Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Криптографические методы обеспечения информационной безопасности»

ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №1

«Анализ исторических шифров с помощью программного средства Cryptool 2»

Выполнил:

Полевцов Артем Сергеевич, студент группы N34511

(подпись)

Проверил:

Волков Александр Григорьевич, инженер ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург
2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель практической работы: с помощью программного средства CrypTool 2 изучить принципы работы исторических шифров, а также провести их криптоанализ.

Задачи практической работы - используя функции программы CrypTool 2, проанализировать следующие криптографические примитивы:

1. Шифр Цезаря, шифры перестановки и замены (как примеры моноалфавитных шифров);
2. Шифр Виженера (как пример полиалфавитного шифра);
3. Структуру и процесс шифрования в роторной машине Энигма

1 АНАЛИЗ ИСТОРИЧЕСКИХ ШИФРОВ С ПОМОЩЬЮ ПРОГРАММНОГО СРЕДСТВА CRYPTOOL

1.1 Ход работы

1.1.1 Шифр Цезаря

1.1.1.1 Процесс шифрования и дешифрования

Установил и запустил CrypTool 2, выбрал Шифр Цезаря:

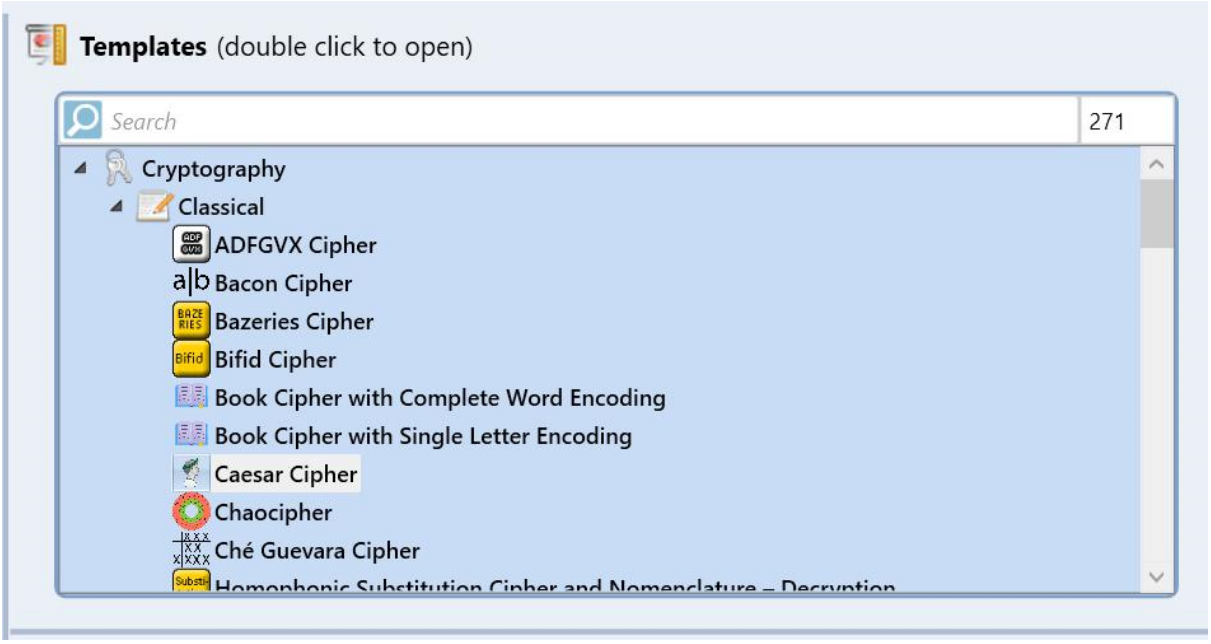

Рисунок 1 - Меню программы

Исходный текст:

Задал в качестве открытого текста:

She leaves me with jelly legs

Where did all my good luck get to

Were curled up like sleeping kittens on the floor

Stowed aboard your big green boat

She took aim with a turned back

Blew holes in me with cold silence

Then a science project volcano erupts inside me

Filling me with flat champagne

Stretched out like a rubber band

From one planet to the next

You were dancing with your grandfather that lonely night

I guess Ill meet you in the afterlife

She leaves me with jelly legs

Where did all my good luck get to

Like a lonely kitten sinking drowning in the harbour

I walked the plank your big green boat

Stretched out like a rubber band

From one planet to the next

You were dancing with your grandfather that lonely night

I guess Ill meet you in the afterlife

Stretched out like a rubber band

From one planet to the next

You were dancing with your grandfather that lonely night

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

Значение криптографического ключа - 11 соответствует одиннадцати сдвигам символов по алфавиту.

Значение алфавита - ABCDEFGHIJKLMNOPQRSTUVWXYZ, то есть все латинские буквы.

Все настройки выглядят следующим образом:

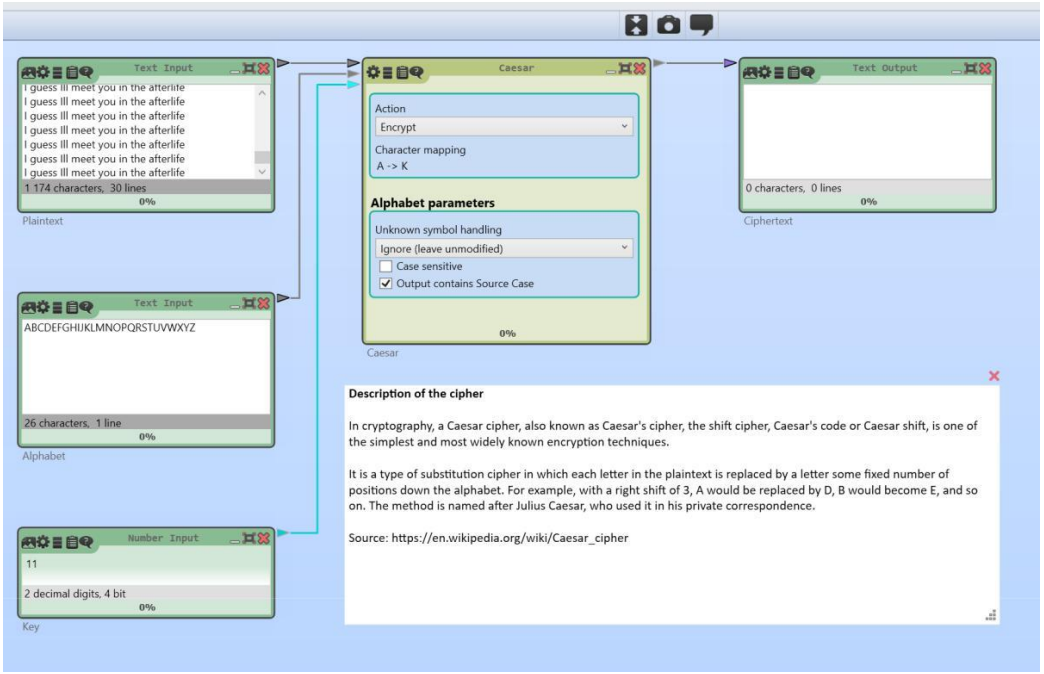

Рисунок 2 - Шифр Цезаря

Запускаем шифрование.

