

**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)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 АНАЛИЗ ИСТОРИЧЕСКИХ ШИФРОВ С ПОМОЩЬЮ ПРОГРАММНОГО СРЕДСТВА CRYPTOOL	4
1.1 Ход работы	4
1.1.1 Шифр Цезаря.....	4
1.1.2 Перестановочный шифр	14
1.1.3 Substitution Cipher	17
1.1.4 Шифр Виженера.....	19
1.1.5 Шифр Энигма.....	23
ЗАКЛЮЧЕНИЕ.....	27
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	28

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 CRYPTOTOOL

1.1 Ход работы

1.1.1 Шифр Цезаря

1.1.1.1 Процесс шифрования и дешифрования

Установил и запустил СrypTool 2, выбрал Шифр Цезаря:

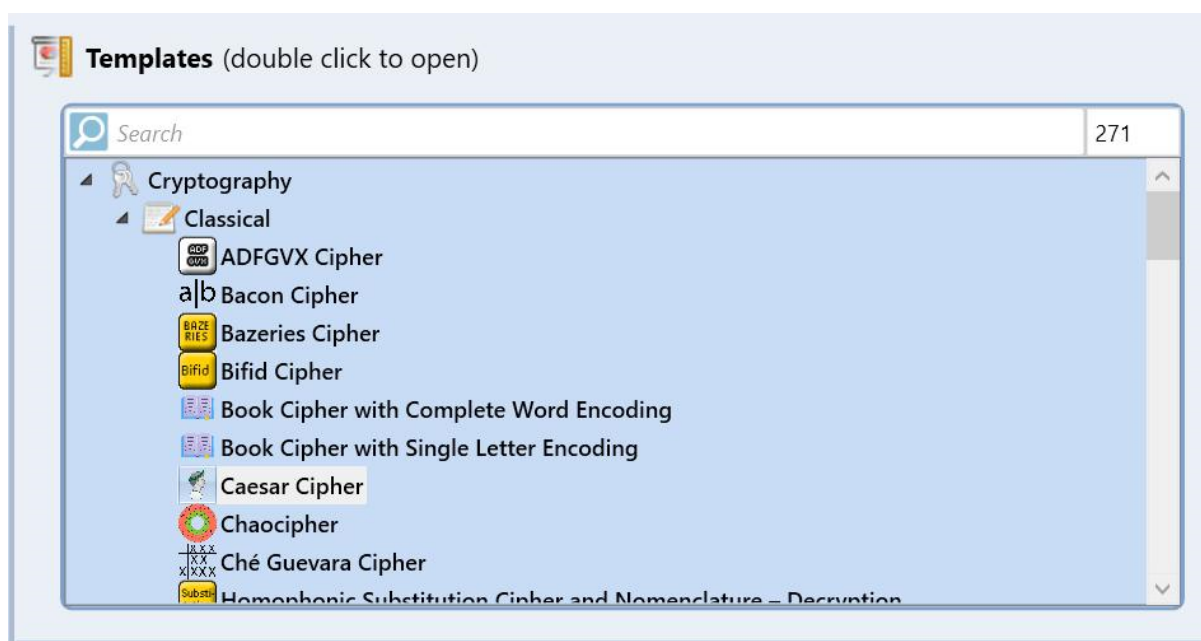


Рисунок 1 - Меню программы

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:

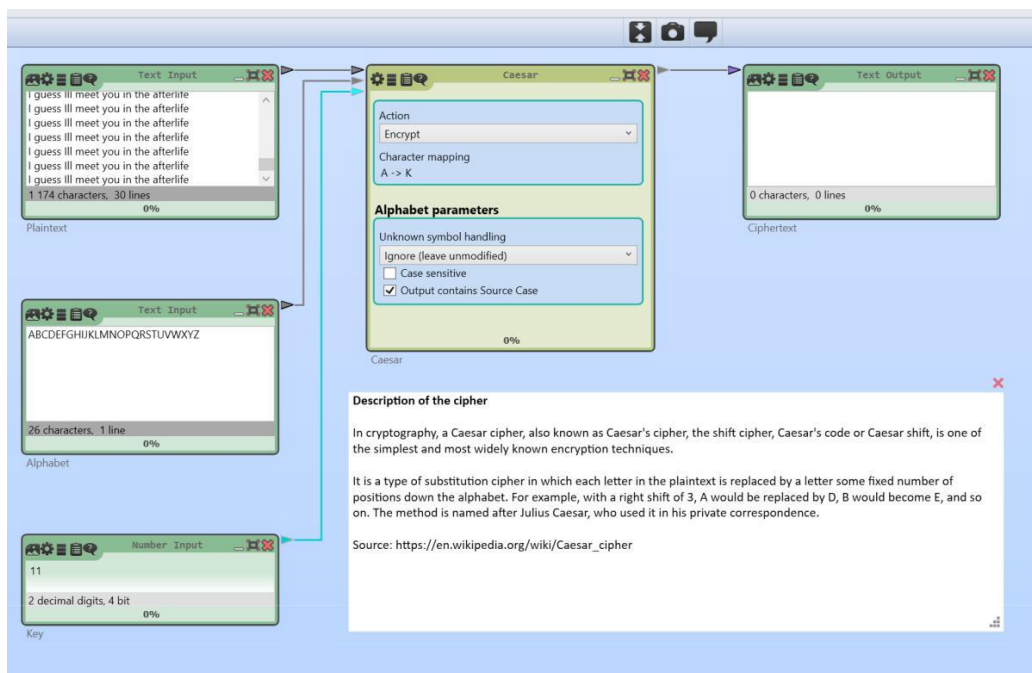


Рисунок 2 - Шифр Цезаря

Запускаем шифрование.

ЗакрЫтый текст:

Dsp wplgpd xp htes upwwj wprd

Hspcp oto lww xj rzzo wfnv rpe ez

Hpcp nfcwpo fa wtpv dwppatyr vteepyd zy esp qwzzc

Dezhpo lmzlco jzfc mtr rcppy mzle

Dsp ezzv ltx htes l efcypo mlnv

Mwph szwpgd ty xp htes nzwo dtwpynp

Espy l dntpynp aczupne gzwnlyz pcfaed tydtop xp

Qtwwtыр xp htes qwle nslxalryp

Decpenspo zfe wtpv l cfmmmpc mlyo

Qczx zyp awlype ez esp ypie

Jzf hpcp olyntыр htes jzfc rclyoqllespc esle wzyppwj ytrse

T rfpdd Tww xppe jzf ty esp lqepcwtqp

Dsp wplgpd xp htes upwwj wprd

Hspcp oto lww xj rzzo wfnv rpe ez

Wtpv l wzyppwj vteepy dtyvтыr oczhyтыr ty esp slcmzfc

T hlwpvpo esp awlyv jzfc mtr rcppy mzle

Decpenspo zfe wtpv l cfmmmpc mlyo

Qczx zyp awlype ez esp ypie

Jzf hpcp olyntyr htes jzfc rclyoqlespc esle wzyppwj ytrse

T rfpdd Tww xppe jzf ty esp lqepcwtqp

Decpenspo zfe wtvplcfmmpcmlyo

Qczx zyp awlype ez esp ypie

Jzf hpcp olyntyr htes jzfc rclyoqlespc esle wzyppwj 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

