**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Основы кибербезопасности»

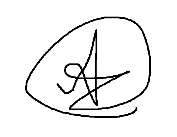
**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

«**Анализ исторических шифров с помощью программного средства Cryptool 2**»

**Выполнил:**

студент группы М32111

Акберов Рустам Ханкишиевич

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Таранов Сергей Владимирович

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

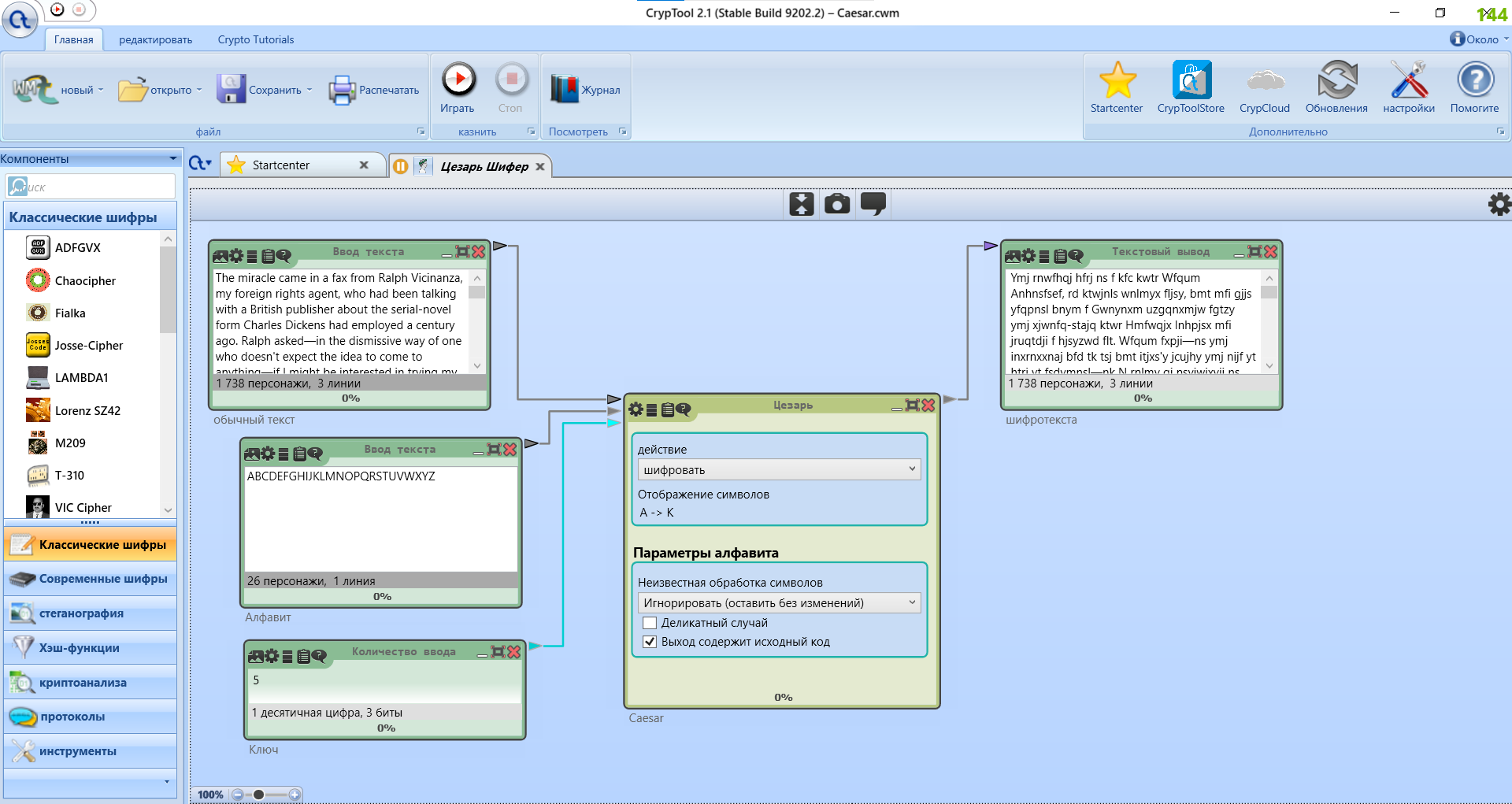
(подпись)

Санкт-Петербург

2022 г.

1. **Цель работы:** с помощью программного средства CrypTool 2 изучить принципы работы исторических шифров, а также провести их криптоанализ.
2. **Ход работы:**
3. *Шифр Цезаря.*

Выполним шифрование открытого текста, используя шаблон из программы CrypTool 2. В качестве открытого текста возьмем отрывок из книги Стивена Кинга «Зеленая миля». В качестве ключа возьмем число 5.

