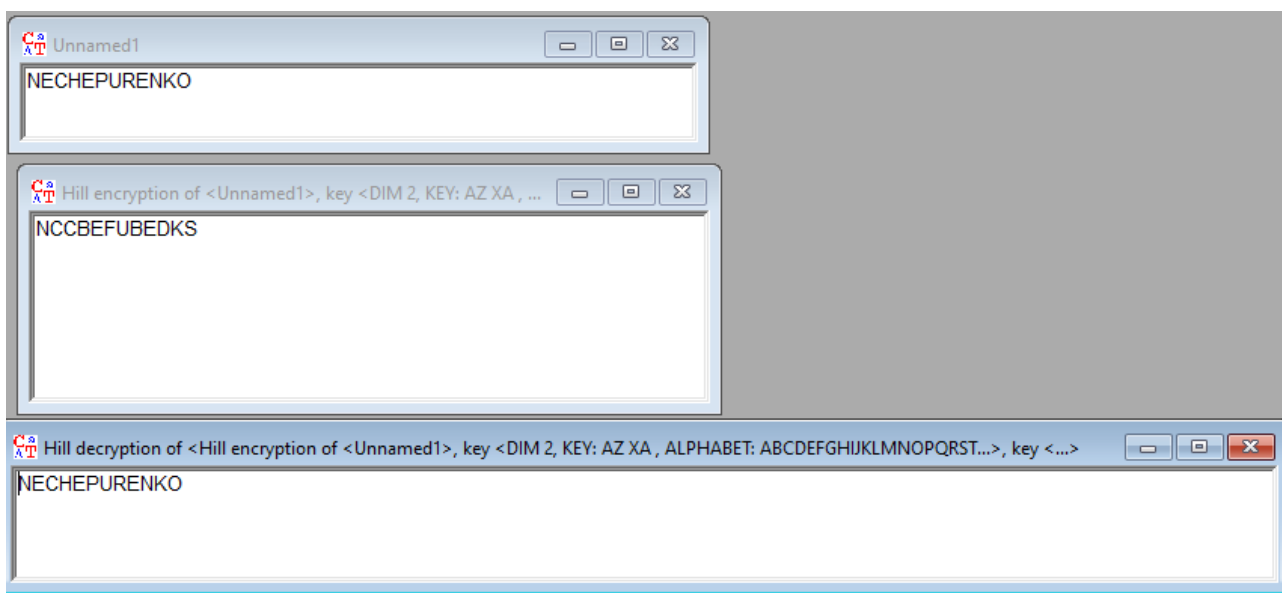


Рисунок 34 – Дешифровка фамилии NECHEPURENKO

Ручные расчеты имеют вид:

$$\begin{pmatrix} 14 & 3 \\ 3 & 2 \\ 5 & 6 \\ 21 & 2 \\ 5 & 4 \\ 11 & 19 \end{pmatrix} \cdot \begin{pmatrix} 1 & 26 \\ 2 & 1 \end{pmatrix}^T = \begin{pmatrix} 14 & 5 \\ 3 & 8 \\ 5 & 16 \\ 21 & 18 \\ 5 & 14 \\ 11 & 15 \end{pmatrix} \pmod{26}$$

Закодируем сообщение «DEAR MR NECHEPURENKO NIKITA ALEKSANDROV THANK YOU VERY MUCH». Результат шифрования и параметры приведены на рисунке 35.

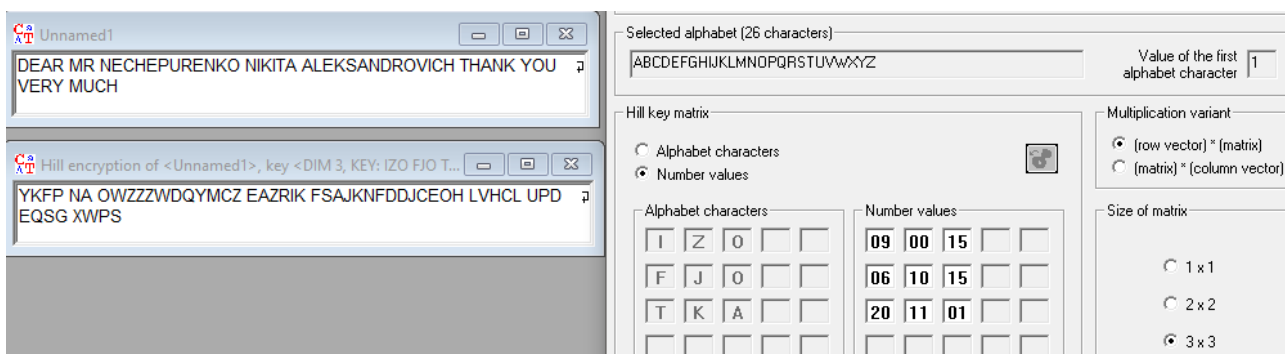


Рисунок 35 – Шифровка фразы

На рисунке 36 приведен интерфейс атаки на шифротекст в программе Cryptool.

