Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ
О ПРАКТИЧЕСКОЙ РАБОТЕ № 1
по дисциплине «Математические основы защиты информации»
Подстановочные шифры

Студент гр. БИБ201
Д.А. Морин
«19» 03.2022 г.

Руководитель
Заведующий кафедрой информационной
безопасности киберфизических систем
канд. техн. наук, доцент
О.О. Евсютин
«___» _____ 2022 г.

Москва 2022

Оглавление

1 Краткие теоретические сведения

Шифр - система обратимых преобразований, зависящая от некоторого секретного параметра (ключа) и предназначенная для обеспечения секретности передаваемой информации.
Ключ - это часть информации, обычно представляющая собой строку цифр или букв, хранящуюся в файле, которая при обработке с помощью криптографического алгоритма может кодировать или декодировать криптографические данные.
Кодирование - это преобразование информации из одной ее формы представления в другую, наиболее удобную для её хранения, передачи или обработки.
Декодирование - процесс восстановления изначальной формы представления информации, т. е. обратный процесс кодирования, при котором закодированное сообщение переводится на язык, понятный получателю.
Шифрование (зашифрование) - обратимое преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней.
Расшифрование - процесс преобразования зашифрованных данных в открытые данные при помощи шифра.
Дешифрование (дешифровка) - процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного.
Открытый текст - в криптографии исходный текст, подлежащий шифрованию, либо получившийся в результате расшифровки. Может быть прочитан без дополнительной обработки (без расшифровки).
Шифротекст, шифртекст, криптограмма - результат операции шифрования.
Шифр простой замены, простой подстановочный шифр, моноалфавитный шифр - класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифртекста.Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которому она генерируется.
Аффинный шифр - это тип моноалфавитного шифра подстановки, где каждая буква алфавита сопоставляется с ее числовым эквивалентом, шифруется с помощью простой математической функции и преобразуется обратно в букву.
аффинный рекуррентный шифр - усиление аффинного шифра, когда для каждого символа открытого текста вычисляется новое ключевое значение на основе предыдущего.
Частотный анализ, частотный криптоанализ - один из методов криптоанализа, основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей, как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и

дешифрования. Частотный анализ предполагает, что частотность появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка.
Метод «грубой силы», полный перебор предполагает перебор всех возможных вариантов ключа шифрования до нахождения искомого ключа.

2 “Ручное” шифрование и расшифрование
1.Шифр простой замены.

(ABCDEFGHIJKLMNOPQRSTUVWXYZ)
Ключ = (KTDILRNBQZWPCJEYMAGOXSHUVF)
1)
X = TOFIGHT => Y = OERQNBO
2)
X = SHORTANDSWEET => Y = GBEAOKJIGHLLO
3)
X = ELOQUENTLY => Y = LPEMXLJOPV

Теперь возьмем другой ключ и зашифруем (и расшифруем) те же слова
(ABCDEFGHIJKLMNOPQRSTUVWXYZ)
Ключ = (LTYRUACMBKQEXWJIFPSDNHVOZG)
4)
X = TOFIGHT => Y = DJABCMD
5)
X = SHORTANDSWEET => Y = SMJPDLWRSVUUD
6)
X = ELOQUENTLY => Y = UEJFNUWDEZ

2.Аффинный шифр
Мощность английского алфавита |A| = m = 26
Группа обратимых элементов Z(26)* данного кольца
{1,3,5,7,9,11,15,17,19,21,23,25}
1)
Пусть a = 17, b = 24
X = TOFIGHT = (19,14,5,8,6,7,19)
y1 = 17*19+24 = 9
y2 = 17*14+24 = 2
y3 = 17*5+24 = 5
y4 = 17*8+24 = 4
y5 = 17*6+24 = 22
y6 = 17*7+24 = 13
y7 = 17*19+24 = 9
Y = JCFEWNJ
Зашифровали. Осталось расшифровать:
находим a^(-1) (таблица 1)

m	a	y2	y1
26	17	0	1
17	9	1	-1
9	8	-1	2
8	1	2	-3

Таблица 1 - нахождение обратного элемента a = a^(-1)
a^(-1) = -3 = 23
x1 = (9-24)*23 = 19
x2 = (2-24)*23 = 14
x3 = (5-24)*23 = 5
x4 = (4-24)*23 = 8
x5 = (22-24)*23 = 6
x6 = (13-24)*23 = 7
x7 = (9-24)*23 = 19
X = TOFIGHT