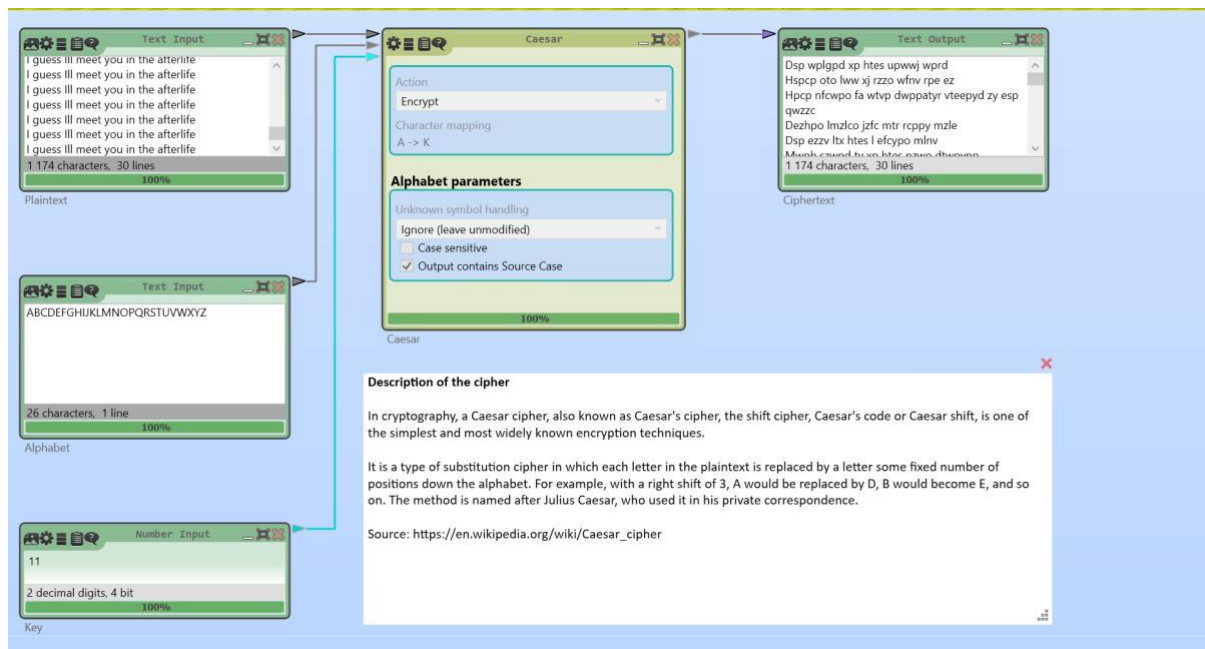


Рисунок 3 - Шифр Цезаря

Далее дешифруем этот текст:

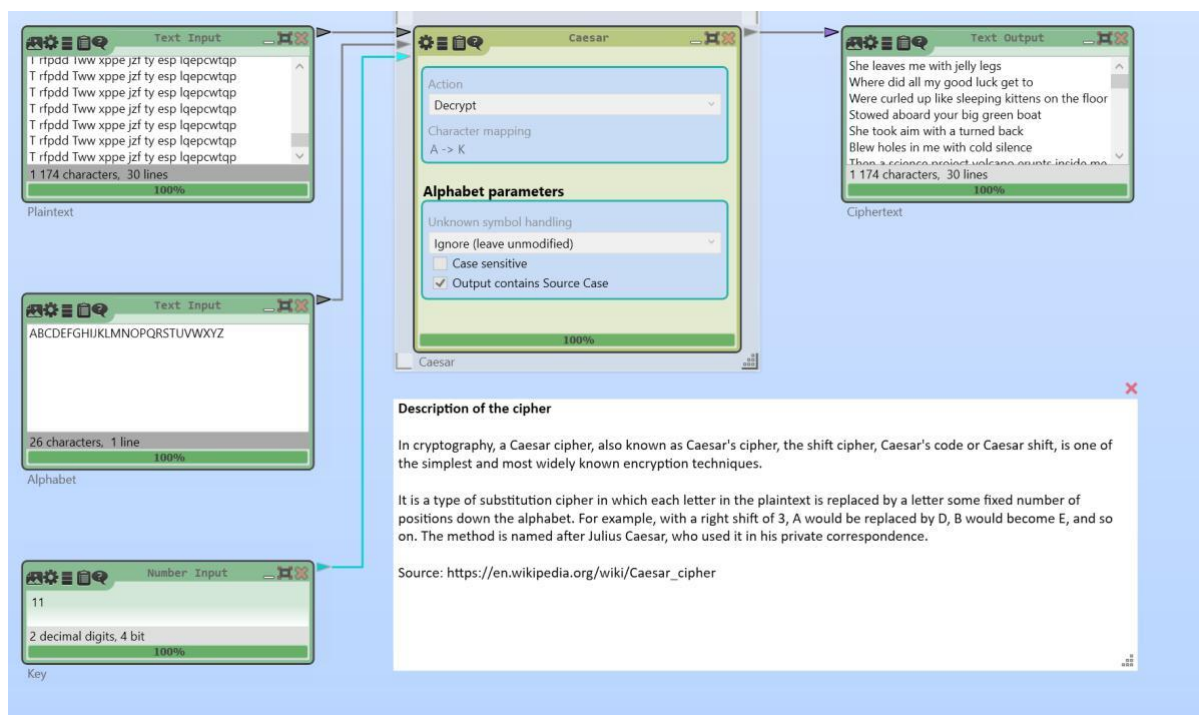


Рисунок 4 - Шифр Цезаря

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:

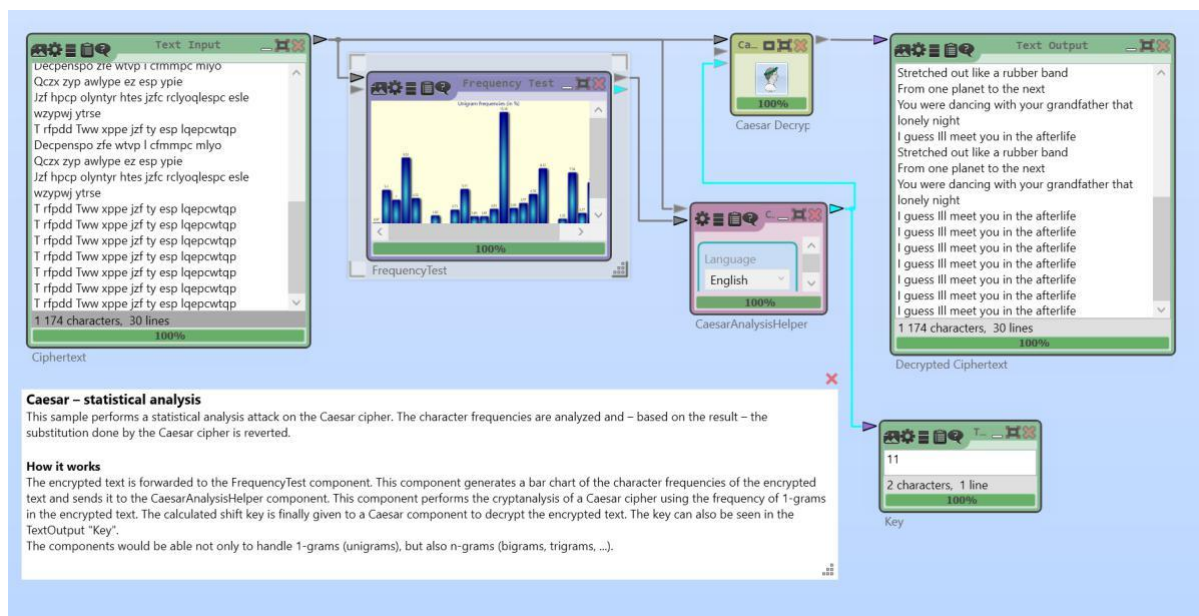


Рисунок 5 - Частотный анализ

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

DspwplgdphtesupwwjwprdHspcpotolwwxjrzzowfnvrpeezHpcpnfcwpofawtvpdwwp
 atyrvttepydyzespqwzzcDezhpolmzlcojzfcmttrccpymzleDspezzvltxhteslefcpomlnvMwphsz
 wpdtyxhtesnzwodtwpynpEspyldntpynpaczupnegzwnlyzpcfaedydtopxpQtwwtvrxphtesqwe
 nslxalrypDecpenspozfewtvplcfmmpcmlyoQczxypawlypeezesypieJzfhpccpolyntyrtesjzfcrl
 yoqlespceslewzywpjytrseTrfpddTwwxppejzftyesplqepcwtqpDspwplgdphtesupwwjwprdHs
 pcpotolwwxjrzzowfnvrpeezWtvplwzywpjvteepydytyvtyroczhytyrtespslcmzfcThlwvpoespawl
 yvjzfcmttrccpymzleDecpenspozfewtvplcfmmpcmlyoQczxypawlypeezesypieJzfhpccpolynty
 rhtesjzfcrlcyoqlespceslewzywpjytrseTrfpddTwwxppejzftyesplqepcwtqpDecpenspozfewtvplcf
 mmpcmlyoQczxypawlypeezesypieJzfhpccpolyntyrtesjzfcrlcyoqlespceslewzywpjytrseTrfpd
 dTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqep
 cwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppe
 jzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqp

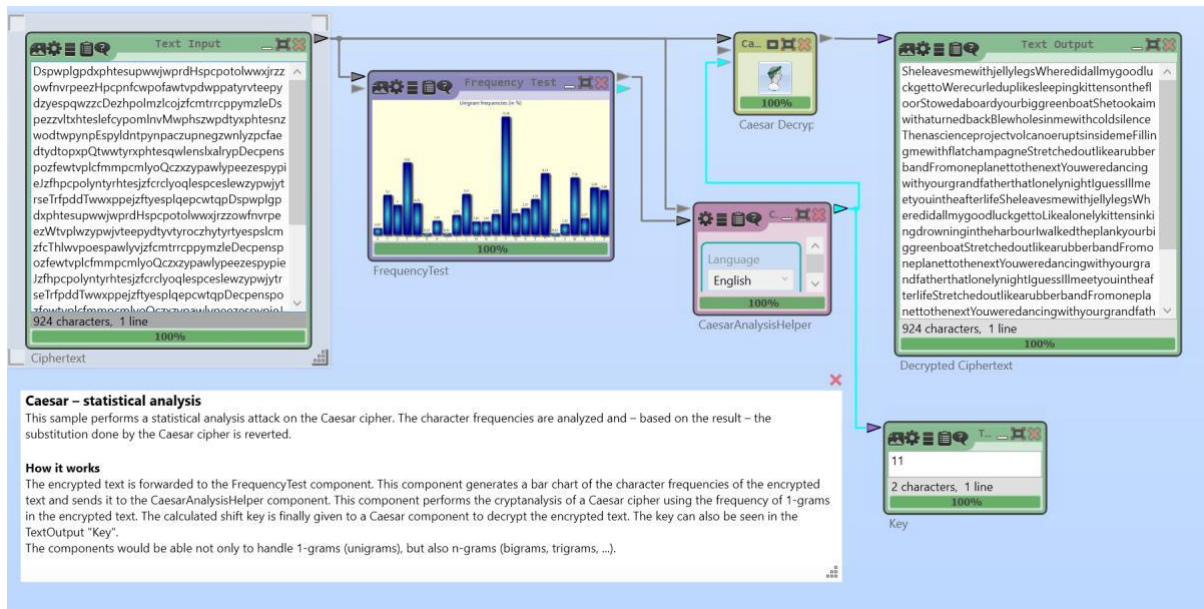


Рисунок 6 - Частотный анализ

И как мы можем увидеть процесс дешифрования опять прошел успешно.

Полный расшифрованный текст:

SheleavesmewithjellylegsWheredidallmygoodluckgettoWerecurleduplikesleepingkitte
 nsonthefloorStowedaboardyourbiggreenboatShetookaimwithaturnedbackBlewholesinmewith
 coldsilenceThenascienceprojectvolcanoeruptsinsidemeFillingmewithflatchampagneStretched
 outlikearubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelyni
 ghtIguessIllmeetyouintheafterlifeSheleavesmewithjellylegsWheredidallmygoodluckgettoLike
 alonelykittensinkingdrowningintheharbourIwalkedtheplankyoubiggreenboatStretchedoutlike
 arubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelynightIgue

ssIllmeetyouintheafterlifeStretchedoutlikearubberbandFromoneplanettothenextYouweredanci
ngwityourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafter
lifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlife
Iguess IllmeetyouintheafterlifeIguessIllmeetyouintheafterlife

Увеличим вдвое количество символов, продублировав исходный текст:

DspwplgdpdxphtesupwwjwprdHspcpotolwwxjrzzowfnvrpeezHpcpnfcwpofawtvpdwpp
atyrvtteepdydespqwzzcDezhpolmzlcojzfcmttrcpymzleDspezzvltxhteslefcpomlnvMwphsz
wpdtyxphtesnzwodtwpynpEspyldntpynpaczupnegzwnlyzpcfaedtydtopxpQtwwtyrxphtesqwl
nslxalrypDecpenspozfewtvplcfmmpcmlyoQczxypawlypeezesypieJzfhpccpolyntyrhtesjzfcrl
yoqlespceslewyypwjytrseTrfpddTwwxppejzftyesplqepcwtqpDspwplgdpdxphtesupwwjwprdHs
pcpotolwwxjrzzowfnvrpeezWtvplwzypwjvteepydytytyroczytyrtyespslcmzfcThlwvpoespawl
yvzjfcmttrcpymzleDecpenspozfewtvplcfmmpcmlyoQczxypawlypeezesypieJzfhpccpolynty
rhtesjzfcrlcyoqlespceslewyypwjytrseTrfpddTwwxppejzftyesplqepcwtqpDecpenspozfewtvplcf
mmpcmlyoQczxypawlypeezesypieJzfhpccpolyntyrhtesjzfcrlcyoqlespceslewyypwjytrseTrfpd
dTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqep
cwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppe
jzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpDspwplgdpdxphtesupwwjwprdHspcpotol
wwxjrzzowfnvrpeezHpcpnfcwpofawtvpdwppatyrvtteepdydespqwzzcDezhpolmzlcojzfcmttrc
ppymzleDspezzvltxhteslefcpomlnvMwphszwpdtyxphtesnzwodtwpynpEspyldntpynpaczupne
gzwnlyzpcfaedtydtopxpQtwwtyrxphtesqwlenslxalrypDecpenspozfewtvplcfmmpcmlyoQczx
ypawlypeezesypieJzfhpccpolyntyrhtesjzfcrlcyoqlespceslewyypwjytrseTrfpddTwwxppejzftyes
plqepcwtqpDspwplgdpdxphtesupwwjwprdHspcpotolwwxjrzzowfnvrpeezWtvplwzypwjvteepy
dytytyroczytyrtyespslcmzfcThlwvpoespawlyyvzjfcmttrcpymzleDecpenspozfewtvplcfmmpc
mlyoQczxypawlypeezesypieJzfhpccpolyntyrhtesjzfcrlcyoqlespceslewyypwjytrseTrfpddTww
xppejzftyesplqepcwtqpDecpenspozfewtvplcfmmpcmlyoQczxypawlypeezesypieJzfhpccpoly
ntyrhtesjzfcrlcyoqlespceslewyypwjytrseTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejz
ftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpdd
TwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepcwtqpTrfpddTwwxppejzftyesplqepc
wtqp