Закрытый текст:

Dsp wplgpd xp htes upwwj wprd

Hspcp oto lww xj rzzo wfnv rpe ez

Hpcp nfcwpo fa wtvp dwppatyr vteepyd zy esp qwzzc

Dezhpo lmzlco jzfc mtr rcppy mzle

Dsp ezzv ltx htes l efcypo mlnv

Mwph szwpd ty xp htes nzwo dtwpynp

Espy l dntpynp aczupne gzwnlyz pcfaed tydtop xp

Qtwwtyr xp htes qwle nslxalryp

Decpenspo zfe wtvp l cfmmpc mlyo

Qczx zyp awlype ez esp ypie

Jzf hpcp olyntyr htes jzfc rclyoqlespc esle wzypwj ytrse

T rfpdd Tww xppe jzf ty esp lqepcwtqp

Dsp wplgpd xp htes upwwj wprd

Hspcp oto lww xj rzzo wfnv rpe ez

Wtvp l wzypwj vteepy dtyvtyr oczhytyr ty esp slcmzfc

T hlwvpo esp awlyv jzfc mtr rcppy mzle

Decpenspo zfe wtvp l cfmmpc mlyo

Qczx zyp awlype ez esp ypie

Jzf hpcp olyntyr htes jzfc rclyoqlespc esle wzypwj ytrse

T rfpdd Tww xppe jzf ty esp lqepcwtqp

Decpenspo zfe wtvp l cfmmpc mlyo

Qczx zyp awlype ez esp ypie

Jzf hpcp olyntyr htes jzfc rclyoqlespc esle wzypwj ytrse

T rfpdd Tww xppe jzf ty esp lqepcwtqp

T rfpdd Tww xppe jzf ty esp lqepcwtqp

T rfpdd Tww xppe jzf ty esp lqepcwtqp

T rfpdd Tww xppe jzf ty esp lqepcwtqp

T rfpdd Tww xppe jzf ty esp lqepcwtqp

T rfpdd Tww xppe jzf ty esp lqepcwtqp

T rfpdd Tww xppe jzf ty esp lqepcwtqp

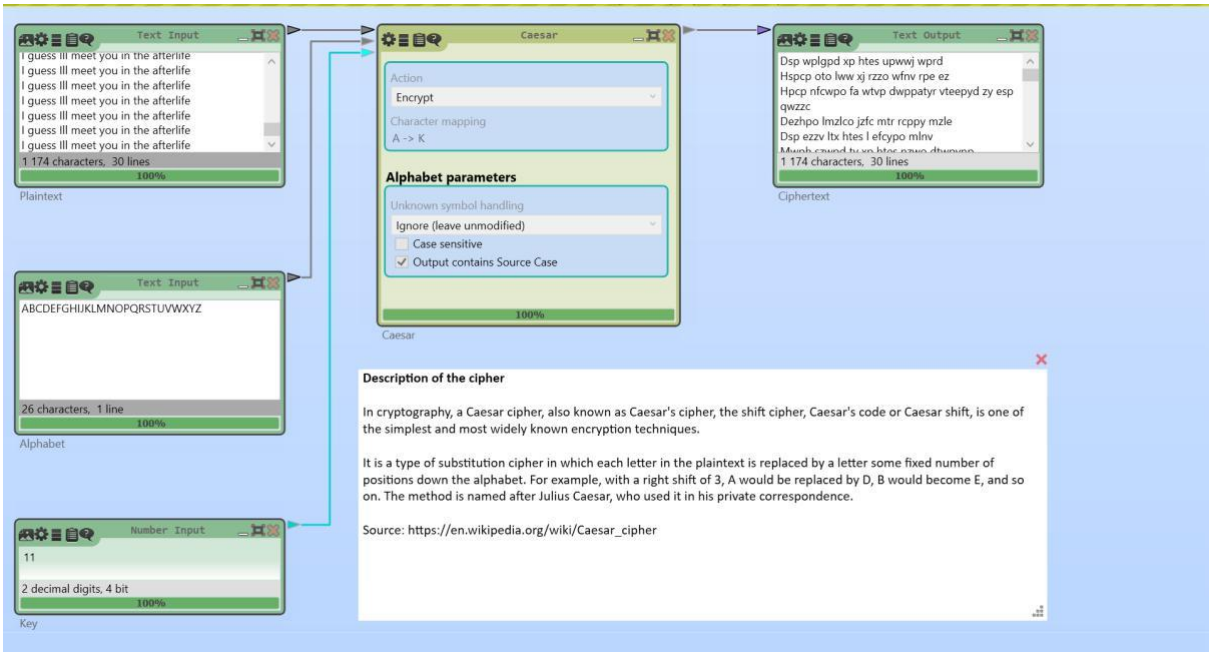

Рисунок 3 - Шифр Цезаря

Далее дешифруем этот текст:

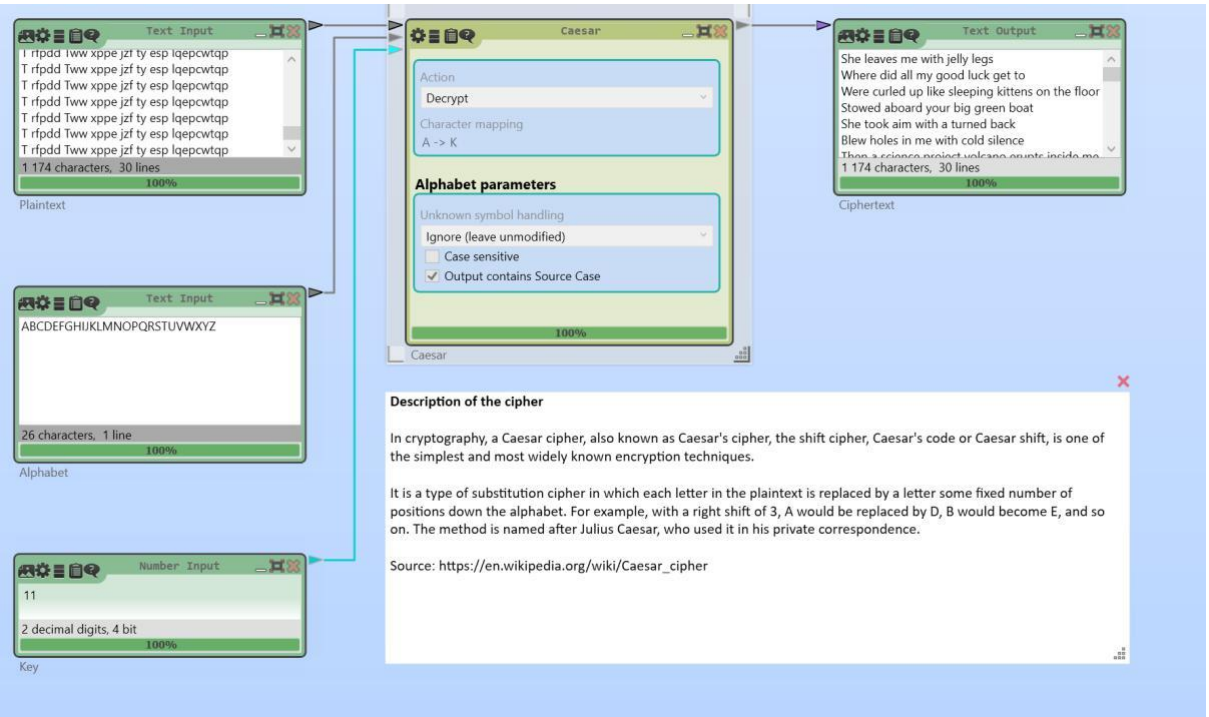

Рисунок 4 - Шифр Цезаря

Получаем полностью корректный изначальный открытый текст:

She leaves me with jelly legs

Where did all my good luck get to

Were curled up like sleeping kittens on the floor

Stowed aboard your big green boat

She took aim with a turned back

Blew holes in me with cold silence

Then a science project volcano erupts inside me

Filling me with flat champagne

Stretched out like a rubber band

From one planet to the next

You were dancing with your grandfather that lonely night

I guess Ill meet you in the afterlife

She leaves me with jelly legs

Where did all my good luck get to

Like a lonely kitten sinking drowning in the harbour

I walked the plank your big green boat

Stretched out like a rubber band

From one planet to the next

You were dancing with your grandfather that lonely night

I guess Ill meet you in the afterlife

Stretched out like a rubber band

From one planet to the next

You were dancing with your grandfather that lonely night

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

I guess Ill meet you in the afterlife

Как мы видим, тот же сдвиг в одиннадцать символов применился в обратную сторону и мы получили текст, что и в самом начале. Сложность атаки на ключ зависит от мощности заданного алфавита, в нашем случае количество вариантов для перебора - 26.