2)
Пусть a = 3, b = 18
X = SHORTANDSWEET = (18,7,14,17,19,0,13,3,18,22,4,4,19)
y1 = 3*18+18 = 20
y2 = 3*7+18 = 13
y3 = 3*14+18 = 8
y4 = 3*17+18 = 17
y5 = 3*19+18 = 23

y6 = 3*0+18 = 18
y7 = 3*13+18 = 5
y8 = 3*3+18 = 1
y9 = 3*18+18 = 20
y10 = 3*22+18 = 6
y11 = 3*4+18 = 4
y12 = 3*4+18 = 4
y13 = 3*19+18 = 23
Y = UNIRXSFBUGEEX
Зашифровали. Осталось расшифровать:
находим a^(-1) (таблица 2)

m	a	y2	y1
26	3	0	1
3	2	1	-8
2	1	-8	9

Таблица 2 - нахождение обратного элемента a = a^(-1)
a^(-1) = -3 = 23
x1 = (20-18)*23 = 18
x2 = (13-18)*23 = 7
x3 = (8-18)*23 = 14
x4 = (17-18)*23 = 17
x5 = (23-18)*23 = 19
x6 = (18-18)*23 = 0
x7 = (5-18)*23 = 13
x8 = (1-18)*23 = 3
x9 = (20-18)*23 = 18
x10 = (6-18)*23 = 22
x11 = (4-18)*23 = 4
x12 = (4-18)*23 = 4
x13 = (23-18)*23 = 19
X = SHORTANDSWEET

3.Аффинный рекуррентный шифр
3)
Пусть a1 = 11, b1 = 10, a2 = 9, b2 = 8
X = BLAND = (1,11,0,13,3)
y1 = 11*1+10=21
y2 = 9*11+8=3
y3 = 99*0+10*8=21*0+2=2
y4 = 99*9*13+80*8=7*13+16=3
y5 = 7*99*3+16*80=17*3+6=5
Y = VDCDF
Найдем a(i)^(-1) (таблица 3)

m	a(i)	y2	y1
26	11	0	1
11	4	1	-2
4	3	-2	5
3	1	5	-7
26	9	0	1
9	8	1	-2
8	1	-2	3
26	21	0	1
21	5	1	-1
5	1	-1	5
26	7	0	1
7	5	1	-3
5	2	-3	4
2	1	4	-11
26	17	0	1
17	9	1	-1
9	8	-1	2
8	1	2	-3

Таблица 3 - нахождение обратного элемента a(i) = a(i)^(-1)
a1^(-1) = -7 => x1 = (21-10)*(-7)=1
a2^(-1) = 3 => x2 = (3-8)*3=11

a3^(-1) = 5 => x3 = (2-2)*5=0
a4^(-1) = -11 => x4 = (3-16)*(-11)=13
a5^(-1) = -3 => x5 = (5-6)*(-3)=3
X = BLAND

4)
Пусть a1 = 3, b1 = 18, a2 = 5, b2 = 22
X = RUSE = (17,20,18,4)
y1 = 3*17+18=17
y2 = 5*20+22=18
y3 = 15*18+18*22=15*18+6=16
y4 = 5*15*4+6*22=23*4+2=16
Y = RSQQ
Найдем a(i)^(-1) (таблица 4)

m	a(i)	y2	y1
26	3	0	1
3	2	1	-8
2	1	-8	9
26	5	0	1
5	1	1	-5
26	15	0	1
15	11	1	-1
11	4	-1	2
4	3	2	-5
3	1	-5	7
26	23	0	1
23	3	1	-1
3	2	-1	8
2	1	8	-9