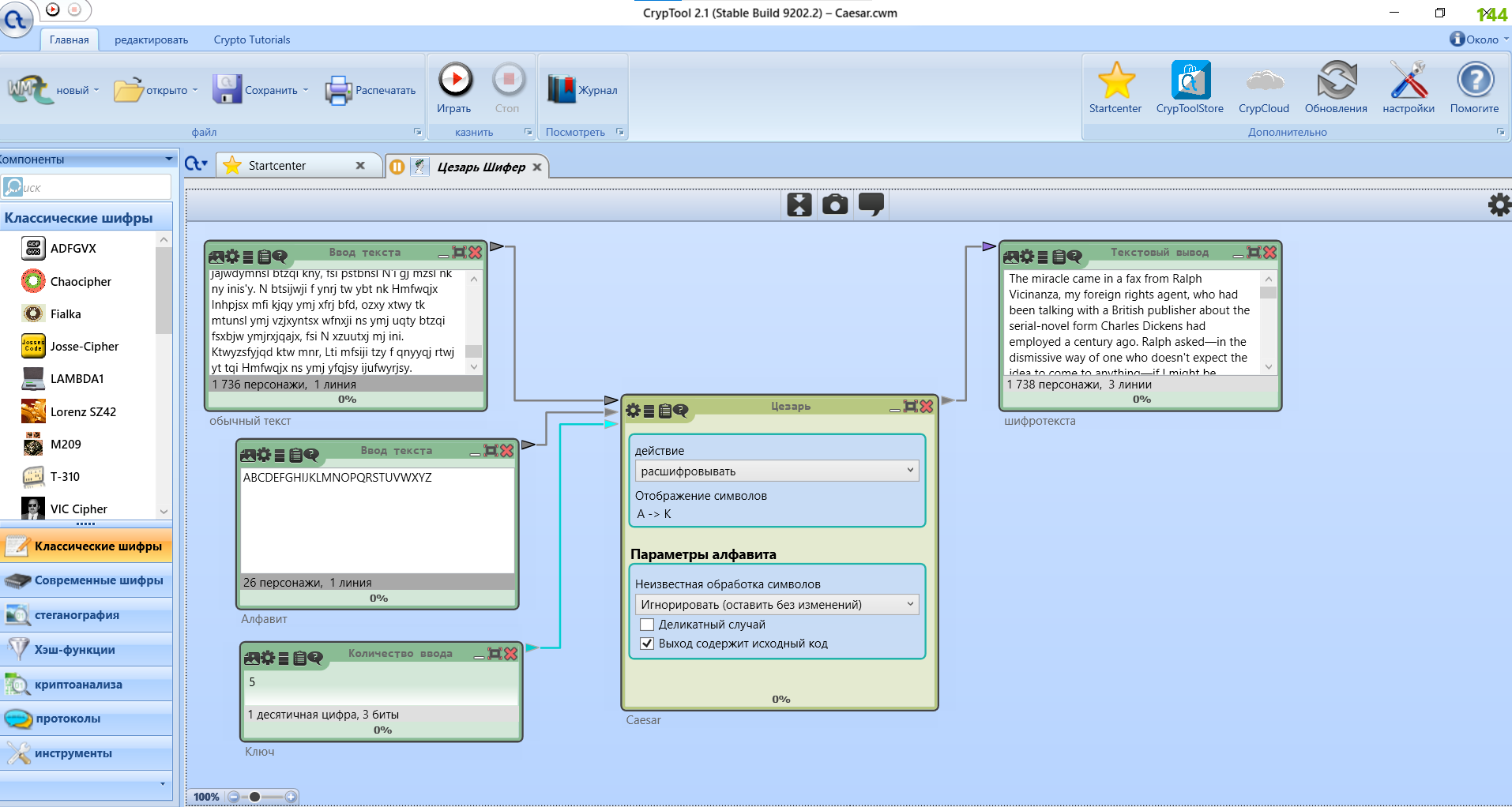


Исходный текст: *The miracle came in a fax from Ralph Vicinanza, my foreign rights agent, who had been talking with a British publisher about the serial-novel form Charles Dickens had employed a century ago. Ralph asked—in the dismissive way of one who doesn't expect the idea to come to anything—if I might be interested in trying my hand at the form. Man, I leaped at it. I understood at once that if I agreed to such a project, I would have to finish The Green Mile. So, feeling like a Roman soldier setting fire to the bridge across the Rubicon, I called Ralph and asked him to make the deal. He did, and the rest you know. John Coffey, Paul Edgecombe, Brutal Howell, Percy Wetmore... they took over and made the story happen. It was most severely cool.  
   The Green Mile had a kind of magical acceptance which I never expected; I thought, in fact, that it might well be a commercial disaster. The feedback from the readers was wonderful, and this time even most of the critics went along for the ride. I think I owe a lot of the book's popular acceptance to my wife's perceptive suggestions, and a lot of its commercial success to the hard work done on its behalf by the people at Dutton Signet.  
   The experience itself, however, was mine alone. I wrote like a madman, trying to keep up with the crazy publishing schedule and at the same time trying to craft the book so that each part would have its own mini-climax, hoping that everything would fit, and knowing I'd be hung if it didn't. I wondered a time or two if Charles Dickens had felt the same way, just sort of hoping the questions raised in the plot would answer themselves, and I suppose he did. Fortunately for him, God handed out a little more to old Charles in the talent department.*

Полученный текст: *Ymj rnwfhqj hfrj ns f kfc kwtr Wfqum Anhnsfsef, rd ktwjnls wnlmyx fljsy, bmt mfi gjjs yfqpnsl bnym f Gwnynxm uzgqnxmjw fgtzy ymj xjwnfq-stajq ktwr Hmfwqjx Inhpjsx mfi jruqtdji f hjsyzwd flt. Wfqum fxpji—ns ymj inxrnxxnaj bfd tk tsj bmt itjxs'y jcujhy ymj nijf yt htrj yt fsdymnsl—nk N rnlmy gj nsyjwjxyji ns ywdnsl rd mfsi fy ymj ktwr. Rfs, N qjfuji fy ny. N zsijwxytti fy tshj ymfy nk N flwjji yt xzhm f uwtojhy, N btzqi mfaj yt knsnxm Ymj Lwjjs Rnqj. Xt, kjjqnsl qnpj f Wtrfs xtqinjw xjyynsl knwj yt ymj gwnilj fhwtxx ymj Wzgnhts, N hfqqji Wfqum fsi fxpji mnr yt rfpj ymj ijfq. Mj ini, fsi ymj wjxy dtz pstb. Otms Htkkjd, Ufzq Jiljhtrgj, Gwzyfq Mtbjqq, Ujwhd Bjyrtwj... ymjd yttp tajw fsi rfij ymj xytwd mfuujs. Ny bfx rtxy xjajwjqd httq. Ymj Lwjjs Rnqj mfi f pnsi tk rflnhfq fhhjuyfshj bmnhm N sjajw jcujhyji; N ymtzlmy, ns kfhy, ymfy ny rnlmy bjqq gj f htrrjwhnfq inxfxyjw. Ymj kjjigfhp kwtr ymj wjfijwx bfx btsijwkzq, fsi ymnx ynrj jajs rtxy tk ymj hwnynhx bjsy fqtsl ktw ymj wnij. N ymnsp N tbj f qty tk ymj gttp'x utuzqfw fhhjuyfshj yt rd bnkj'x ujwhjuynaj xzlljxyntsx, fsi f qty tk nyx htrrjwhnfq xzhhjxx yt ymj mfwi btwp itsj ts nyx gjmfqk gd ymj ujtuqj fy Izyyts Xnlsjy. Ymj jcujwnjshj nyxjqk, mtbjajw, bfx rnsj fqtsj. N bwtyj qnpj f rfirfs, ywdnsl yt pjju zu bnym ymj hwfed uzgqnxmnsl xhmjizqj fsi fy ymj xfrj ynrj ywdnsl yt hwfky ymj gttp xt ymfy jfhm ufwy btzqi mfaj nyx tbs rnsn-hqnrfc, mtunsl ymfy jajwdymnsl btzqi kny, fsi pstbnsl N'i gj mzsl nk ny inis'y. N btsijwji f ynrj tw ybt nk Hmfwqjx Inhpjsx mfi kjqy ymj xfrj bfd, ozxy xtwy tk mtunsl ymj vzjxyntsx wfnxji ns ymj uqty btzqi fsxbjw ymjrxjqajx, fsi N xzuutxj mj ini. Ktwyzsfyjqd ktw mnr, Lti mfsiji tzy f qnyyqj rtwj yt tqi Hmfwqjx ns ymj yfqjsy ijufwyrjsy.*

* 1. Выполним дешифрование полученного текста:

Для этого нужно будет выбрать действие «Расшифровать» в блоке Цезарь.