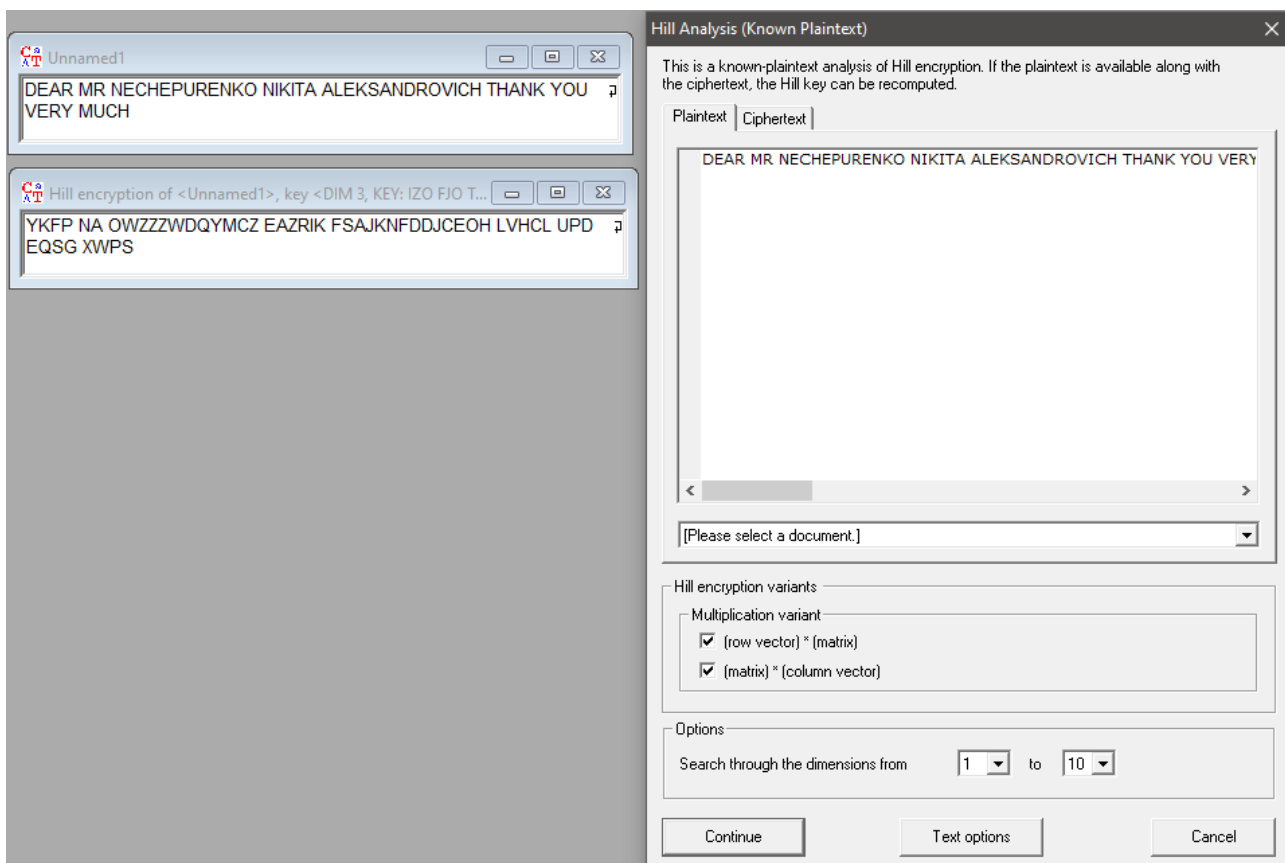


Рисунок 36 – Интерфейс атаки на шифр Hill

Атака была произведена успешно, был получен ключ (см. рис. 37).