Таблица 4 - нахождение обратного элемента a(i) = a(i)^(-1)
a1^(-1) = 9 => x1 = (17-18)*9=17
a2^(-1) = -5 => x2 = (18-22)*(-5)=20
a3^(-1) = 7 => x3 = (16-6)*7=18
a4^(-1) = -9 => x4 = (16-2)*(-9)=4
X = RUSE

3 Программная реализация зашифрования и расшифрования
Шифр простой замены
1)
Ответ программы 1.py (рисунок 1):

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
New alphabet:
KTDILRNBQZWPCJEYMAGOXSHUVF
Text:
TOFIGHT
enc or dec: enc
Ciphertext:  OERQNBO

C:\Users\HONOR\Desktop\security>C:/U
Key:
Alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
New alphabet:
KTDILRNBQZWPCJEYMAGOXSHUVF
Text:
OERQNBO
enc or dec: dec
Original text:  TOFIGHT
```

Рисунок 1 - результат программы зашифрования и расшифрования текста
2)
Ответ программы 1.py (рисунок 2):

```
Key:
Alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
New alphabet:
KTDILRNBQZWPCJEYMAGOXSHUVF
Text:
SHORTANDSWEET
enc or dec: enc
Ciphertext:  GBEAOKJIGHLLO

C:\Users\HONOR\Desktop\security>
Key:
Alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
New alphabet:
KTDILRNBQZWPCJEYMAGOXSHUVF
Text:
GBEAOKJIGHLLO
enc or dec: dec
Original text:  SHORTANDSWEET
```

Рисунок 2 - результат программы зашифрования и расшифрования текста
3)
Ответ программы 1.py (рисунок 3):

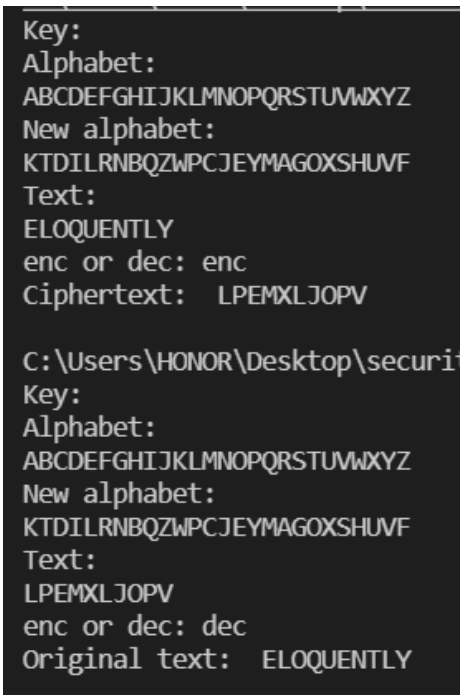

Рисунок 3 - результат программы зашифрования и расшифрования текста 4)

Ответ программы 1.py (рисунок 4):

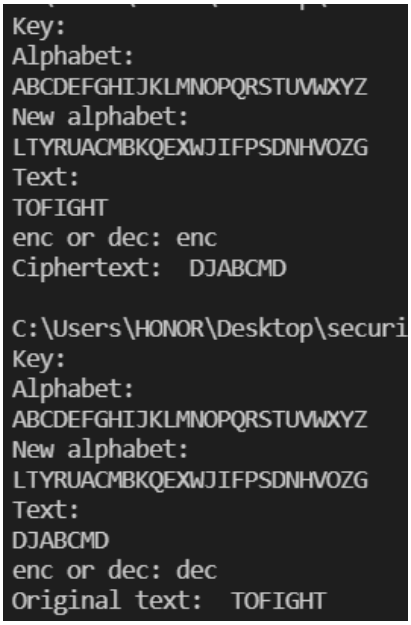

Рисунок 4 - результат программы зашифрования и расшифрования текста 5)

Ответ программы 1.py (рисунок 5):

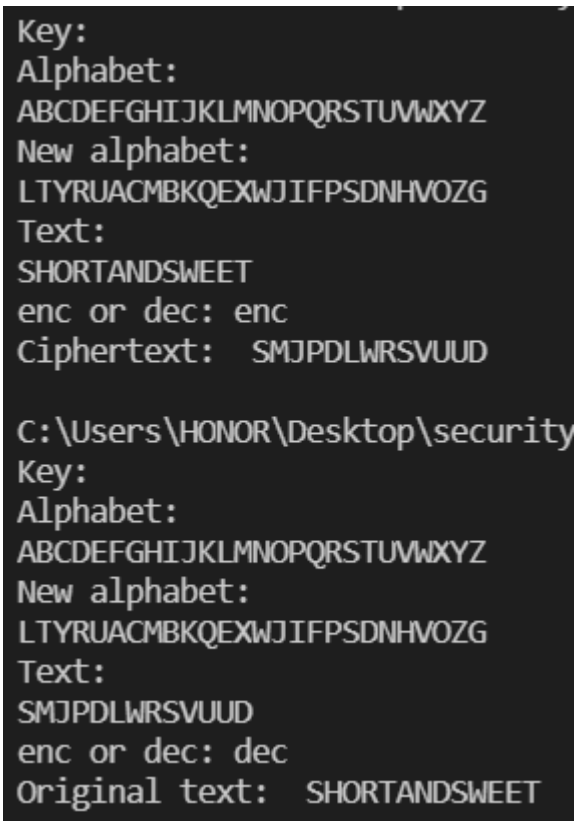

Рисунок 5 - результат программы зашифрования и расшифрования текста

6)

Ответ программы 1.py (рисунок 6):