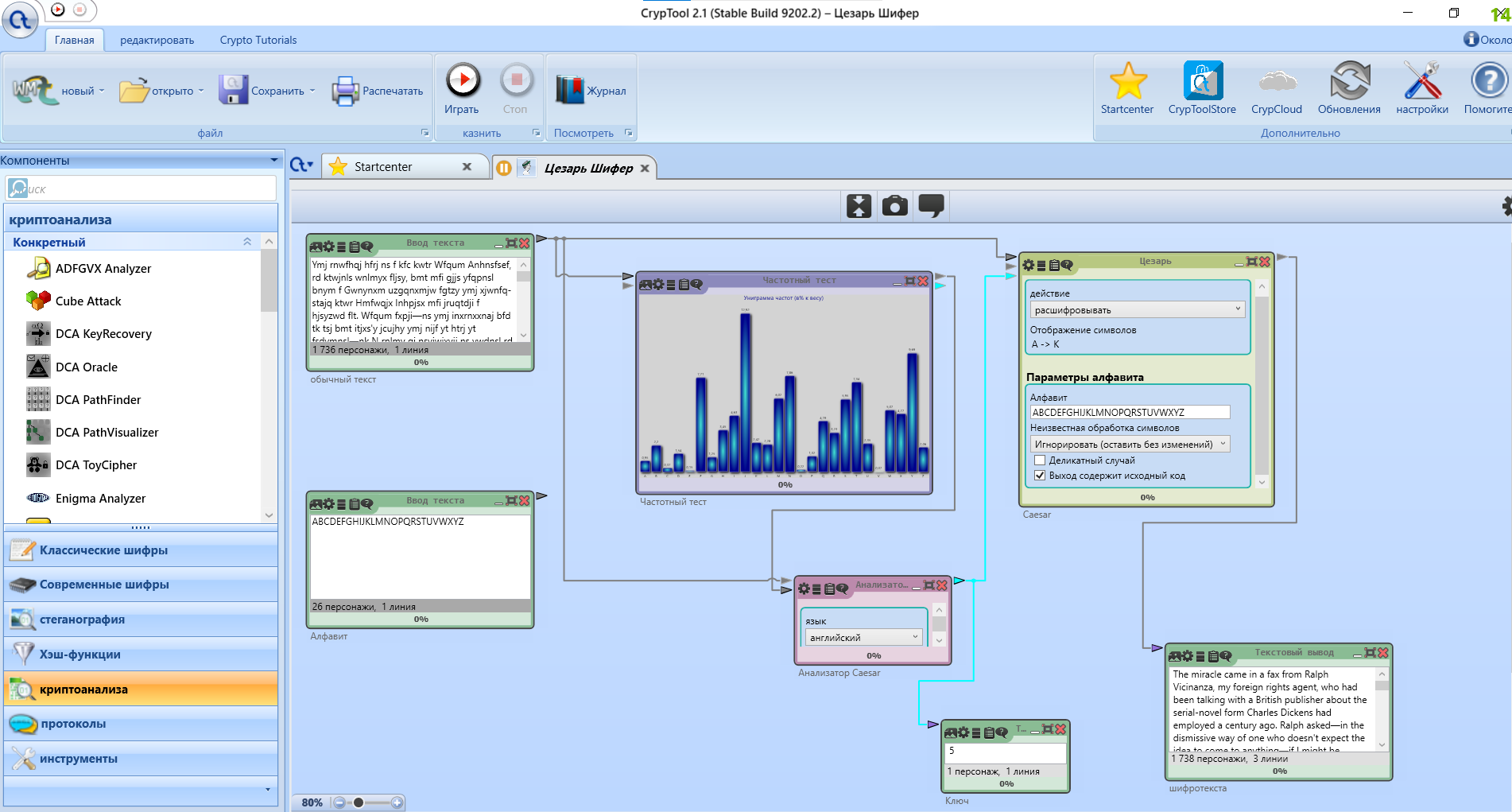


* 1. Сравним исходный текст из пункта a и полученный текст из пункта b:

|  |  |
| --- | --- |
| Исходный открытый текст | Текст после дешифровки в пункте b |
| The miracle came in a fax from Ralph Vicinanza, my foreign rights agent, who had been talking with a British publisher about the serial-novel form Charles Dickens had employed a century ago. Ralph asked—in the dismissive way of one who doesn't expect the idea to come to anything—if I might be interested in trying my hand at the form. Man, I leaped at it. I understood at once that if I agreed to such a project, I would have to finish The Green Mile. So, feeling like a Roman soldier setting fire to the bridge across the Rubicon, I called Ralph and asked him to make the deal. He did, and the rest you know. John Coffey, Paul Edgecombe, Brutal Howell, Percy Wetmore... they took over and made the story happen. It was most severely cool.  The Green Mile had a kind of magical acceptance which I never expected; I thought, in fact, that it might well be a commercial disaster. The feedback from the readers was wonderful, and this time even most of the critics went along for the ride. I think I owe a lot of the book's popular acceptance to my wife's perceptive suggestions, and a lot of its commercial success to the hard work done on its behalf by the people at Dutton Signet.  The experience itself, however, was mine alone. I wrote like a madman, trying to keep up with the crazy publishing schedule and at the same time trying to craft the book so that each part would have its own mini-climax, hoping that everything would fit, and knowing I'd be hung if it didn't. I wondered a time or two if Charles Dickens had felt the same way, just sort of hoping the questions raised in the plot would answer themselves, and I suppose he did. Fortunately for him, God handed out a little more to old Charles in the talent department. | The miracle came in a fax from Ralph Vicinanza, my foreign rights agent, who had been talking with a British publisher about the serial-novel form Charles Dickens had employed a century ago. Ralph asked—in the dismissive way of one who doesn't expect the idea to come to anything—if I might be interested in trying my hand at the form. Man, I leaped at it. I understood at once that if I agreed to such a project, I would have to finish The Green Mile. So, feeling like a Roman soldier setting fire to the bridge across the Rubicon, I called Ralph and asked him to make the deal. He did, and the rest you know. John Coffey, Paul Edgecombe, Brutal Howell, Percy Wetmore... they took over and made the story happen. It was most severely cool.  The Green Mile had a kind of magical acceptance which I never expected; I thought, in fact, that it might well be a commercial disaster. The feedback from the readers was wonderful, and this time even most of the critics went along for the ride. I think I owe a lot of the book's popular acceptance to my wife's perceptive suggestions, and a lot of its commercial success to the hard work done on its behalf by the people at Dutton Signet.  The experience itself, however, was mine alone. I wrote like a madman, trying to keep up with the crazy publishing schedule and at the same time trying to craft the book so that each part would have its own mini-climax, hoping that everything would fit, and knowing I'd be hung if it didn't. I wondered a time or two if Charles Dickens had felt the same way, just sort of hoping the questions raised in the plot would answer themselves, and I suppose he did. Fortunately for him, God handed out a little more to old Charles in the talent department. |