1.1.1.2 Анализ Character Frequencies

Давайте проведем анализ Character Frequencies:

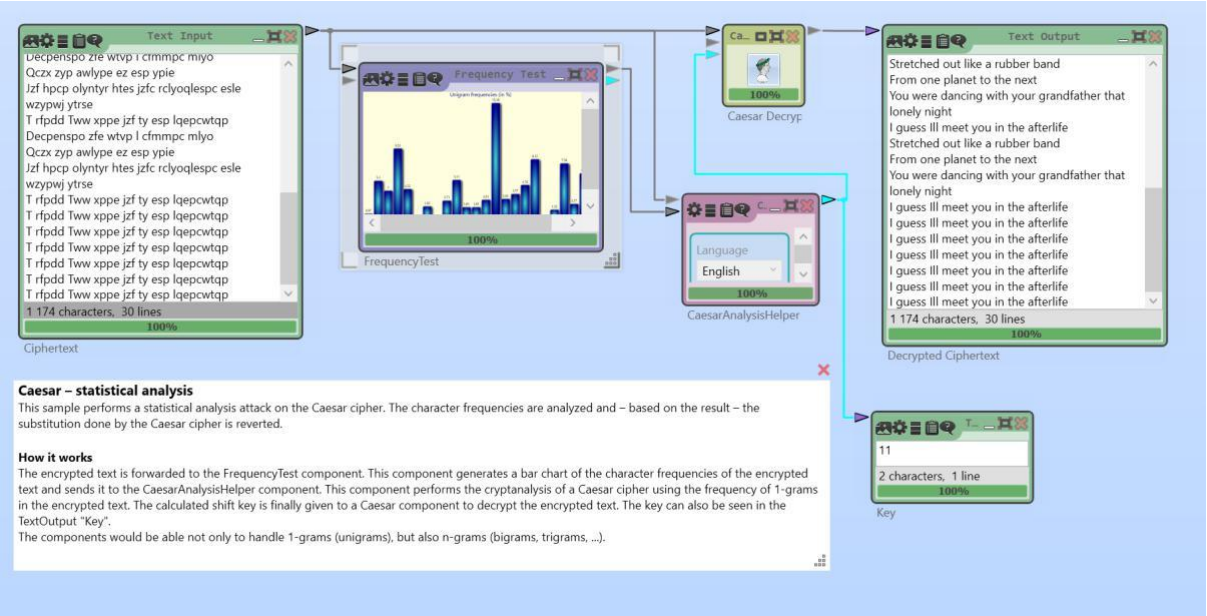

Рисунок 5 - Частотный анализ

Далее попытаемся усложнить задачу и удалим все пробелы и переносы строк из нашего шифротекста:

DspwplgpdxphtesupwwjwprdHspcpotolwwxjrzzowfnvrpeezHpcpnfcwpofawtvpdwpp atyrvteepydzyespqwzzcDezhpolmzlcojzfcmtrrcppymzleDspezzvltxhteslefcypomlnvMwphsz wpdtyxphtesnzwodtwpynpEspyldntpynpaczupnegzwnlyzpcfaedtydtopxpQtwwtyrxphtesqwle nslxalrypDecpenspozfewtvplcfmmpcmlyoQczxzypawlypeezespypieJzfhpcpolyntyrhtesjzfcrcl yoqlespceslewzypwjytrseTrfpddTwwxppejzftyesplqepcwtqpDspwplgpdxphtesupwwjwprdHs pcpotolwwxjrzzowfnvrpeezWtvplwzypwjvteepydtyvtyroczhytyrtyespslcmzfcThlwvpoespawl yvjzfcmtrrcppymzleDecpenspozfewtvplcfmmpcmlyoQczxzypawlypeezespypieJzfhpcpolynty rhtesjzfcrclyoqlespceslewzypwjytrseTrfpddTwwxppejzftyesplqepcwtqpDecpenspozfewtvplcf mmpcmlyoQczxzypawlypeezespypieJzfhpcpolyntyrhtesjzfcrclyoqlespceslewzypwjytrseTrfpd dTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqep cwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppe jzftyesplqepcwtqpTrfpddT wwxppejzftyesplqepcwtqp

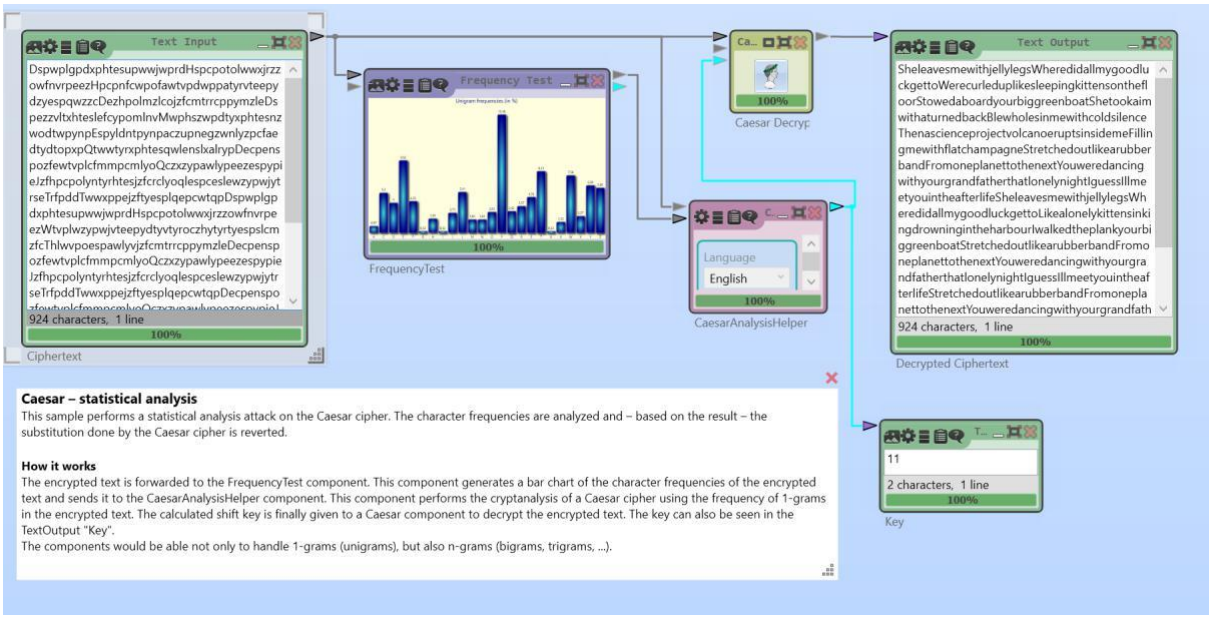

Рисунок 6 - Частотный анализ

И как мы можем увидеть процесс дешифрования опять прошел успешно.