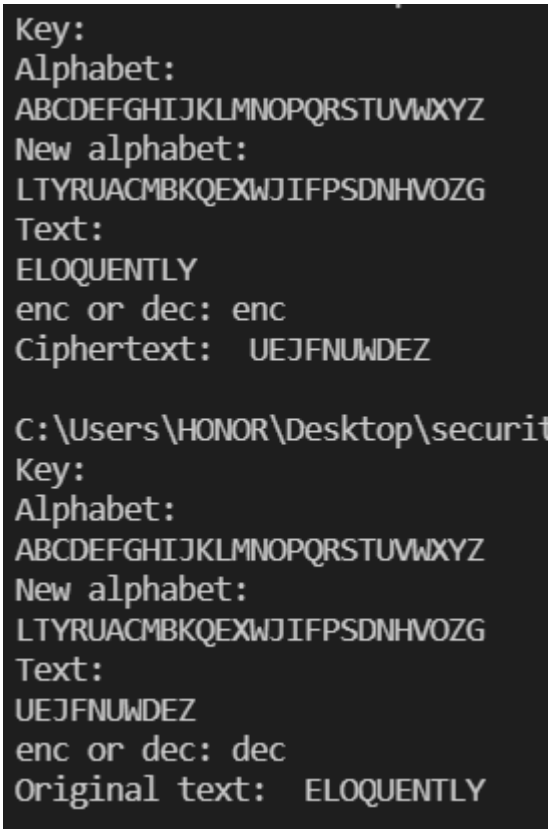

Рисунок 6 - результат программы зашифрования и расшифрования текста

Аффинный шифр

1)

Возьму ключ a = 17 и b = 24, текст TOFIGHT и воспользуюсь текущим шифром. Тогда я получу зашифрованный текст, показанный на рисунке 7. Тем же ключом и взяв зашифрованный текст можно расшифровать его, задействовав другую функцию в файле 2.py. Как видно на рисунке 7, мы получили правильный открытый текст

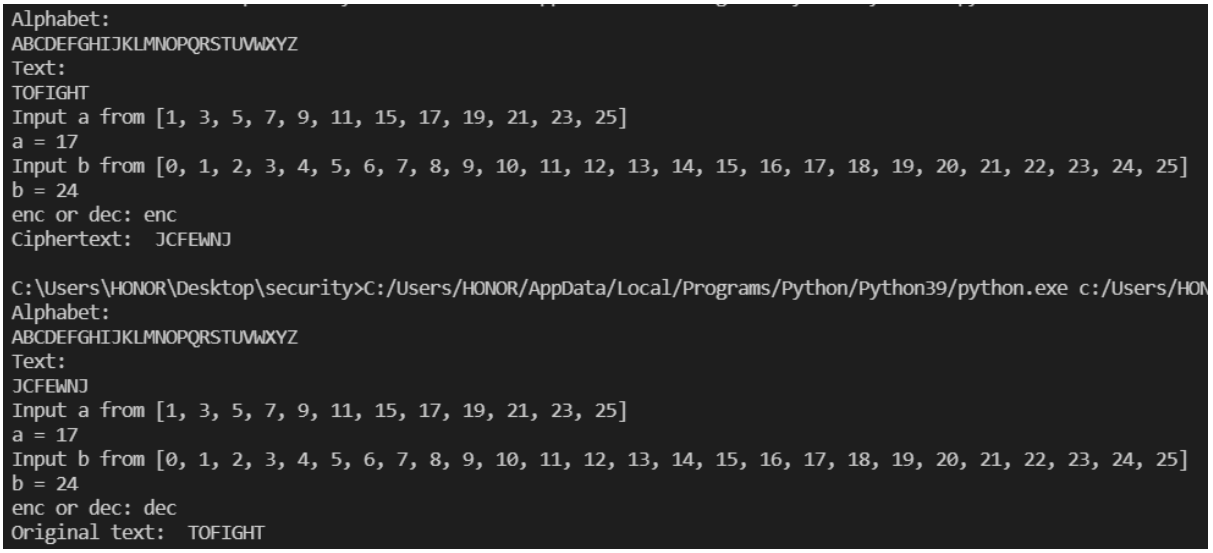

Рисунок 7 - реализация аффинного шифра

2)

Аналогичную работу можно проделать с другим открытым текстом (рисунок 8)

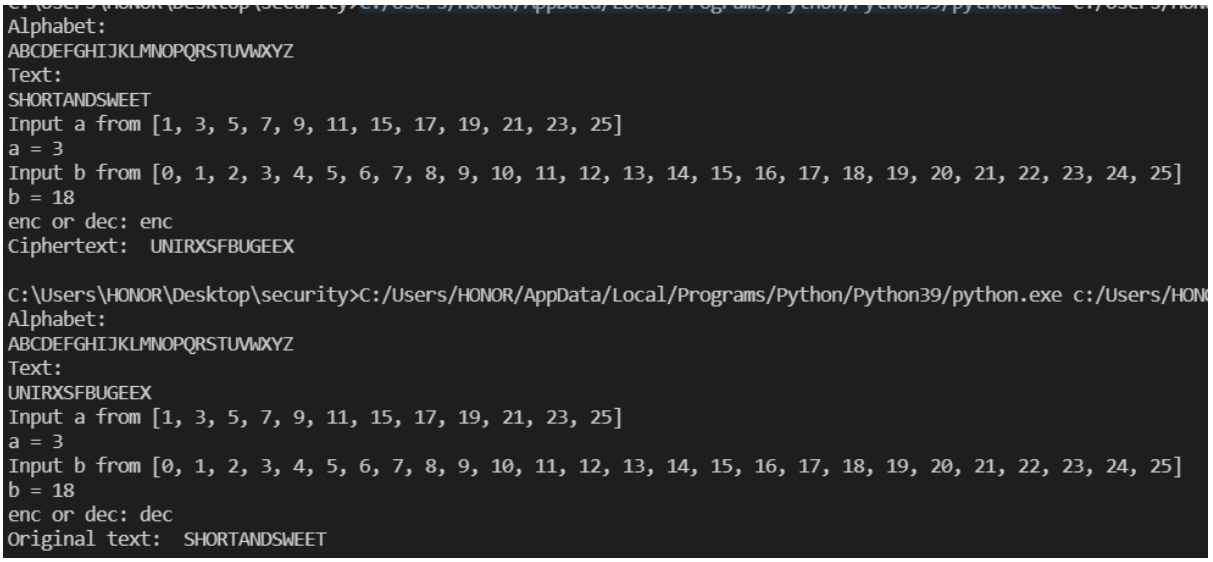

Рисунок 7 - реализация аффинного шифра (другой пример)

Аффинный рекуррентный шифр

3)

Таким же образом, как и “ручным” зашифрованием и расшифрованием, реализован алгоритм аффинного рекуррентного шифра (рисунок 8,9)