В результате сравнения этих двух текстов было выявлено их полное совпадение.

* 1. Выполним простейший криптоанализ, используя шаблон для атаки на основе частотного анализа из программы CrypTool 2. Целью данной атаки является восстановление секретного ключа и исходного текста на основе частотного анализа закрытого текста.

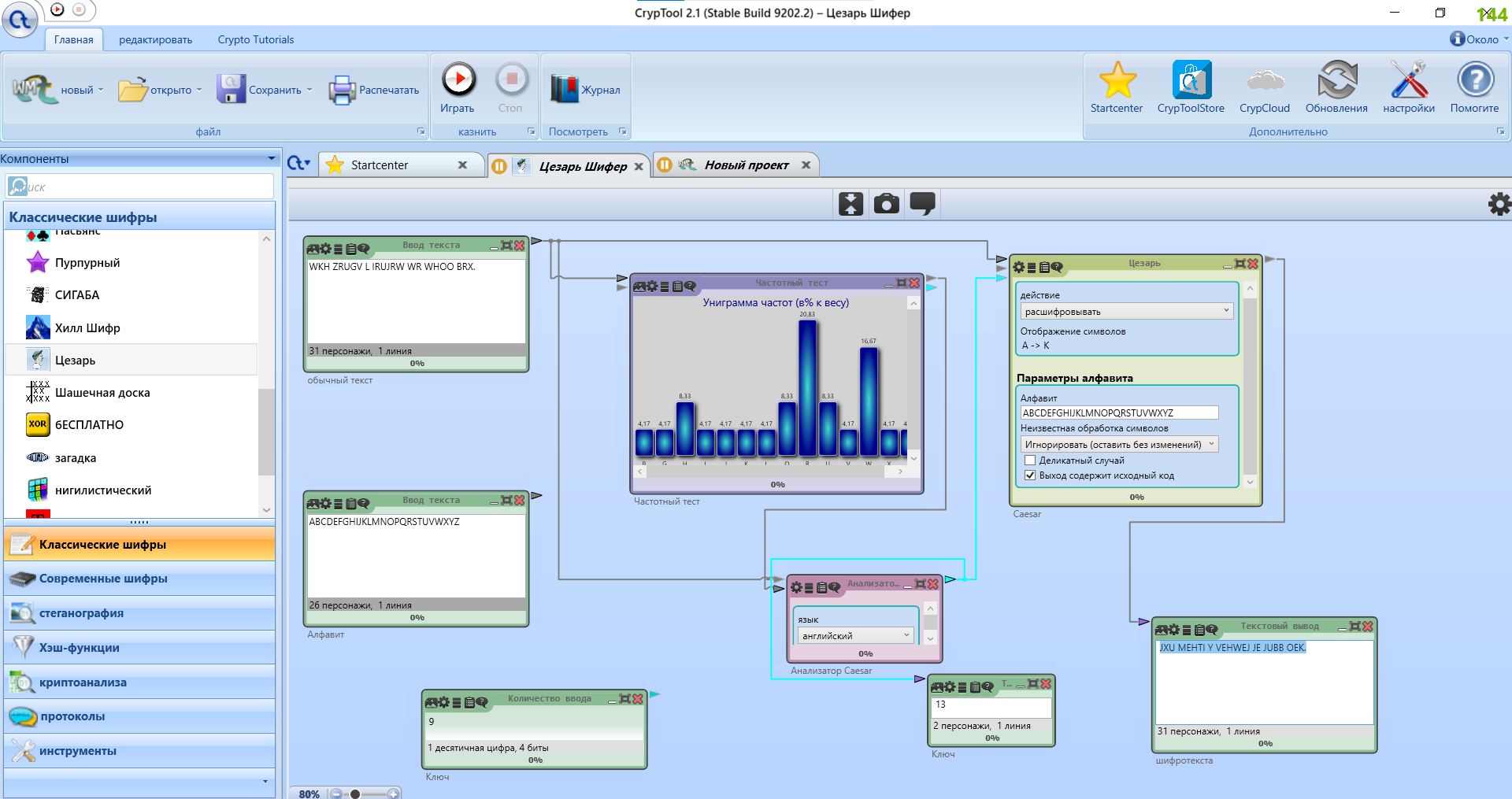


Проанализируем как разные факторы влияют на успешность криптоанализа:

* Длина открытого текста влияет сильно на успех криптоанализа. Так, если взять короткий закрытый текст, то оно неправильно дешифруется. Из этого следует, что чем длиннее закрытый текст, тем выше вероятность успешной его дешифровки.