Полный расшифрованный текст:

SheleavesmewithjellylegsWheredidallmygoodluckgettoWerecurleduplikesleepingkitte nsonthefloorStowedaboardyourbiggreenboatShetookaimwithaturnedbackBlewholesinmewith coldsilenceThenascienceprojectvolcanoeruptsinsidemeFillingmewithflatchampagneStretched outlikearubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelyni ghtIguessIllmeetyouintheafterlifeSheleavesmewithjellylegsWheredidallmygoodluckgettoLike alonelykittensinkingdrowningintheharbourIwalkedtheplankyourbiggreenboatStretchedoutlike arubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelynightIgue

ssIllmeetyouintheafterlifeStretchedoutlikearubberbandFromoneplanettothenextYouweredanci
ngwityourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafter
lifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlife
Iguess IllmeetyouintheafterlifeIguessIllmeetyouintheafterlife

Увеличим вдвое количество символов, продублировав исходный текст:

DspwplgpdxphtesupwwjwprdHspcpotolwwxjrzzowfnvrpeezHpcpnfcwpofawtvpdwpp
atyrvteepydzyespqwzzcDezhpolmzlcojzfcmtrrcppymzleDspezzvltxhteslefcypomlnvMwphsz
wpdtyxphtesnzwodtwpynpEspyldntpynpaczupnegzwnlyzpcfaedtydtopxpQtwwtyrxphtesqwle
nslxalrypDecpenspozfewtvplcfmmpcmlyoQczxzypawlypeezespypieJzfhpcpolyntyrhtesjzfcrcl
yoqlespceslewzypwjytrseTrfpddTwwxppejzftyesplqepcwtqpDspwplgpdxphtesupwwjwprdHs
pcpotolwwxjrzzowfnvrpeezWtvplwzypwjvteepydtyvtyroczhytyrtyespslcmzfcThlwvpoespawl
yvjzfcmtrrcppymzleDecpenspozfewtvplcfmmpcmlyoQczxzypawlypeezespypieJzfhpcpolynty
rhtesjzfcrclyoqlespceslewzypwjytrseTrfpddTwwxppejzftyesplqepcwtqpDecpenspozfewtvplcf
mmpcmlyoQczxzypawlypeezespypieJzfhpcpolyntyrhtesjzfcrclyoqlespceslewzypwjytrseTrfpd
dTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqep
cwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppe
jzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpDspwplgpdxphtesupwwjwprdHspcpotol
wwxjrzzowfnvrpeezHpcpnfcwpofawtvpdwppatyrvteepydzyespqwzzcDezhpolmzlcojzfcmtrrc
ppymzleDspezzvltxhteslefcypomlnvMwphszwpdtyxphtesnzwodtwpynpEspyldntpynpaczupne
gzwnlyzpcfaedtydtopxpQtwwtyrxphtesqwlenslxalrypDecpenspozfewtvplcfmmpcmlyoQczxz
ypawlypeezespypieJzfhpcpolyntyrhtesjzfcrclyoqlespceslewzypwjytrseTrfpddTwwxppejzftyes
plqepcwtqpDspwplgpdxphtesupwwjwprdHspcpotolwwxjrzzowfnvrpeezWtvplwzypwjvteepy
dtyvtyroczhytyrtyespslcmzfcThlwvpoespawlyvjzfcmtrrcppymzleDecpenspozfewtvplcfmmpc
mlyoQczxzypawlypeezespypieJzfhpcpolyntyrhtesjzfcrclyoqlespceslewzypwjytrseTrfpddTww
xppejzftyesplqepcwtqpDecpenspozfewtvplcfmmpcmlyoQczxzypawlypeezespypieJzfhpcpoly
ntyrhtesjzfcrclyoqlespceslewzypwjytrseTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejz
ftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpdd
TwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepc
wtqp

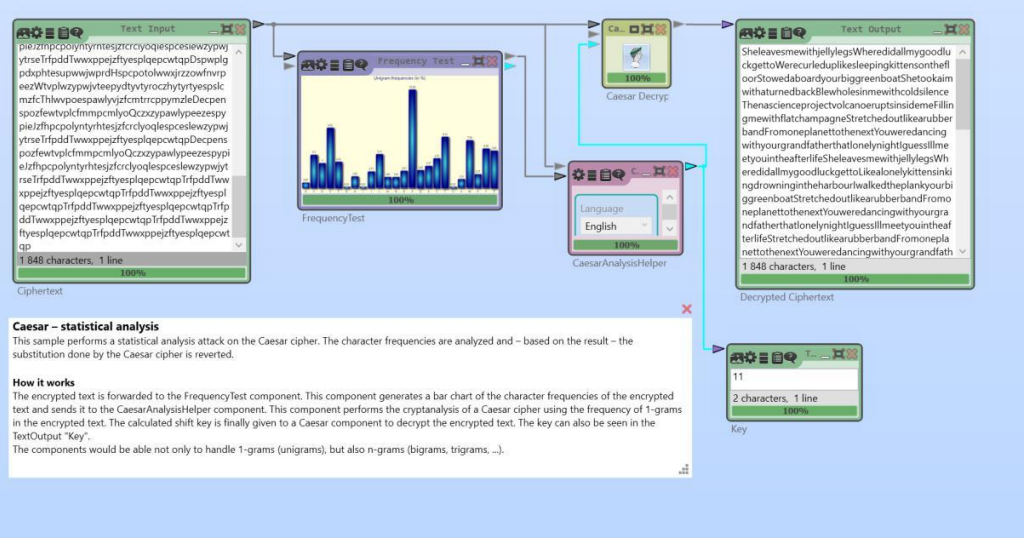

Рисунок 7 - Частотный Анализ

Как мы видим, текст так же успешно был дешифрован:

SheleavesmewithjellylegsWheredidallmygoodluckgettoWerecurleduplikesleepingkittensonthefloorStowedaboardyourbiggreenboatShetookaimwithaturnedbackBlewholesinmewithcoldsilenceThenascienceprojectvolcanoeruptsinsidemeFillingmewithflatchampagneStretchedoutlikearubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeSheleavesmewithjellylegsWheredidallmygoodluckgettoLikealonelykittensinkingdrowningintheharbourIwalkedtheplankyourbiggreenboatStretchedoutlikearubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeStretchedoutlikearubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeSheleavesmewithjellylegsWheredidallmygoodluckgettoWerecurleduplikesleepingkittensonthefloorStowedaboardyourbiggreenboatShetookaimwithaturnedbackBlewholesinmewithcoldsilenceThenascienceprojectvolcanoeruptsinsidemeFillingmewithflatchampagneStretchedoutlikearubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeSheleavesmewithjellylegsWheredidallmygoodluckgettoLikealonelykittensinkingdrowningintheharbourIwalkedtheplankyourbiggreenboatStretchedoutlikearubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeStretchedoutlikearubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIgues

sIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIll
meetyouintheafterlife

1.1.1.3 Атака полным перебором

Проведем брутфорс атаку на шифротекст:

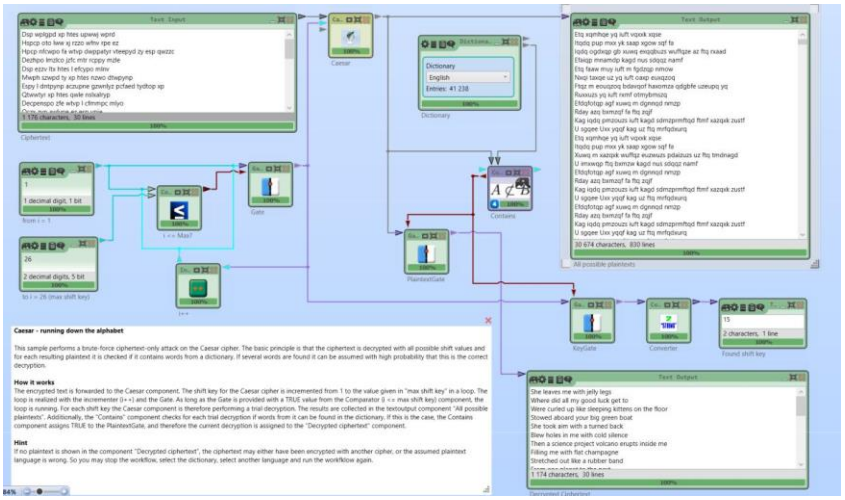

Рисунок 8 - Атака перебором

Как мы видим, путем полного перебора чуть более за длительный промежуток времени мы получаем исходный текст.