```
Alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Text:
BLAND
Input a1, a2 from [1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]
a1 = 11
a2 = 9
Input b1, b2 from [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]
b1 = 10
b2 = 8
enc or dec: enc
21
3
2
3
5
Ciphertext:  VDCDF

C:\Users\HONOR\Desktop\security>C:/Users/HONOR/AppData/Local/Programs/Python/Python39/python.exe c:/Users/HONOR/De
Alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Text:
VDCDF
Input a1, a2 from [1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]
a1 = 11
a2 = 9
Input b1, b2 from [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]
b1 = 10
b2 = 8
enc or dec: dec
Original text:  BLAND
```

Рисунок 8 - реализация аффинного рекуррентного шифра (другой пример)

4)

```
Alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Text:
RUSE
Input a1, a2 from [1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]
a1 = 3
a2 = 5
Input b1, b2 from [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]
b1 = 18
b2 = 22
enc or dec: enc
Ciphertext:  RSQQ

C:\Users\HONOR\Desktop\security>C:/Users/HONOR/AppData/Local/Programs/Python/Python39/python.exe c:/Users/HONOR/De
Alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Text:
RSQQ
Input a1, a2 from [1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]
a1 = 3
a2 = 5
Input b1, b2 from [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]
b1 = 18
b2 = 22
enc or dec: dec
Original text:  RUSE
```

Рисунок 9 - реализация аффинного рекуррентного шифра (другой пример)

4 Криптоанализ вышеупомянутых шифров

1)

Частотный анализ

Для него мне понадобится частота встречаемости букв английского алфавита (рисунок 10)

A	8,17%	H	6,09%	O	7,51%	V	0,98%
B	1,49%	I	6,97%	P	1,93%	W	2,36%
C	2,78%	J	0,15%	Q	0,10%	X	0,15%
D	4,25%	K	0,77%	R	5,99%	Y	1,97%
E	12,70%	L	4,03%	S	6,33%	Z	0,07%
F	2,29%	M	2,41%	T	9,06%		
G	2,02%	N	6,75%	U	2,76%		

Рисунок 10 - частота встречаемости букв в английском алфавите

Следующий текст будет подвергаться криптоанализу:

WHATISWIFIANDWHEREISITUSEDTHEWORLDOFMODERNTELECOMMUNICATI
ONTECHNOLOGYISAWASHWITHACRONYMSLONGNUMBERSANDOTHERWEIR
DBITSOFCODETHATFEWPEOPLEUNDERSTANDBUTWIFIDOESNTREALLYSTAN
DFORWIRELESSFIDELITYUSINGTHISSTANDARDCOMPUTERSANDOTHERDEVI
CESCANLINKINAWIRELESSLOCALAREANETWORKWLANWHICHISANUMBERO
FCOMPUTERSORCOMPUTERLIKEDEVICESTHATCANTALKTOEACHOTHERUSI
NGHIGHFREQUENCYRADIOWAVESINSTEADOFCONNECTINGCABLESTHEWLA