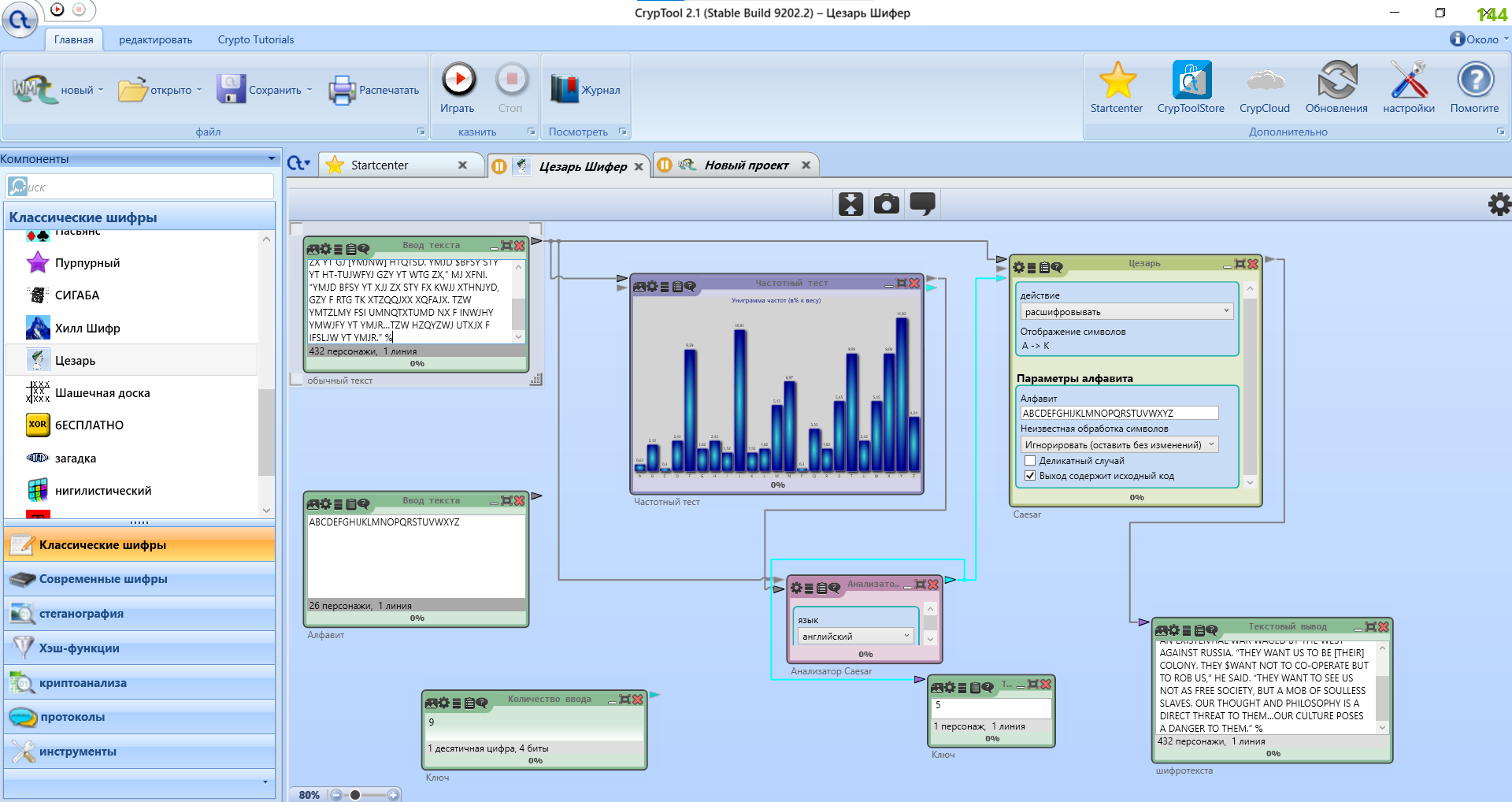
Example

|  |  |  |
| --- | --- | --- |
| Открытый текст с ключом 3 | The words I forgot to tell you. | WKH ZRUGV L IRUJRW WR WHOO BRX. |
| Закрытый текст с использованием частотного анализа | WKH ZRUGV L IRUJRW WR WHOO BRX. | JXU MEHTI Y VEHWEJ JE JUBB OEK. |