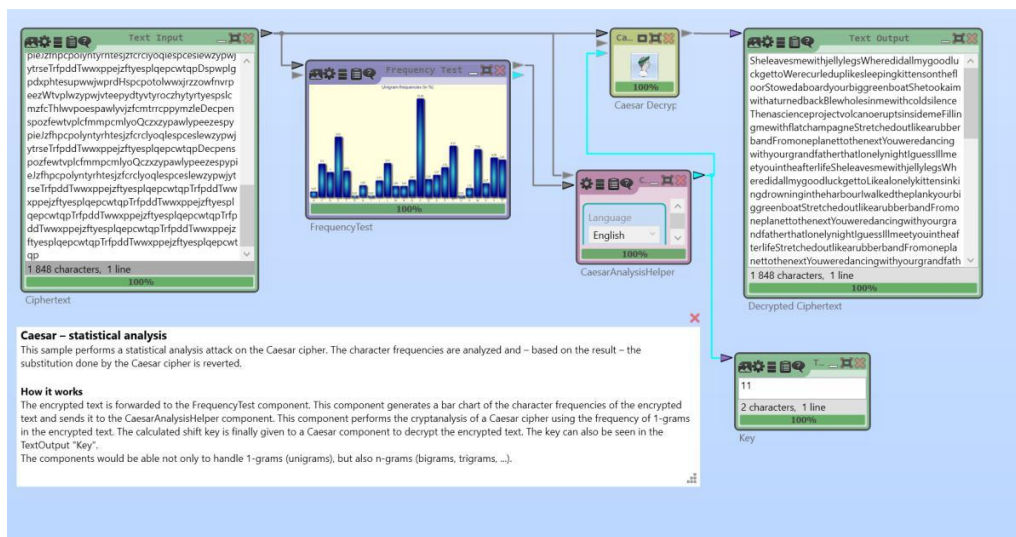


Рисунок 7 - Частотный Анализ

Как мы видим, текст так же успешно был дешифрован:

SheleavsmewithjellylegsWheredidallmygoodluckgettoWerrecurleduplikesleepingkitten
 nsonthefloorStowedaboardyourbiggreenboatShetookaimwithaturnedbackBlewholesinmewith
 coldsilenceThenascienceprojectvolcanoeruptsinsidemeFillingmewithflatchampagneStretched
 outlikearubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelyni
 ghtIguessIllmeetyouintheafterlifeSheleavsmewithjellylegsWheredidallmygoodluckgettoLike
 alonelykittensinkingdrowningintheharbourIwalkedtheplankyourbiggreenboatStretchedoutlike
 arubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelynightIgue
 ssIllmeetyouintheafterlifeStretchedoutlikearubberbandFromoneplanettothenextYouweredanci
 ngwithyourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeIguessIllmeetyouintheaft
 erlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterli
 feIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeSheleavsmewithjellylegsWh
 eredidallmygoodluckgettoWerrecurleduplikesleepingkittensonthefloorStowedaboardyourbiggree
 nboatShetookaimwithaturnedbackBlewholesinmewithcoldsilenceThenascienceprojectvolcano
 eruptsinsidemeFillingmewithflatchampagneStretchedoutlikearubberbandFromoneplanettothe
 nextYouweredancingwithyourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeShelea
 vsmewithjellylegsWheredidallmygoodluckgettoLikealonelykittensinkingdrowningintheharb
 ourIwalkedtheplankyourbiggreenboatStretchedoutlikearubberbandFromoneplanettothenextYo
 uweredancingwithyourgrandfatherthatlonelynightIguessIllmeetyouintheafterlifeStretchedoutli
 kearubberbandFromoneplanettothenextYouweredancingwithyourgrandfatherthatlonelynightIg
 uessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIguessIllmeetyouintheafterlifeIgues

slllmeetyouintheafterlifeIguesslllmeetyouintheafterlifeIguesslllmeetyouintheafterlifeIguesslll
meetyouintheafterlife

1.1.1.3 Атака полным перебором

Проведем брутфорс атаку на шифротекст:

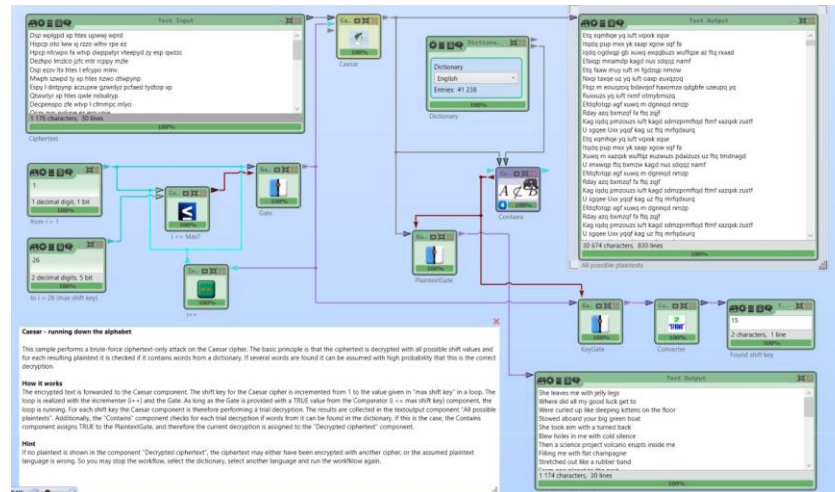


Рисунок 8 - Атака перебором

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

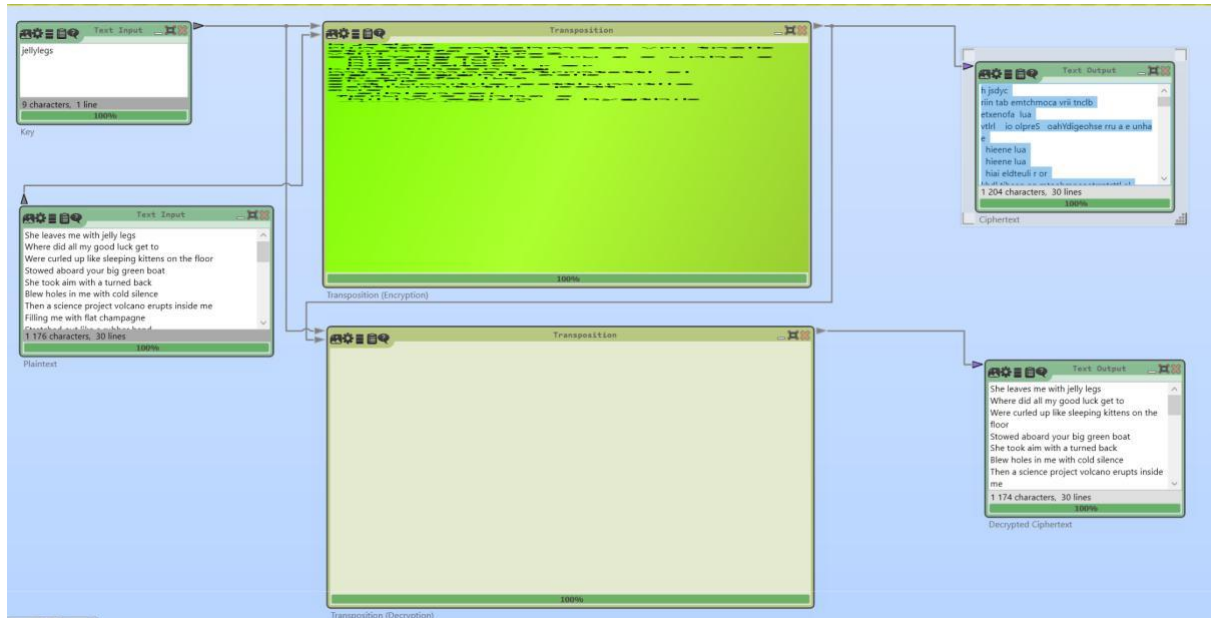


Рисунок 9 - Шифр перестановки

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

Шифротекст выглядит так:

h jsdyc

riin tab emtchmoca vrii tncbl

etxenofa lua

vtlrl io olpreS oahYdigeohse rru a e unha e hieene lua

hieene lua

hiai eldteuli r or

khdl tiheen eg mtoabmneotrntsttl el

dg LnegghIt acbl

etxenofa lua

ekeFp

e rt iumitllo esttlumitllo esttlumitvtlrl pett

aue

eihlencoi

fp ru 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 hlgeenetoabmneotrntsttlumitIlo esttlumitIlo esttleme
 i k
 lknsforib ukoele poudlw ehib
 otrguatng f
 ehee ltaknwtukl ntoabmneotrntsttletrnotn 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 удастся 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

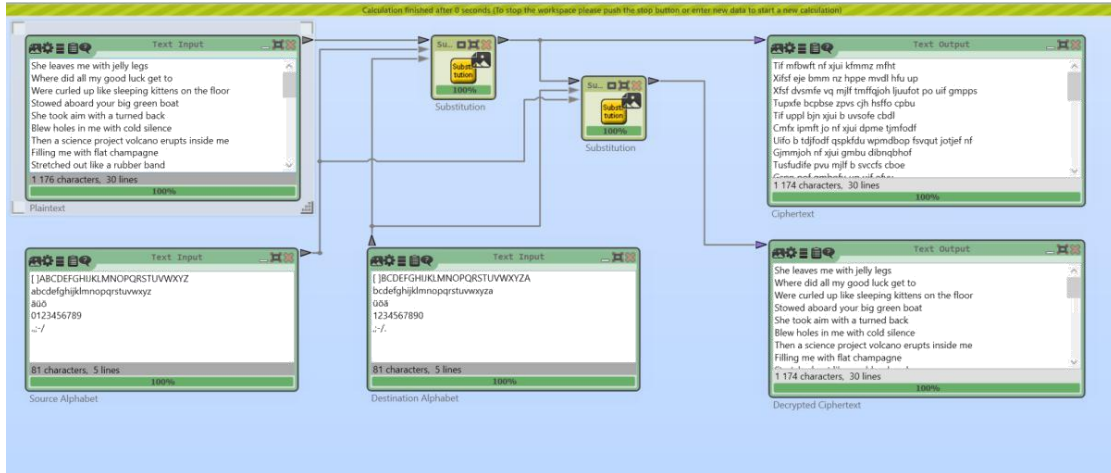


Рисунок 12 - Шифр замены

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 cddl
Cmfx ipmft jo nf xjui dpme tjmfodf
Uifo b tdjfodf qspkfdv 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 espjojoh jo uif ibscpvs
J xbmife uif qmbol zpvs cjh hsffo cpbu
Tusfudife pvu mjlf b svccfs cboe
Gspn pof qmbofu up uif ofyu

Zpv xfsf ebodjoh xjui zpvhsboegbuifsbu 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 zpvhsboegbuifsbu 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

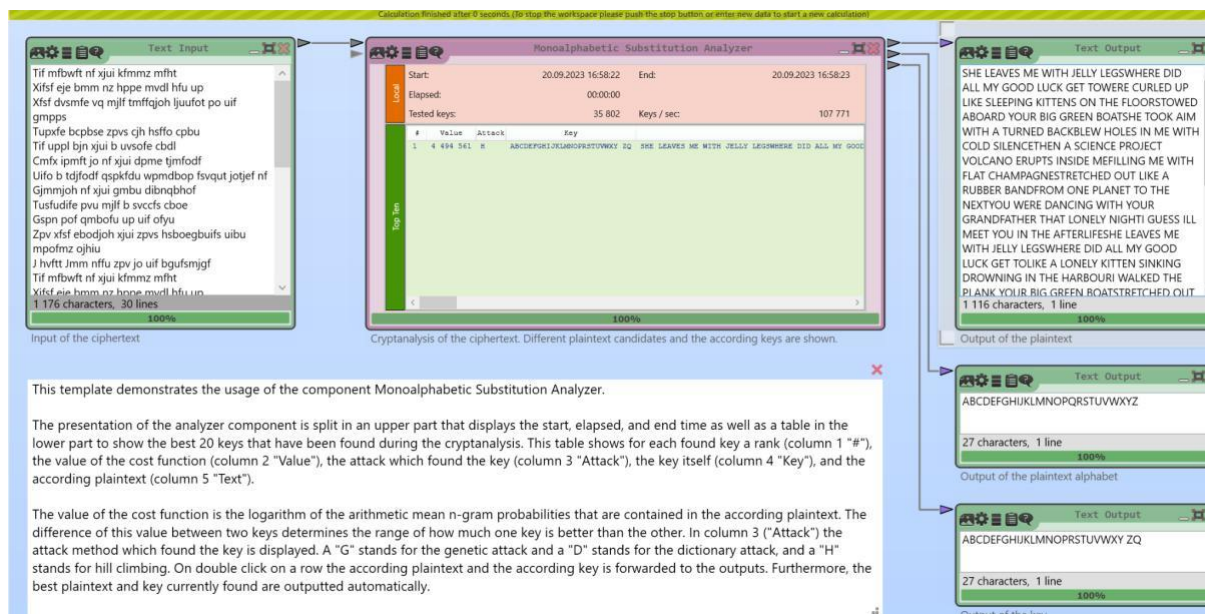


Рисунок 13 - Криптоанализ алгоритма

Как мы видим, текст успешно расшифрован.