1.1.2 Перестановочный шифр

1.1.2.1 Процесс шифрования и дешифрования

Используем тот же открытый текст

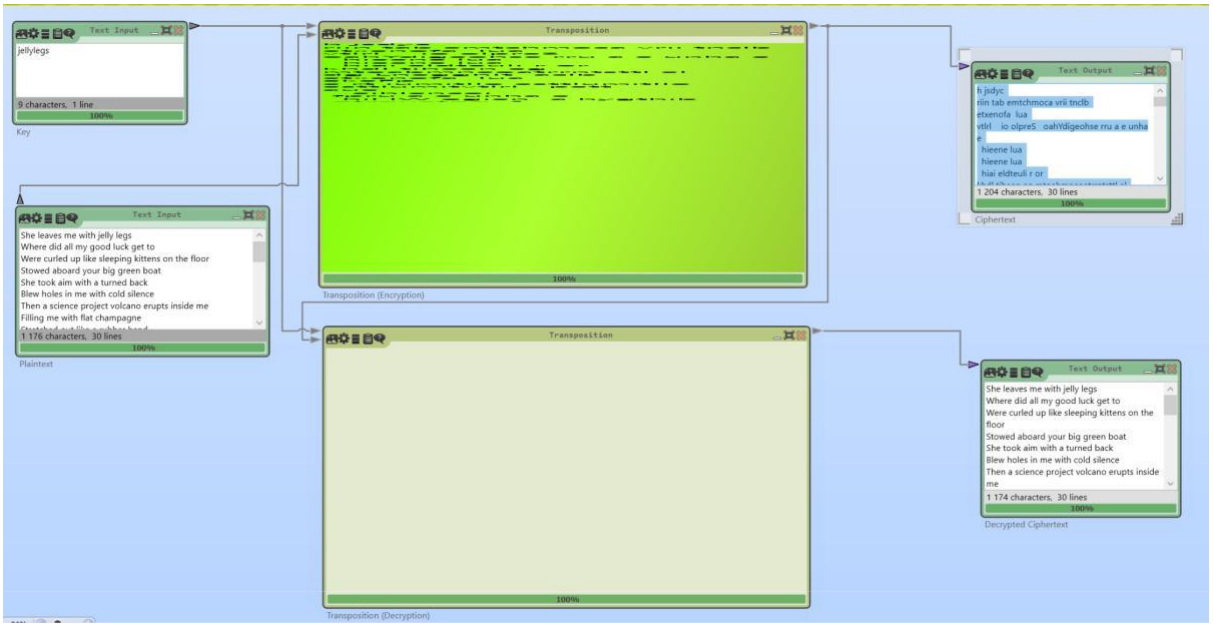

Рисунок 9 - Шифр перестановки

Тут же алгоритм дает нам расшифрованное сообщение, которое полностью сходится с открытым текстом.

Шифротекст выглядит так:

h jsdyc

riin tab emtchmoca vrii tnclb

etxenofa lua

vtlrl io olpreS oahYdigeohse rru a e unha e hieene lua

hieene lua

hiai eldteuli r or

khdl tiheen eg mtoabmneoatrrntsttl el

dg LnegghIt aclb

etxenofa lua

ekeFp

e rt iumitIlo esttlumitIlo esttlumitvtlrl pett

aue

eihlencoi

fpru a e unha e

hil lW ogien a hygthib

otrguatng f

derrlt

w hlgeene lua

hieene lua

hieeneSs g muoulpeeSo nhi a cn e esFeagt udn ewiydhyIlo eai eldteysrnba ue derrlt

w hlgeenetoabmneoatrrntsttlumitIlo esttlumitIlo esttleme

i k

lknsforib ukoele poudlw ehib

otrguatng f

ehee ltaknwtukl ntoabmneoatrrntsttletrnotn c ntl

Iyefse rg f

Iyefse rg f

Iyef el

dg Weeg lwdgotwr

l d srlpelic ekeFp

e rt iumitSs g muo iknhreab ru a e unha e

hit udn ewiydhyIlo esttlumitIlo esttlumitIlo eewyhaoer sknodygtoteBsisTijasmnhaS oahYdigeohse reme

i k otnn

kgot udn ewiydhyIlo ehib otrguatng f

Iyefse rg f Iyefse rg f ehee ltc eth breSaabwn enct n mlaetrnotn c ntl Iyefewyhaoekl dirweor ekeFp

e rt iumitS oahYdigeohse rg f Iyefse rg f

Iyefse rl lW oged ooe aoin ew

coct ith derrlt

w hlgeeneh jsdyc ltiie dnibetrnotn c ntl Iyefclb etxenofa lua hieene lua hieene lua

Данный шифр составляет матрицу с количеством столбцов соответствующих количеству символов в кодовом слове. Далее нумерует буквы в кодовом слове по их алфавитному порядку, затем сортирует столбцы по соответствующим номерам и перемешивает открытый текст.

1.1.2.2 Атака полным перебором

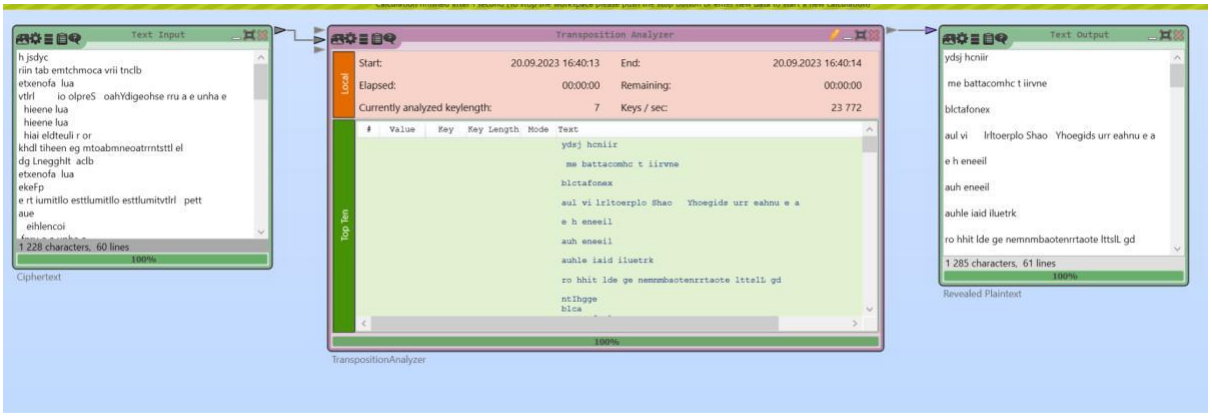

Рисунок 10 - Атака перебором

Видим, что не удается это сделать

1.1.2.3 Generic Analysis

Рисунок 11 - Гибридный анализ

Как видим, здесь тоже не получается дешифровать текст.

1.1.3 Substitution Cipher

1.1.3.1 Процесс шифрования и дешифрования

Открытый текст тот же, все остальное по умолчанию

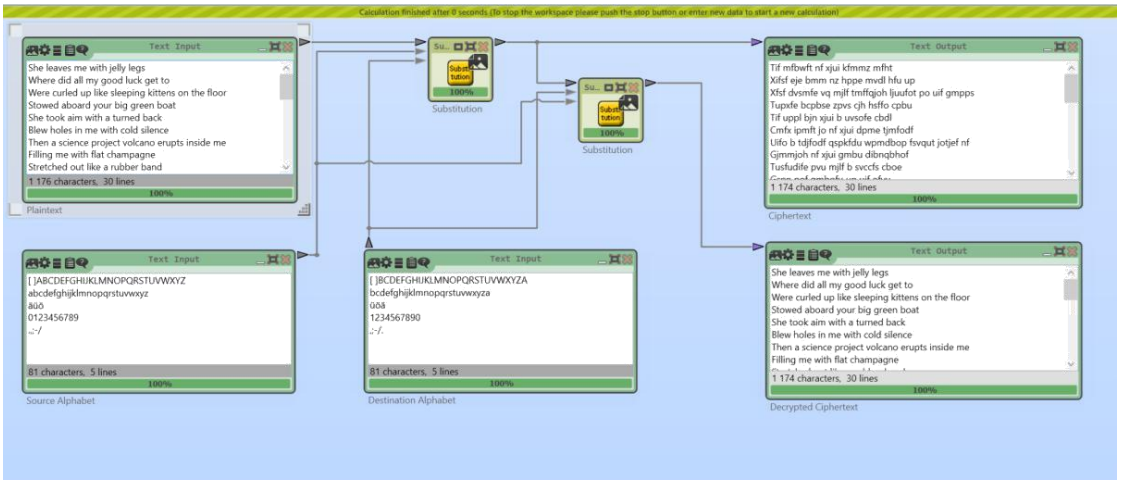

Рисунок 12 - Шифр замены

Шифротекст:

Tif mfbwft nf xjui kfmmz mfht

Xifsf eje bmm nz hppe mvdl hfu up

Xfsf dvsmfe vq mjlf tmffqjoh ljuufot po uif gmpps

Tupxfe bcpbse zpvs cjh hsffo cpbu

Tif uppl bjn xjui b uvsofe cbdl

Cmfx ipmft jo nf xjui dpme tjmfodf

Uifo b tdjfodf qspkfdu wpmdbop fsvqut jotjef nf

Gjmmjoh nf xjui gmbu dibnqbhof

Tusfudife pvu mjlf b svccfs cboe

Gspn pof qmbofu up uif ofyu

Zpv xfsf ebodjoh xjui zpvs hsboegbuifs uibu mpofmz ojhiu

J hvftt Jmm nffu zpv jo uif bgufsmjgf

Tif mfbwft nf xjui kfmmz mfht

Xifsf eje bmm nz hppe mvdl hfu up

Mjlf b mpofmz ljuufo tjoljoh espxojoh jo uif ibscpvs

J xbmlfe uif qmbol zpvs cjh hsffo cpbu

Tusfudife pvu mjlf b svccfs cboe

Gspn pof qmbofu up uif ofyu

Zpv xfsf ebodjoh xjui zpvs hsboegbuifs uibu mpofmz ojhiu

J hvftt Jmm nffu zpv jo uif bgufsmjgf

Tusfudife pvu mjlf b svccfs cboe

Gspn pof qmbofu up uif ofyu

Zpv xfsf ebodjoh xjui zpvs hsboegbuifs uibu mpofmz ojhiu

J hvftt Jmm nffu zpv jo uif bgufsmjgf

J hvftt Jmm nffu zpv jo uif bgufsmjgf

J hvftt Jmm nffu zpv jo uif bgufsmjgf

J hvftt Jmm nffu zpv jo uif bgufsmjgf

J hvftt Jmm nffu zpv jo uif bgufsmjgf

J hvftt Jmm nffu zpv jo uif bgufsmjgf

J hvftt Jmm nffu zpv jo uif bgufsmjgf

Данный алгоритм сразу же предлагает расшифрованный на основе ключа текст, который полностью соответствует изначальному.

Проведем криптоанализ:

1.1.3.2 Monoalphabetic Substitution Analyzer

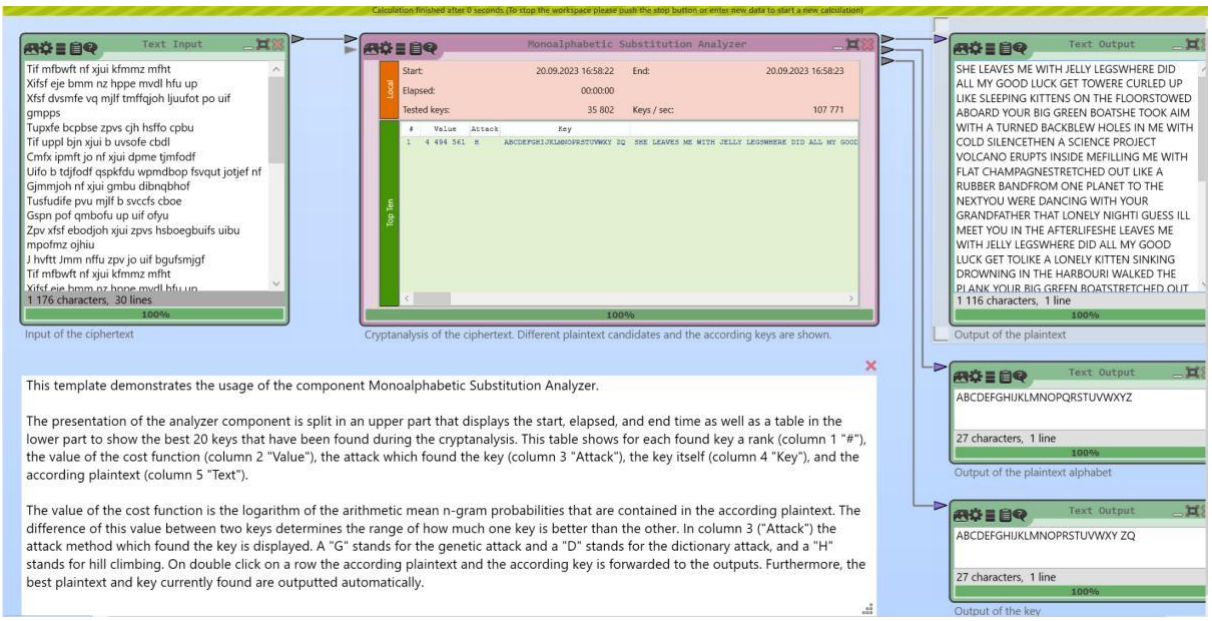

Рисунок 13 - Криптоанализ алгоритма

Как мы видим, текст успешно расшифрован.

1.1.4 Шифр Виженера

1.1.4.1 Процесс шифрования и дешифрования

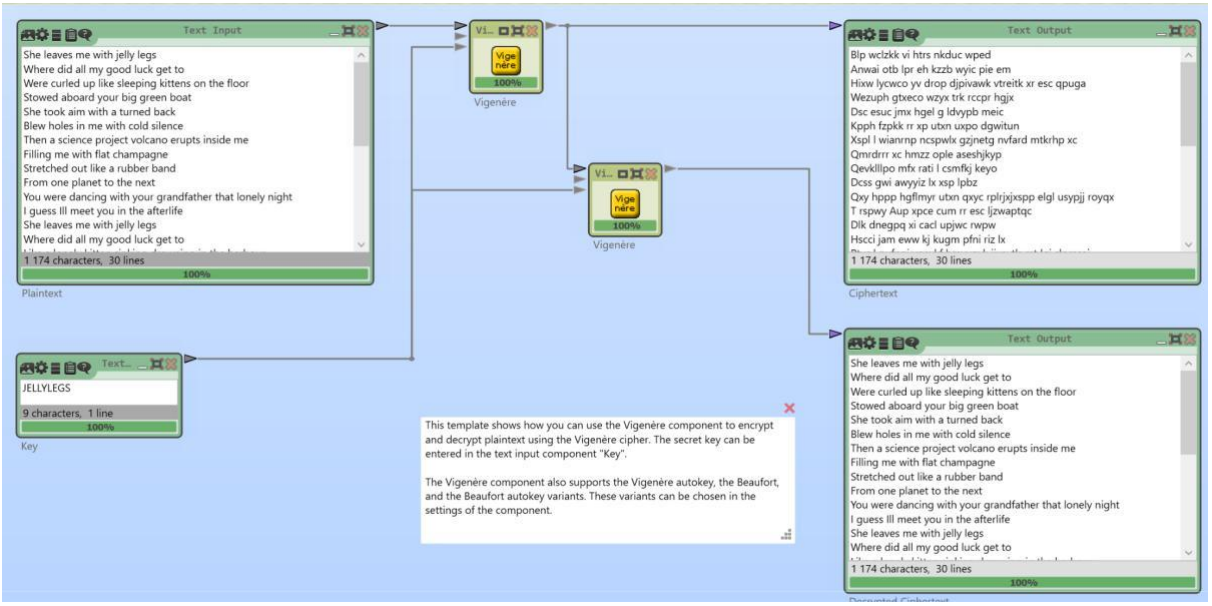

Рисунок 14 - Шифр Виженера

На вход подали текст уже знакомой нам музыкальной композиции, на выходе получили шифротекст:

Blp wclzkk vi htrs nkduc wped

Anwai otb lpr eh kzzb wyic pie em

Hixw lycwco yv drop djpivawk vtreitk xr esc qpuga

Wezuph gtxeco wzyx trk rccpr hgjx

Dsc esuc jmx hgel g ldvypb meic

Kpph fzpkk rr xp utxn uxpo dgwitun

Xspl l wianrnp ncspwlx gzjnetg nvfard mtkrhp xc

Qmrdrrr xc hmzz ople aseshjkyp

Qevkllpo mfx rati l csmfkj keyo

Dcss gwi awyyiz lx xsp lpbz

Qxy hppp hgflmyr utxn qxyc rplrjxjxspp elgl usypjj royqx

T rspwy Aup xpce cum rr esc ljzwaptqc

Dlk dnegpq xi cacl upjwc rwpw

Hscci jam eww kj kugm pfni riz lx

Ptvc l pufnpj vgexkf bmyvgyk jjxaytlr mt lqi slpmsaj

R alwiph zzn twllv cuma ftr ecikf ksle

Qevkllpo mfx rati l csmfkj keyo

Dcss gwi awyyiz lx xsp lpbz

Qxy hppp hgflmyr utxn qxyc rplrjxjxspp elgl usypjj royqx

T rspwy Aup xpce cum rr esc ljzwaptqc

Dxxwcgspb zyz drop l pffhwa flyb

Qvue xrp ajlrkl cs esc yidl

Hsf hcci jswgtye hmzz hsfc ecetvoeescc xnsc pzycwc taple

T efiyk Rpw xcpx egd my efp ellnvwtdp

M mmnwd Tjw qkwc czf gy xnw jjeppwmlw

R kfpqd Mrd vipe wzy of clp ldeixdrjp

T efiyk Rpw xcpx egd my efp ellnvwtdp

M mmnwd Tjw qkwc czf gy xnw jjeppwmlw

R kfpqd Mrd vipe wzy of clp ldeixdrjp

T efiyk Rpw xcpx egd my efp ellnvwtdp

Также среда CrypTool 2 сразу же предоставляет расшифрованный текст, который соответствует заданному вначале.

Пространство ключей для данного шифра сильно зависит от количества символов ключа, например в нашем случае ключ - JELLYLEG состоит из 8 позиций, а в латинском алфавите 26 букв, значит, пространство ключей: 26^8. Для повышения безопасности можно увеличить длину ключа.

1.1.4.2 Атака перебором

Произвести атаку с помощью перебора уже значительно сложнее, чем в случае с Шифром Цезаря, так как мы уже имеем гораздо большее количество вариантов перебора ключа, напомню, что в нашем случае это значение равняется 26^8, что в итоге равняется 208 827 064 576.Воспользуемся встроенным инструментом Vigenère Analysi:

Рисунок 15 - Анализ Виженера

Как мы можем заметить, процесс взлома шифра происходил 17 секунд, что значительно дольше, чем подбор шифра Цезаря, который был скомпрометирован за доли секунды.

Еще следует заметить, что текст был расшифрован корректно, но немного в другом формате - все символы были переведены в верхний регистр и удалены все переносы строк и пробелы.

Давайте посмотрим, что произойдет, если мы в зашифрованном тексте уберем пробелы и переносы:

Рисунок 16 - Анализ Виженера

Как мы можем заметить, алгоритм дешифровки справился с задачей примерно за то же время.

Расшифрованный исходный текст:

SHELEAVESMEWITHJELLYLEGSWHEREDIDALLMYGOODLUCKGETTOWE
RECURLEDUPLIKESLEEPINGKITTENSONTHEFLOORSTOWEDABOARDYOURBIG
GREENBOATSHETOOKAIMWITHATURNEDBACKBLEWHOLESINMEWITHCOLDSI
LENCETHENASCIENCEPROJECTVOLCANOERUPTSINSIDEMEFILLINGMEWITHFL
ATCHAMPAGNESTRETCHEDOUTLIKEARUBBERBANDFROMONEPLANETTOTHE
NEXTYOUWEREDANCINGWITHYOURGRANDFATHERTHATLONELYNIGHTIGUE
SSILLMEETYOUINTHEAFTERLIFESHELEAVESMEWITHJELLYLEGSWHEREDIDA
LLMYGOODLUCKGETTOLIKEALONELYKITTENSINKINGDROWNINGINTHEHAR
BOURIWALKEDTHEPLANKYOURBIGGREENBOATSTRETCHEDOUTLIKEARUBBE
RBANDFROMONEPLANETTOTHENEXTYOUWEREDANCINGWITHYOURGRANDF
ATHERTHATLONELYNIGHTIGUESSILLMEETYOUINTHEAFTERLIFESTRETCHED
OUTLIKEARUBBERBANDFROMONEPLANETTOTHENEXTYOUWEREDANCINGWI
THYOURGRANDFATHERTHATLONELYNIGHTIGUESSILLMEETYOUINTHEAFTER
LIFEIGUESSILLMEETYOUINTHEAFTERLIFEIGUESSILLMEETYOUINTHEAFTERLI
FEIGUESSILLMEETYOUINTHEAFTERLIFEIGUESSILLMEETYOUINTHEAFTERLIFE
IGUESSILL MEETYOUINTHEAFTERLIFEIGUESSILLMEETYOUINTHEAFTERLIFE

1.1.5 Шифр Энигма

1.1.5.1 Процесс шифрования и дешифрования

Оставим настройки машины по умолчанию:

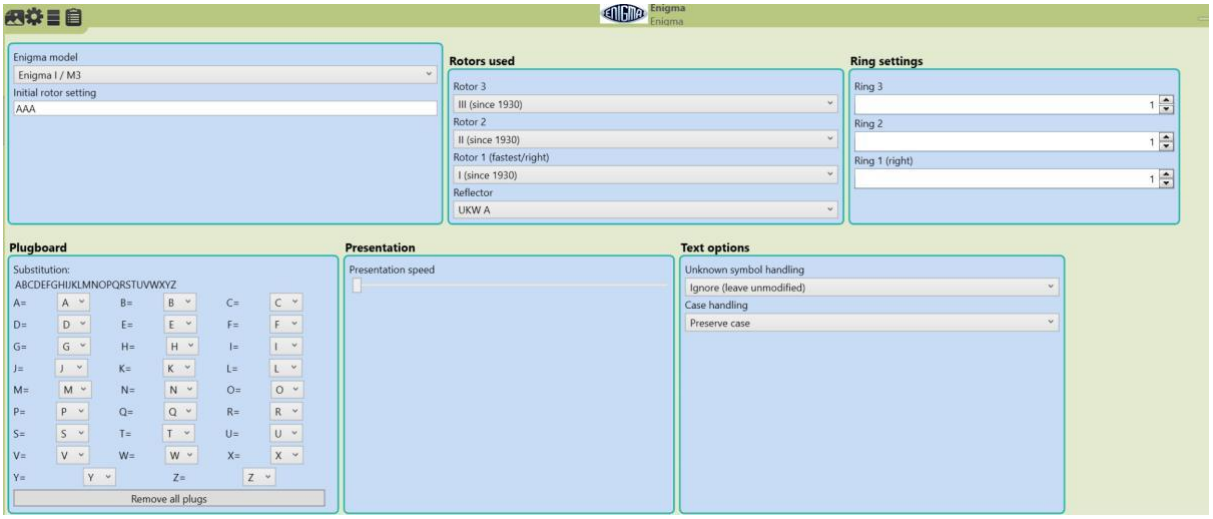

Рисунок 17 - Шифр Энигма

Используем все тот же открытый текст:

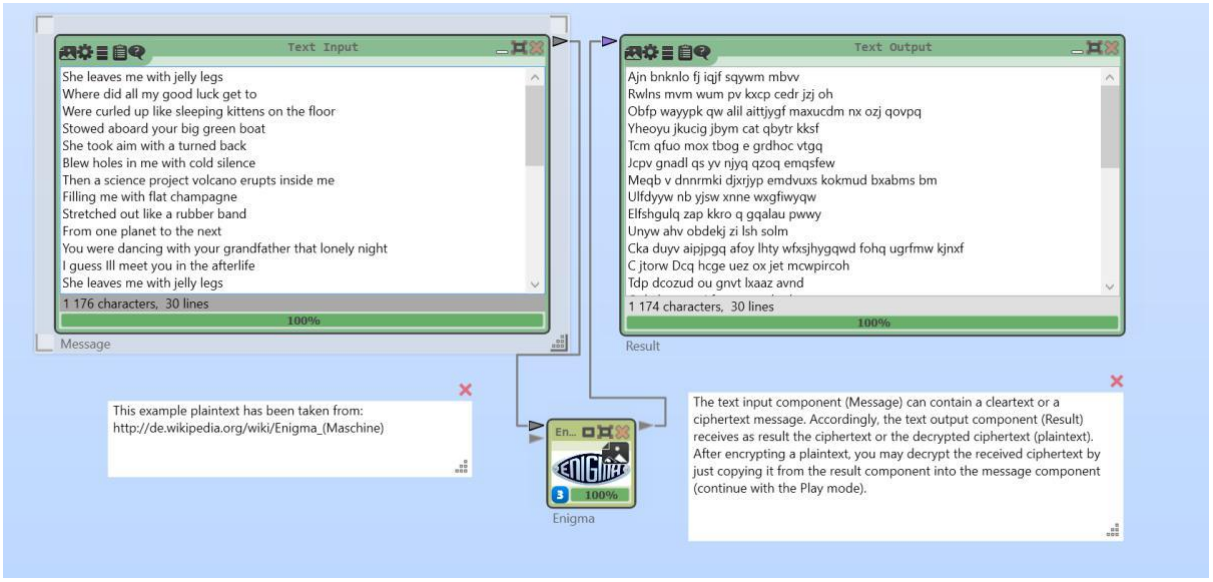

Рисунок 18 - Шифрование

Получаем шифротекст:

Ajn bnknlo fj iqjf sqywm mbvv

Rwlns mvm wum pv kxcp cedr jzj oh

Obfp wayypk qw alil aittjygf maxucdm nx ozj qovpq

Yheoyu jkucig jbym cat qbytr kksf

Tcm qfuo mox tbog e grdhoc vtgq

Jcpv gnadl qs yv njyq qzoq emqsfew

Meqb v dnnrmki djxrjyp emdvuxs kokmud bxabms bm

Ulfdyyw nb yjsw xnne wxgfiwyqw

Elfshgulq zap kkro q gqalau pwwy

Unyw ahv obdekj zi lsh solm

Cka duyv aipjpgq afoy lhty wfxsjhygqwd fohq ugrfmw kjnxf

C jtorw Dcq hcge uez ox jet mcwpircoh

Tdp dcozud ou gnvt lxaaz avnd

Qehxb use yvi fn nzwr pphu krg pv

Mpov j xhbpbz rrcjbg brcsgrr fefkrfjp hx vrt fnyeacz

P hurmrp qdw jacai fzfh sei ofrxe iexl

Oxprifgau rnm yudt j tppdtw scav

Nefu xud xooiun je gkl rlfi

Vnz oidv zbrhphy komz cctc yhdwvssnnic urss jmcbkc mbfgq

L hwygq Xrp aunm vgf hg wjb ivqzzevxf

Cbamltiva ugl kvuv x eisvcs qncp

Pfex bkn cqxrwv gt dmu bosf

Zaa nwtr zhgdwzk bggf lizc izbulqmsxij gysz yrdkyu lcvta

A mfghm Znk orxs zgj rs daz rkwfdyfbk

C fwcja Loz gfqz avn pq hpv lgxklypuk

W bjuut Jfi pgsd gls dg ikc mtqosmyzo

G wrbqu Xhk nikv hrp zb lkb vxzjknnzu

D souuy Znt qraj fxy zp ljn lcppqkgqc

T adxou Sby sdhj oxv pz smh mawwxywtk

K flqvl Jjm yxzj llf ag zfo lxbnxqnsu

Машина Энигма состоит из пяти роторов, три из которых выбираются для шифрования 5*4*3 = 60 вариантов, в каждом из которых по 26 позиций - 26^3 = 17576. Итого получаем 5*4*3*26^3 = 1 054 560 возможных комбинаций. Также существует дополнительная мера безопасности - коммутаторы, запутывающие буквы по парам: 26!/(6!10!2^10) = 150 738 274 937 250 вариантов.

Итого вместе мы получаем 158 962 555 217 826 360 000 возможных настроек данной машины.

1.1.5.2 Enigma gillogly attack

Рисунок 19 - Gillogly Attack

Видно, что алгоритм не справился с задачей и в результате вывел неправильный текст.

Хотя шифротекст из примера алгоритм дешифрует успешно:

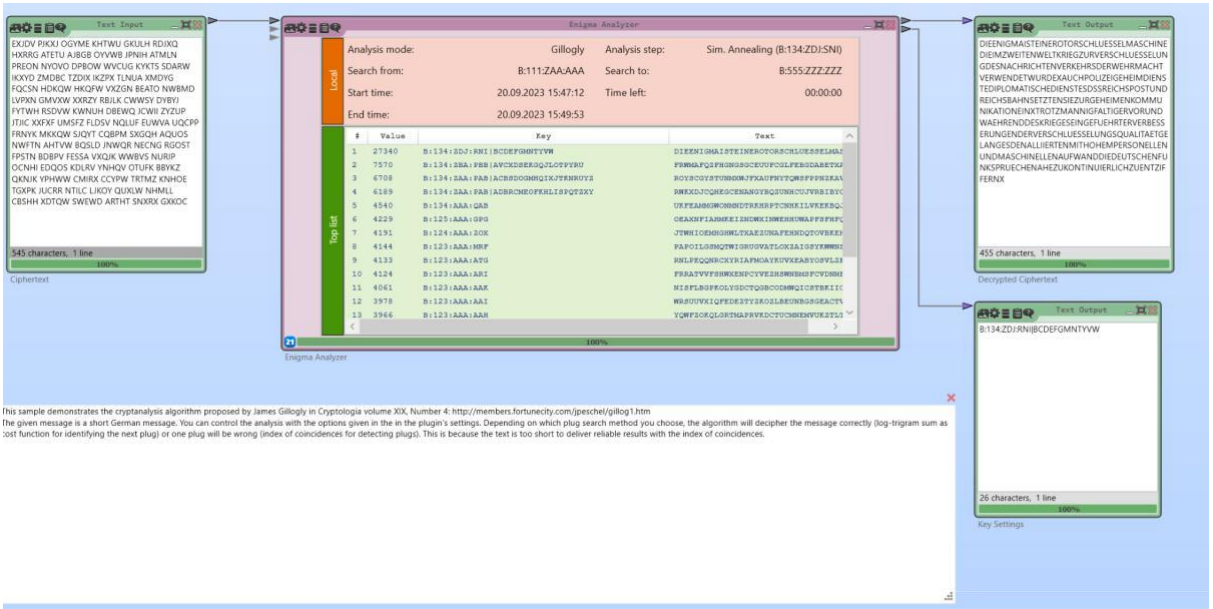

Рисунок 20 - Gillogly Attack

1.1.5.3 Hill-climbing attack

Рисунок 21 - Hill-Climbing Attack

Открытый текст получить не удается.

ЗАКЛЮЧЕНИЕ

В ходе данной лабораторной работы были рассмотрены основные наивные криптографические алгоритмы, был зашифрован открытый текст с помощью ключей, далее было декодирование шифротекста. Был проведен криптоанализ с попыткой взломать каждый из алгоритмов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. - 376 с.

2. Бабенко, Л.К. Современные интеллектуальные пластиковые карты / Л.К. Бабенко. - М.: Гелиос АРВ, 2015. - 921 с.

3. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. - М.: КомКнига, 2012. - 306 с.

4. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. - М.: Горячая линия - Телеком, 2016. - 186 с.