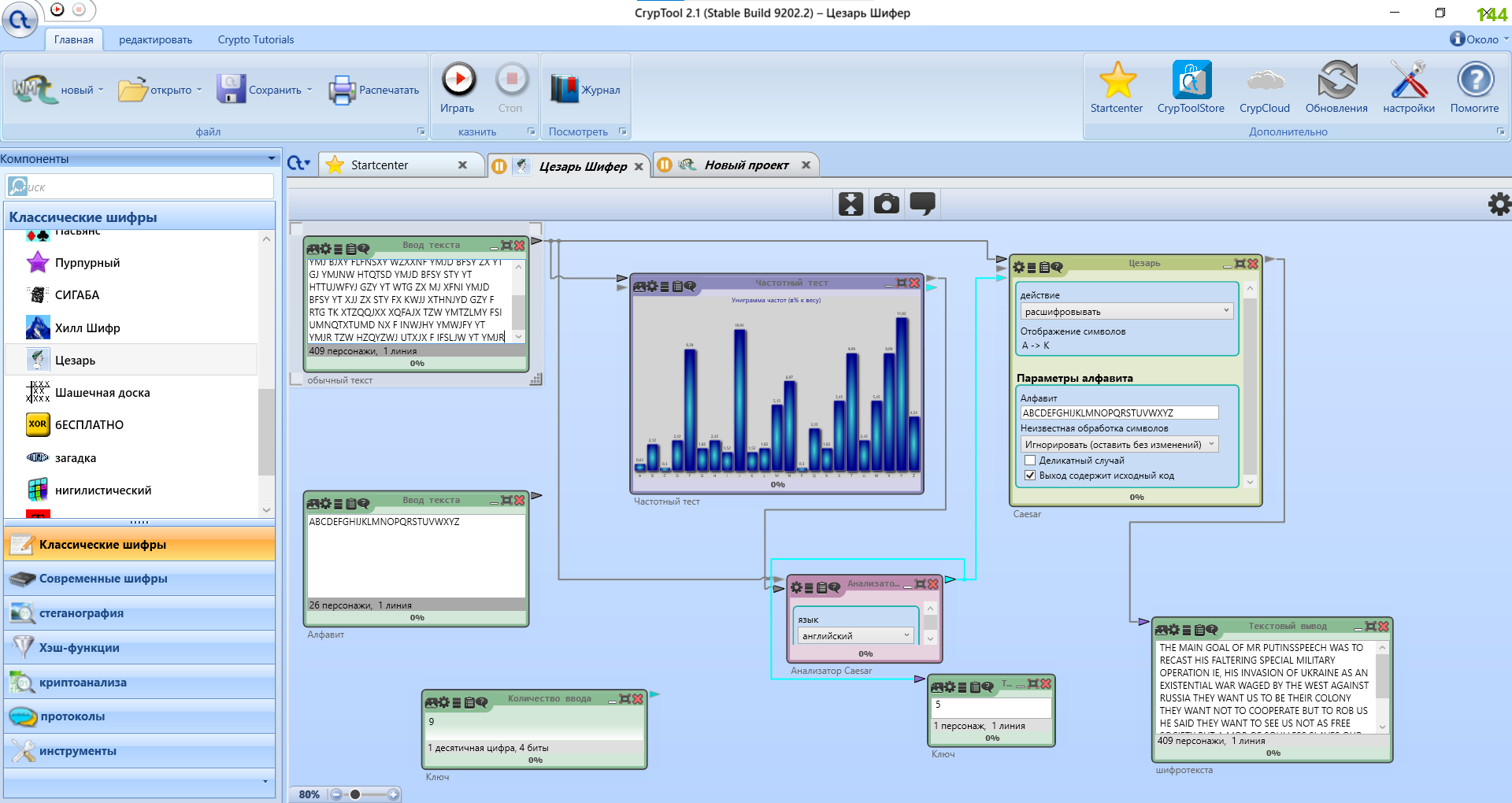


* Посмотрим, как влияет удаление специальных символов и вставок, которые не входят в алфавит шифра.

Example.

Для этого возьмем текст, содержащий кавычки, скобки и от себя добавил еще парочку специальных символов для более показательной проверки. 

Как можно заметить, дешифровка прошла успешно, тем уберем специальные символы.



Дешифровка также прошла успешно. Из этого можно заключить, что специальные символы не влияют на получение успешного расшифрованного текста

* Удаление пробелов между словами.

Example.

Возьмем этот же текст без специальных символов и уберем все пробелы. Изображение выглядит как текст

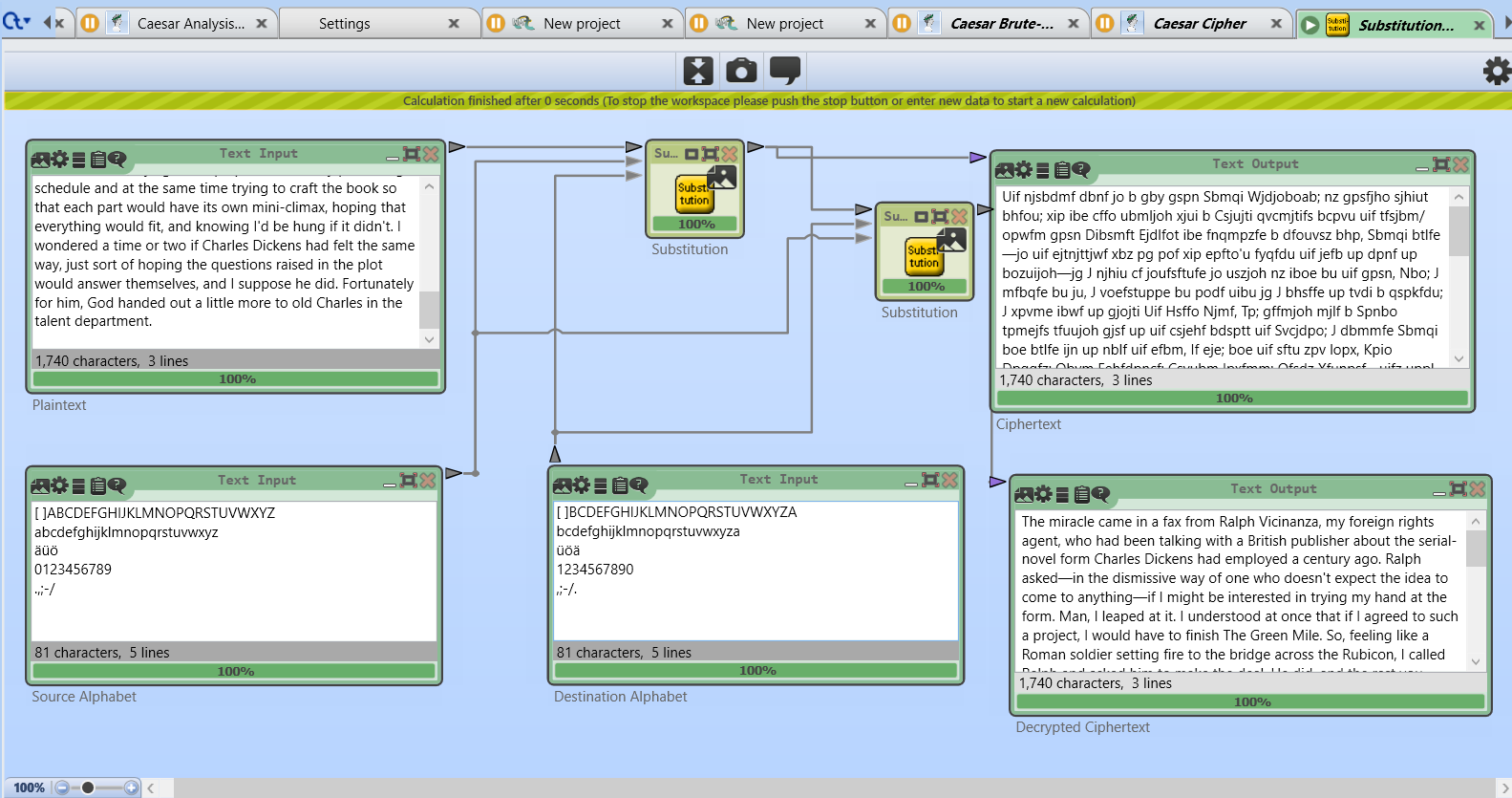
Автоматически созданное описание

Закрытый текст также корректно расшифровывается без символов пробелов.