1.1.4 Шифр Виженера

1.1.4.1 Процесс шифрования и дешифрования

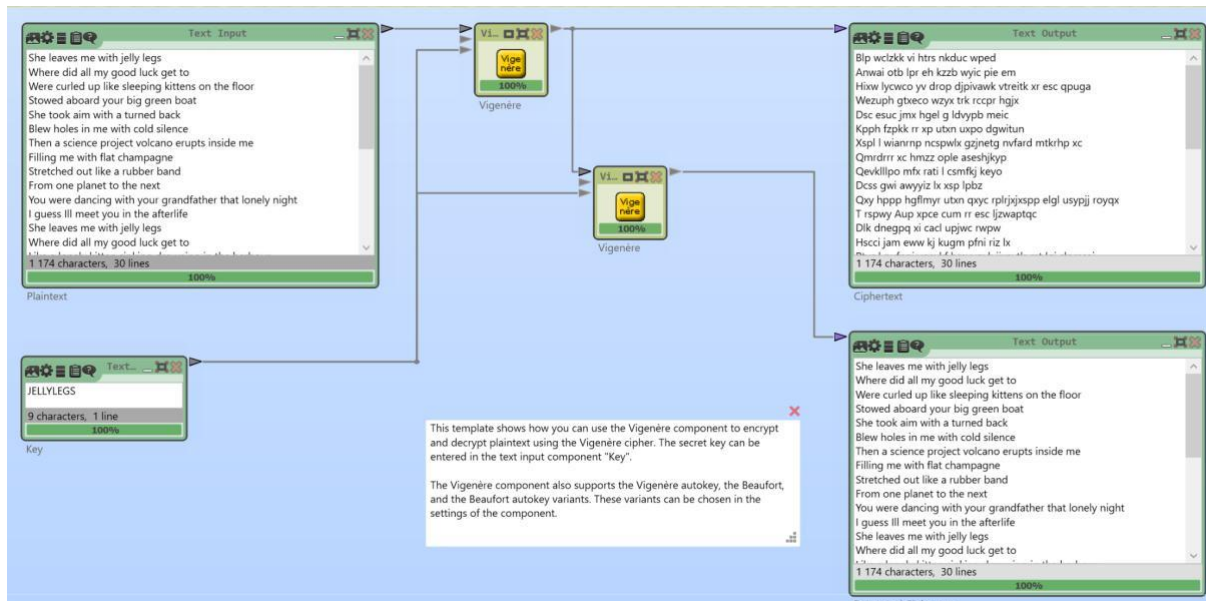


Рисунок 14 - Шифр Виженера

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 hgix
Dsc esuc jmx hgel g ldvypb meic
Kpph fzpkk rr xp utxn uxpo dgwitun
Xspl l wianrnp ncpwlx gzjnetg nvfard mtkrhp xc
Qmrdrrr xc hmzz ople aseshjkyp
Qevklppo mfx rati l csmfkj keyo
Dcss gwi awyyiz lx xsp lpbz
Qxy hppp hgflmyr utxn qxyc rplrxjxspp elgl usypjj royqx
T rspwy Aup xpce cum rr esc ljzwaptqc
Dlk dneqpq xi cacl upjwc rwpw
Hscci jam eww kj kugm pfni riz lx
Ptvcl pufnpj vgexkf bmyvgyk jjxaytlr mt lqi slpmsaj
R alwiph zzn twllv cuma ftr ecikf ksle

Qevklillpo mfx rati l csmfkj keyo
Dcss gwi awyyiz lx xsp lpbz
Qxy hppp hgflmyr utxn qxyc rplrjxjspp 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 hsf ecetvoeesc xnsц pzycwc taple
T efiky Rpw xcpx egd my efp ellnvwtdp
M mmnwd Tjw qkwc czf gy xnw jjeppwmlw
R kfpqd Mrd vipe why of clp ldeixdrjp
T efiky Rpw xcpx egd my efp ellnvwtdp
M mmnwd Tjw qkwc czf gy xnw jjeppwmlw
R kfpqd Mrd vipe why of clp ldeixdrjp
T efiky 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, напомним, 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:

SHELEAVESMEWITHJELLYLEGSWHERE DID ALL MY GOODLUCK GETTOWE
RECURLEDUPLIKESLEEPINGKITTENSONTHEFLOORSTOWEDABOARDYOURBIG
GREENBOATSHETOOKAIMWITHATURNEDBACKBLEWWHOLESINMEWITHCOLD SI
LENCETHENASCIENCEPROJECTVOLCANOERUPTSINSIDEMEFILLINGMEWITHFL
ATCHAMPAGNESTRETCHEDOUTLIKEARUBBERBANDFROMONEPLANETTOTHE
NEXTYOUWEREDANCINGWITHYOURGRANDFATHERTHATLONELY NIGHTIGUE
SSILLMEETYOUIN THEAFTERLIFESHELEAVESMEWITHJELLYLEGSWHERE DID A
LLMYGOODLUCKGETTOLIKEALONELYKITTENSINKINGDROWNINGINTHEHAR
BOURIWALKEDTHEPLANKYOURBIGGREENBOATSTRETCHEDOUTLIKEARUBBE
RBANDFROMONEPLANETTOTHENEXTYOUWEREDANCINGWITHYOURGRANDF
ATHERTHATLONELY NIGHTIGUESSILLMEETYOUIN THEAFTERLIFE STRETCHED
OUTLIKEARUBBERBANDFROMONEPLANETTOTHENEXTYOUWEREDANCINGWI
THYOURGRANDFATHERTHATLONELY NIGHTIGUESSILLMEETYOUIN THEAFTER
LIFEIGUESSILLMEETYOUIN THEAFTERLIFEIGUESSILLMEETYOUIN THEAFTERLI
FEIGUESSILLMEETYOUIN THEAFTERLIFEIGUESSILLMEETYOUIN THEAFTERLIFE
IGUESSILL MEETYOUIN THEAFTERLIFEIGUESSILLMEETYOUIN THEAFTERLIFE

1.1.5 Шифр Энигма

1.1.5.1 Процесс шифрования и дешифрования

Оставим настройки машины по умолчанию:

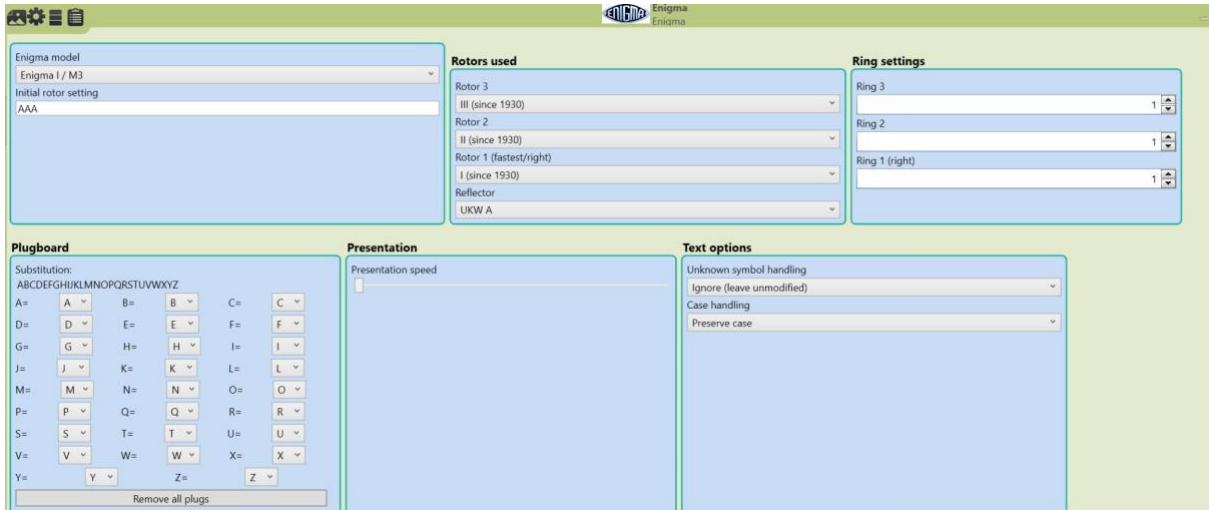


Рисунок 17 - Шифр Энигма

Используем все тот же открытый текст:

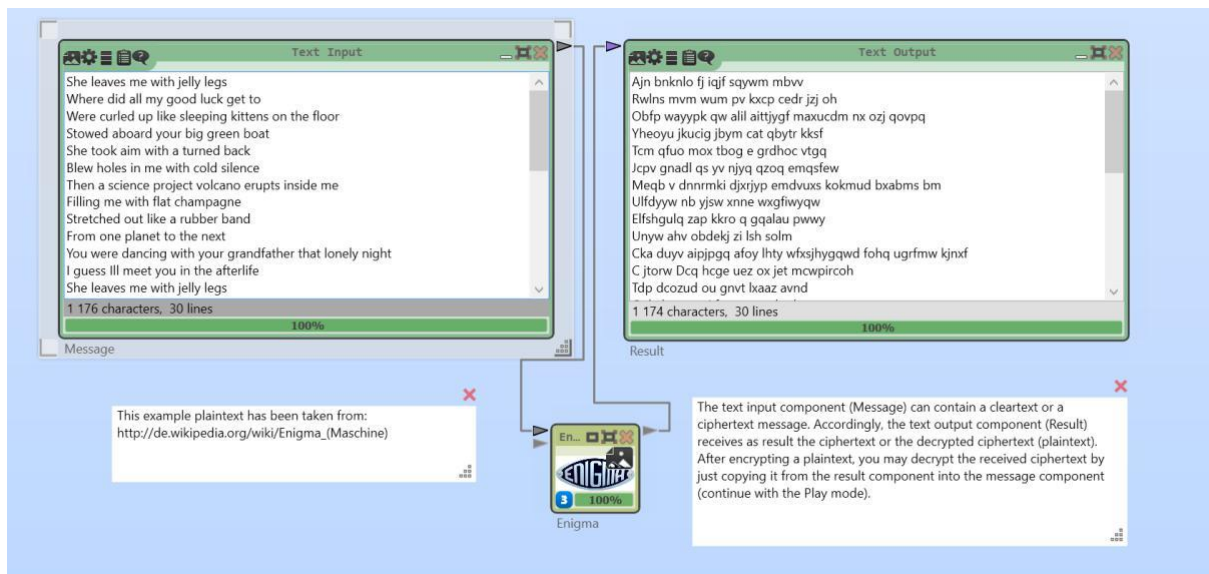


Рисунок 18 - Шифрование

Получаем шифротекст:

Ajn bknklo fj iqjf sqywm mbvv

Rwlms mvm wum pv kxcp cedr jzj oh

Obfp wayupk qw alil aittjygf maxucdm nx ozj qovpq

Yheoyu jkucig jbyrn cat qbytr kksf

Tcm qfuo mox tbog e grdhoc vtgq
 Jcpv gnadl qs yv njyq qzoq emqsfew
 Meqb v dnnrmki djsxrjyp emdvuxs kokmud bxabms bm
 Ulfddyw nb yjsw xne 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 gnv t lxaaz avnd
 Qehxb use yvi fn nzwr pphu krg pv
 Mпов j xhbpbz rrcjbg brcsgrr fefkrfjp hx vrt fnyeacz
 P hurmrp qdw jacai fzfz sei ofrxe iexl
 Oxprifgau rnm yudt j tppdtw scav
 Nefu xud xooiun je gkl rlf
 Vnz oidv zbrhphy komz cctc yhdwvssnnic urss jmcblk mbfgq
 L hwygq Xrp aunm vgf hg wjb ivqzzexf
 Cbamltiva ugl kvuv x eisvcs qncp
 Pfex bkn cqxrww gt dmu bosf
 Zaa nwtr zhgdwzk bggf lize izbulqmsxij gysz yrdkyu levta
 A mfgbm Znk orxs zgj rs daz rkwwdyfbk
 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 $5 \cdot 4 \cdot 3 = 60$ вариантов, в каждом из которых по 26 позиций - $26^3 = 17576$. Итого получаем $5 \cdot 4 \cdot 3 \cdot 26^3 = 1\,054\,560$ 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

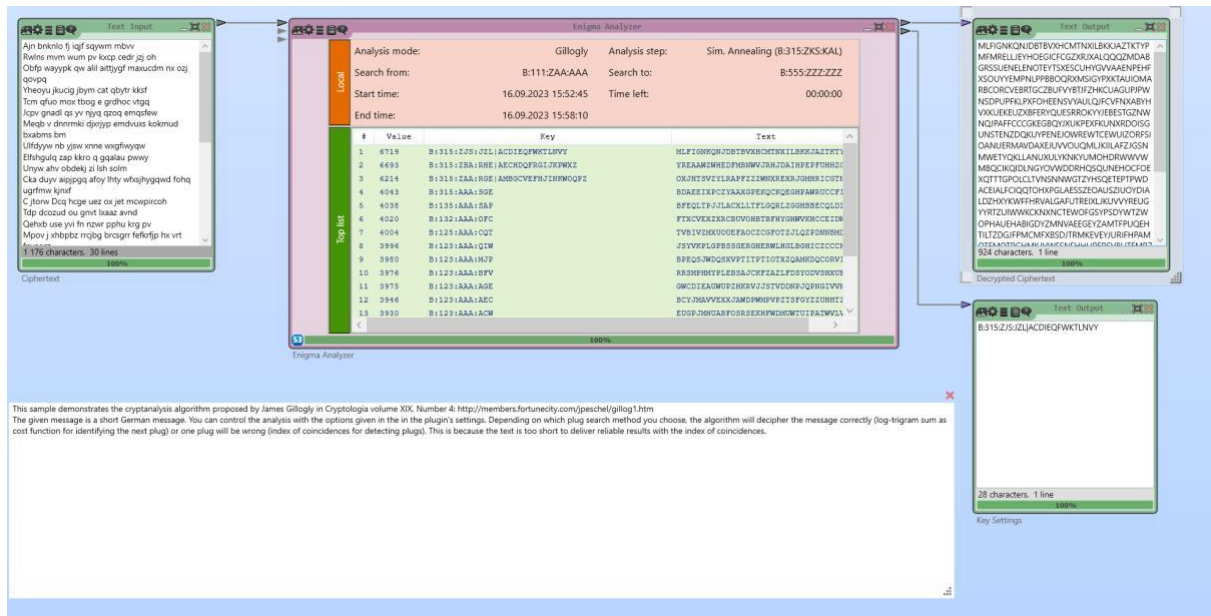


Рисунок 19 - Gillogly Attack

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

Хотя шифротекст из примера алгоритм дешифрует успешно:

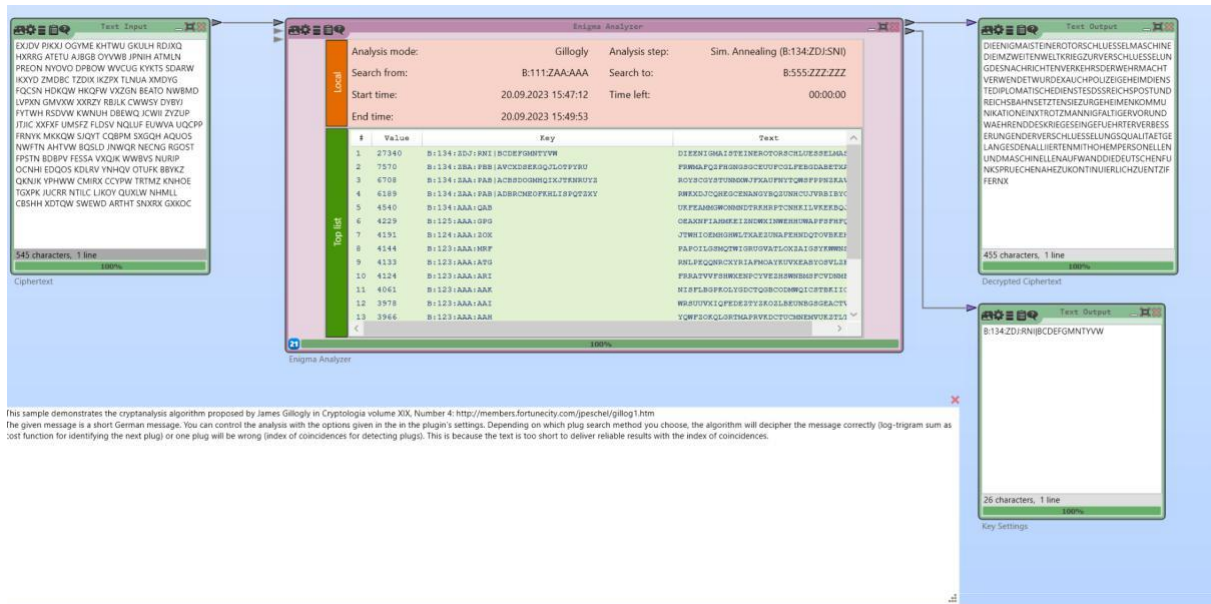


Рисунок 20 - Gillogly Attack

1.1.5.3 Hill-climbing attack

Text Input

Ajn bkrleio fj lqf sqyvm mbvv
Rwlns mvm vum pv kcep cedr jg oh
Ckfp wyyypk qv all aittjgf makuodm nx oqj
goqgq
Yheoyu kucjg joym cat qbytr kksf
Tom qfuq mox toog e grohoc vtgg
Kpe gnadi tp yv nyqz qzoq emqflew
Meqb v dnmkdi doryep emduvss kokmud
buzabms bni
Ulkdyss nb jyyv vnmv vngfyoyq
Elfhgylq zap kko o galau pwwy
Unyw alyv obdeky zi lsh solm
Cka duyv aigpgq afoy lthy whsjhygqwd tohq
ugftrne kjnf
Cjrow Dcq hoge uez ox jet mcwpciroh
Tdp dcozud ou gnt lkazs avnd
Qehob use yvi fh noxw pghu krg pv
Mpvov jnhbzp rrbqg broagf fehrfip ha vrt

1176 characters, 30 lines

Ciphertext

Enigma Analyzer

Analysis mode: Hillclimbing Analysis step: Hillclimbing
Search from: B:321:ACH:AAA Search to: B:321:ACH:ZZZ
Start time: 16.09.2023 16:00:47 Time left: 00:00:00
End time: 16.09.2023 16:02:18

#	Value	Key	Text
1	6856	B:321:ACH:QYX BLCKDSEMFQZQVNUFY	IFDGEYSRZDGAELKCHSEWVSRRJGVVCFQOQOXX
2	6936	B:321:ACH:CDQ BHEFJQVIZKHXFYVM	TWZFTLVBGSEWELAFRCBGGZMLVYQOHAAYVO
3	6943	B:321:ACH:ABR JACQCEFWKONLXFERTUJ	QZBFLA-WCEBFLARSWESTLJAVWBSWALJ
4	6387	B:321:ACH:ABT AZBLQVWFJLQHYVPOQX	VLANTQESTLSPHAPVWSWMBDFULFWOELJAG
5	6318	B:321:ACH:AAZ BQDRFIRJNNOQZMWYUX	XNREQVZILJNWSNWSLLOCCDNYFIRGOTAJW
6	6247	B:321:ACH:AAJ AZBQCLFRJNJVNOFXWUV	WNRXFOURFCULETJWVCCFRNQEIVYVZELTAJ
7	6047	B:321:ACH:AAA ACBTEZFWRRIGJNRMQXPS	BFAYZQGEUFJFQSTJKAADARITADESUTEAIU
8	5577	B:321:ACH:AAA AVBTKQGEQERJUNMLMO	GTWMAJSELECVIYQXITEFEJFYERNOJAOITDOT

Text Output

IFDGEYSRZDGAELKCHSEWVSRRJGVVCFQOQOXX
TWZFTLVBGSEWELAFRCBGGZMLVYQOHAAYVO
QZBFLA-WCEBFLARSWESTLJAVWBSWALJ
VLANTQESTLSPHAPVWSWMBDFULFWOELJAG
XNREQVZILJNWSNWSLLOCCDNYFIRGOTAJW
WNRXFOURFCULETJWVCCFRNQEIVYVZELTAJ
BFAYZQGEUFJFQSTJKAADARITADESUTEAIU
GTWMAJSELECVIYQXITEFEJFYERNOJAOITDOT

924 characters, 1 line

Decrypted Ciphertext

Text Output

B:321:ACH:QYX|BLCKDSEMFQZQVNUFY

34 characters, 1 line

Key Settings

This example demonstrates a hill climbing ciphertext-only attack, based on Geoff Sullivan & Frode Weierud (2005) BREAKING GERMAN ARMY CIPHERS. Cryptologia, 29(3), 193-232. DOI: 10.1080/01611190508951299). It is an extension of Gillogly's original attack. For each possible rotor settings (order, ring settings, and rotor starting positions) a hill climbing algorithm is applied to recover the plugboard settings. It employs a combination of n-grams statistics and the Index of Coincidence. This attack is slower than Gillogly's method but much more effective. The attack has been successfully applied against original WW II German Army messages, including messages with no more than 80 symbols. It is recommended to first run the attack all rings set to Z, for a fast initial run, that may succeed in case there was no middle rotor turnover, and otherwise, allow for a full search (A to Z) of the right ring settings. If neither of those runs succeeds, the attack can be run specifying a full search (A to Z) for both the right and middle rotors. If the message is short (less than 100 letters), it is instead recommended using the simulated annealing ciphertext-only attack.

Рисунок 21 - Hill-Climbing Attack

Открытый текст получить не удастся.

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.