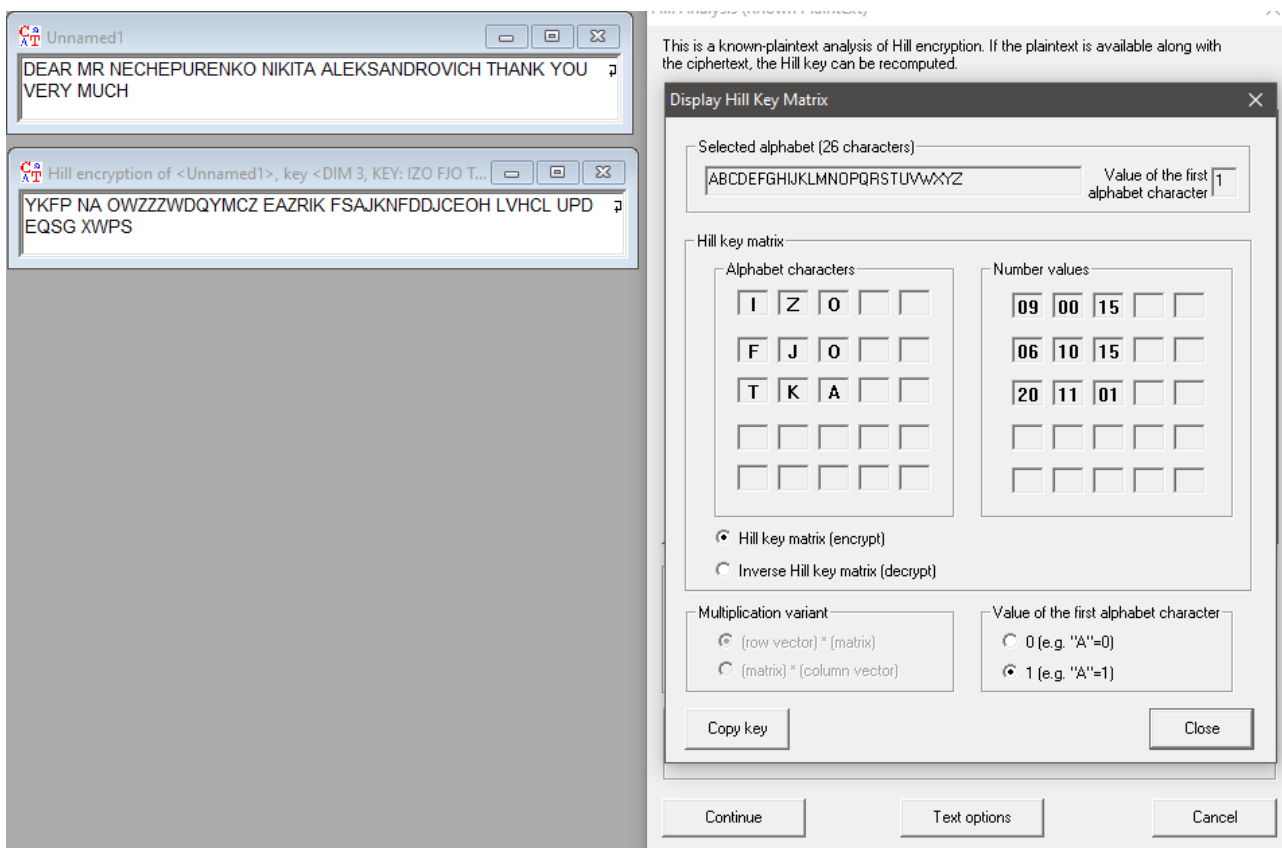


Рисунок 37 – Результат атаки на шифр Hill

Удалим из шифротекста и сообщения фрагменты NECHEPURENKO NIKITA ALEKSANDROVICH и повторим атаку. Ключ совпал.

Атака может найти один из возможных ключей шифра. Принцип работы атаки следующий:

1. Выбрать n – размерность шифрующей матрицы
2. Разделить текст на блоки размера n
3. Вычислить шифрующую матрицу
4. Если полученная матрица обратима в кольце вычетов по модулю 26, то принимаем ее за ключ

Сложность атаки вычисляется из пространства возможных n , процесса матричного умножения и обращения матриц. Асимптотически имеем оценку $O(n^4)$.

Атака на шифротекст коллеги.

Для коллеги по учебной группе был предложен следующий шифротекст:
«RAHW SL DPKH JKPM TVBW CODM X CDBS VQF»

Начало имеет вид «DEAR MR» и окончание «HAVE A NICE DAY».

От коллеги был получен текст:

«BQDX IG ZQIOOR JREHBCRH DTEG UC MKO TFP»

Было известно, что он начинается на «DEAR MR» и оканчивается на «GOOD TO SEE YOU». В результате атаки был найден ключ, приведенный на рисунке 38.

Display Hill Key Matrix

×

Selected alphabet (26 characters)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Value of the first alphabet character

1

Hill key matrix

Alphabet characters

| | | | | |
|---|---|---|---|--|
| V | A | Y | U | |
| U | W | N | R | |
| Q | C | I | K | |
| E | X | N | M | |
| | | | | |

☒ Hill key matrix (encrypt)
☐ Inverse Hill key matrix (decrypt)

Number values

| | | | | |
|----|----|----|----|--|
| 22 | 01 | 25 | 21 | |
| 21 | 23 | 14 | 18 | |
| 17 | 03 | 09 | 11 | |
| 05 | 24 | 14 | 13 | |
| | | | | |

Multiplication variant

☒ (row vector) * (matrix)
☐ (matrix) * (column vector)

Value of the first alphabet character

☐ 0 (e.g. "A"=0)
☒ 1 (e.g. "A"=1)

Copy key

Close

Рисунок 38 – Ключ от переданного коллегой шифротекста

Дешифрованное сообщение имеет вид: «DEAR MR ALBERT EINSTEIN
GOOD TO SEE YOU».

Заключение.

В результате выполнения работы были изучены 3 классических шифра: Scytale, Substitution, Hill. Были изучены принципы шифрования, используемые ключи и сложность атаки методом грубой силы. С помощью программ Cryptool 1 и Cryptool 2 были произведены шифровки и дешифровки различных сообщений и шифротекстов. Были изучены инструменты автоматических атак на упомянутые шифры. С помощью атак были дешифрованы полученные от коллеги сообщения.