* 1. Выполним криптоанализ шифра Цезарь, используя шаблон атаки полным перебором

Изображение выглядит как текст

Автоматически созданное описание

1. *Шифр подстановки (Substitution Cipher):*
2. Произведем шифрование и дешифрование открытого текста шифром подстановки. Возьмем в качестве открытого текста отрывок из произведения Стивена Кинга «Зеленая Миля» 
3. Произведем атаку на шифр подстановки Изображение выглядит как текст

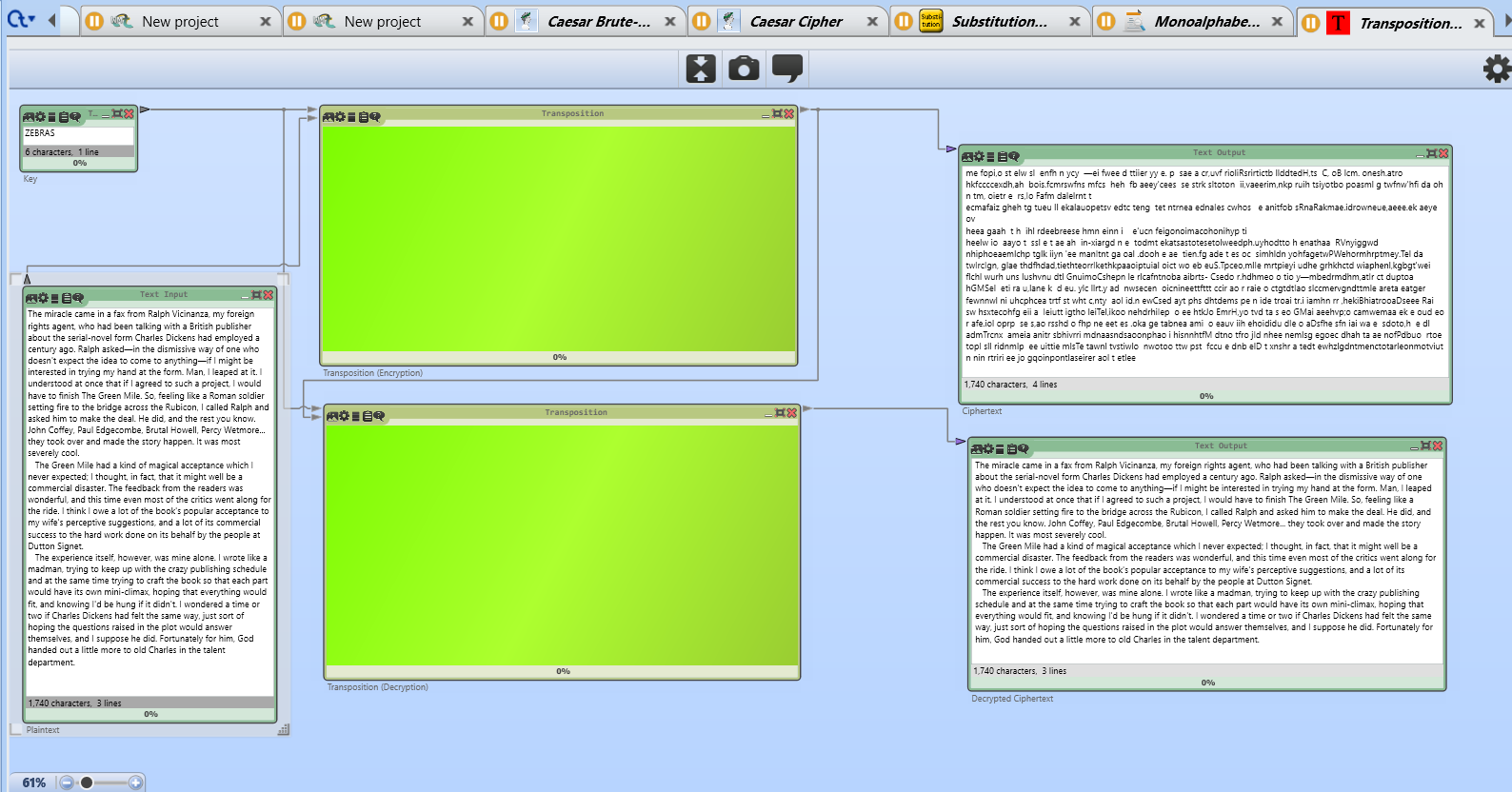
   Автоматически созданное описание
4. Сократим исходный текст

Изображение выглядит как текст

Автоматически созданное описание

Из результатов видно, что для шифра подстановки также важна длина, хоть и часть слов удалось восстановить. Однако, при повторном запуске, ситуация меняется и теперь ни одно слово не было расшифровано, следовательно, и для шифра подстановки длина имеет значение, т.к. две строчки были расшифрованы некорректно.

1. *Перестановачный шифр (Transposition Cipher)*
2. Произведем шифрование и дешифрование открытого текста шифром перестановки. В качестве открытого текста возьмем фрагмент произведения Стивена Кинга «Зеленая миля» с ключом – ZEBRAS



Как видно со снимка экрана шифрование и дешифрование прошло успешно. Хотя следует отметить, что, т.к. был взят относительно большой текст, шифрование и дешифрование происходило довольно долго.

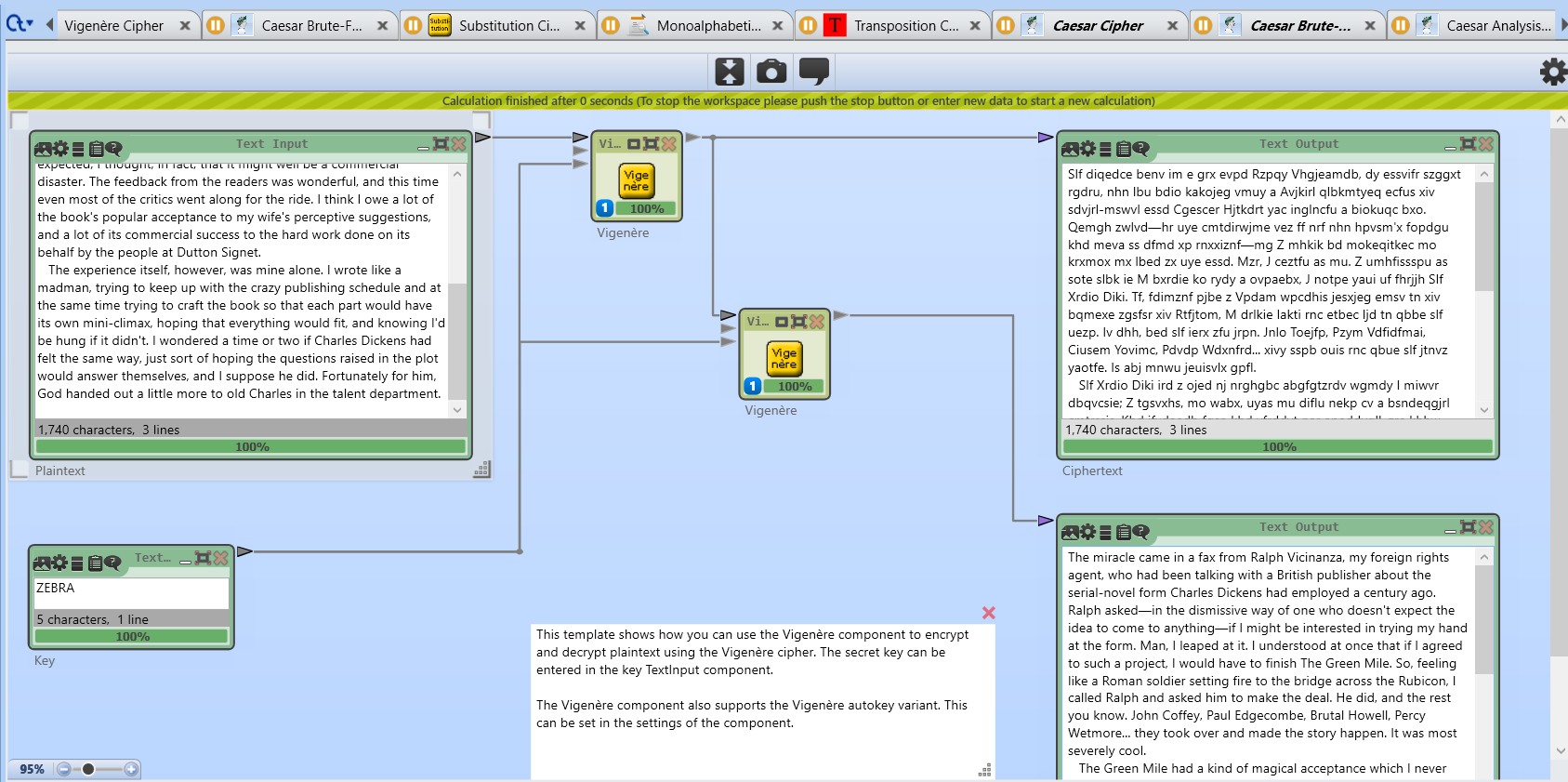
1. Произведем атаку по шаблону Transposition Brute-Force Analysis:

Изображение выглядит как текст

Автоматически созданное описание

Замечаем, что атака провалилась и дешифрование было выполнено некорректно.

1. *Шифр Веженера:*
2. Произведем шифрование и дешифрование открытого текста с помощью шифра Веженера с ключом ZEBRA



1. Произведем атаку на зашифрованный текст с помощью шаблона Vigenere Analysis

Изображение выглядит как текст

Автоматически созданное описание

Атака прошла успешно, хотя следует отметить, что ключ был найден не тот, точнее это был утроенный вариант изначального ключа (ZEBRAZEBRAZEBRA). Теперь сократим исходный текст до двух строчек, чтобы проверить, как влияет длина текста на расшифровку.

Изображение выглядит как текст

Автоматически созданное описание

Как видно из результатов, расшифровка прошла успешно и длина зашифрованного текста практически не влияет, также расшифрованный текст не содержит в себе специальных символов и пробелов. Проверим также влияют ли специальные символы на расшифровку.

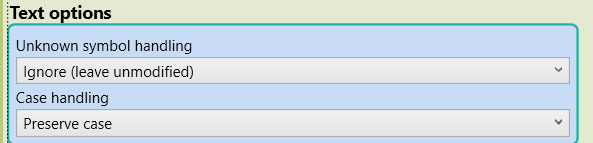
Изображение выглядит как текст

Автоматически созданное описание

На полученный результат не повлияло, но как и в первом случае ключ был подобран не совсем верно.

1. *Шифр Энигма*
2. Зашифруем открытый текст с помощью шаблона Enigma Cipher Machine, используя следующие настройки машины:

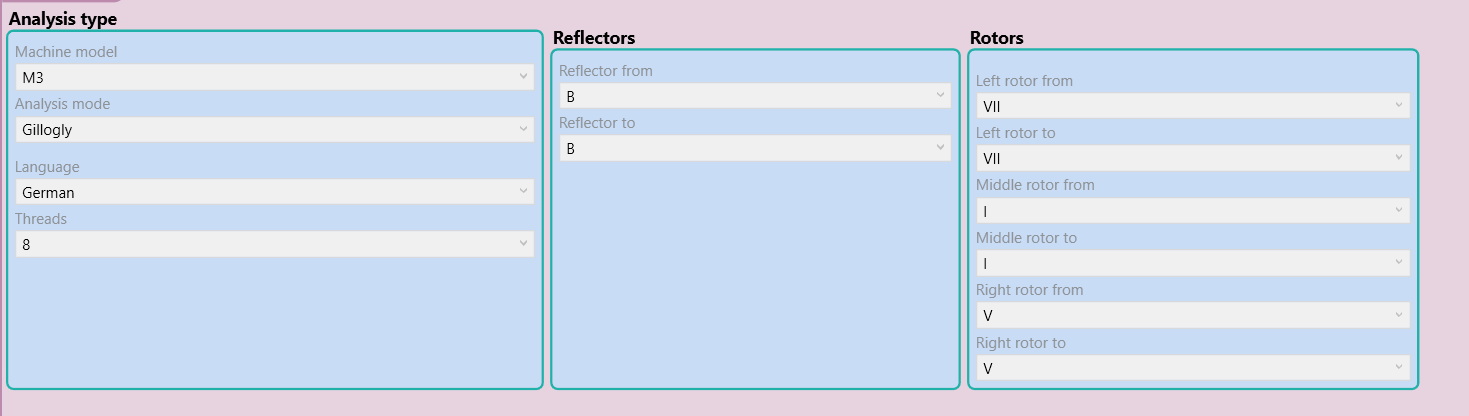
Изображение выглядит как стол

Автоматически созданное описание 

Изображение выглядит как текст

Автоматически созданное описание

1. Дешифруем закрытый текст с помощью шаблона анализатора Enigma Gillogy Analysis. Для ускорения процесса будем использовать следующие настройки.



Изображение выглядит как стол

Автоматически созданное описание

Запустим анализатор Изображение выглядит как текст

Автоматически созданное описание

1. ***Вывод:***

В ходе выполнения данной лабораторной работы, мною было изучено устройство и принципы работы программы CrypTool2. Также было проведено ознакомление с шифрованием и дешифрованием данных и факторы влияющие на исход декодировки. Были изучены механизмы простейшего криптоанализа, моно- полиалфавитные шифры, а также принцип работы роторной машины Энигмы.