NCANINTURNBEHOOKEDINTOTHEINTERNETUSUALLYWITHTHEAIDOFACABL
EBASICALLYTHENWIFIISAGENERICNAMEFORTHEMAINMETHODBYWHICHAW
LANISSETUPBUTTHETERMWIFIASWELLASTHETECHNOLOGYITSELFHASEVO
LVEDQUITEABITSINCEITWASFIRSTCOINEDINABOUTANDISNOWUSEDMOREB
ROADLYPARTICULARLYBYTHEGENERALPUBLICTOMEANAWIDERANGEOFWIR
ELESSCOMMUNICATIONTECHNOLOGIESWIFIUSESPERHAPSTHEMOSTVISIBL
EMANIFESTATIONOFWIFIISTHECOFFEESHOPLAPTOPTUNEDCORDLESSLYINT
OAWLANANDHENCEINTOTHEWORLDWIDEWEBBUTSOMEPHONEUSERSMIGH
TALSOBEDOINGITBYWIFIVOIPVOICEOVERTHEINTERNETPROTOCOLPHONES
ENABLEUSERSTOSPEAKTOOTHERSVIATHEINTERNETTHEINCREASINGAVAIL
ABILITYOFWIFIMEANSTHATPEOPLEWITHVOIPPHONESCANUSETHEMMOREA
NDMORELIKEMOBILEPHONESTALKINGWITHFRIENDSANDCOLLEAGUESOVER
THEINTERNETFROMTHESAMECOFFEESHOPINWHICHTHEYCONNECTTHEIRL
APTOPSTOTHEWORLDWIDEWEBWIFIISUSEDINMANYOTHERAPPLICATIONSA
SWELLSOMETELEVISIONSAREGOINGWIFIALLOWINGVIEWERSTOWANDERAB
OUTTHEIRHOUSESWITHTHEIROWNPORTABLESCREENSONECOMPANYRECE
NTLYOFFEREDACAMERATHATCONNECTSTOTHEINTERNETVIAWIFIALLOWIN
GPEOPLETOEMAILPHOTOSTOFRIENDSANDCOLLEAGUESDIRECTLYFROMTH
EIRCAMERASAMOREMUNDANEBUTWIDESPREADUSEOFWIFIISINCOMMUNIC

ATIONBETWEENCOMPUTERSANDPERIPHERALDEVICESSUCHASPRINTERSA
NDPROJECTORSTHEGREATADVANTAGEOFWIFIOVERWIREDNETWORKSISTH
ATITDOESNOTREQUIREWIRESTOCONNECTITTOANETWORKPOTENTIALLYWI
FIANDOTHERWIRELESSTECHNOLOGIESCOULDBEMADEAVAILABLEEVERYWH
ERETOEVERYONENOTONLYHELPINGABUSINESSPERSONONTHEMOVEBUTA
LSOREMOTECOMMUNITIESTHATMIGHTOTHERWISEWAITYEARSFORCABLES
TOREACHTHEMHOWDOESITWORKWIFIEQUIPMENTWORKSBYRADIOWAVES
WHICHHAVEAVERYWIDEANDINCREASINGLYSOUGHTAFTERRANGEOFFREQU
ENCIESIFTHEWORLDOFCOMMUNICATIONTECHNOLOGYISAWASHWITHACRO
NYMSTHERADIOWAVESPECTRUMISINCREASINGLYJAMMEDWITHSIGNALSAS
DIFFERENTKINDSOFDEVICESTRYTOCOMMUNICATEWITHEACHOTHEREXTRE
MELYLOWFREQUENCIESOFHERTZORCYCLESPERSECONDAREUSEDFORRA
DIOCOMMUNICATIONSWITHSUBMARINESTHEWAVELENGTHSCANBETHOUSA
NDSOFKILOMETRESINLENGTHINCONTRASTWIFIEQUIPMENTUSESRADIOWA
VESINTHEFREQUENCYRANGESTHERANGESARECLASSIFIEDBYTHEINTERNA
TIONALTELECOMMUNICATIONUNIONASSUPERHIGHFREQUENCYANDISMUCH
HIGHERTHANTHEFREQUENCYUSEDFORAMRADIOKILOHERTZSHORTWAVER
ADIOMEGAHERTZMHZANDFMRADIOANDTELEVISIONBROADCASTINGBOTHM
HZITISALSOGENERALLYALITTLEHIGHERTHANTHEFREQUENCYUSEDFORMO
BILEPHONESANDTWOWAYRADIOSMHZTOGHZTELSTRASNEWNEXTGSYSTEM
WHICHALLOWSHIGHSPEEDWIRELESSINTERNETCONNECTIONSOPERATESAT
MHZOTHERDEVICESTHATUSERADIOWAVESINTHESUPERHIGHFREQUENCYR
ANGEINCLUDEMICROWAVESAUTOMATICROLLERDOORSANDCORDLESSPHO
NESBLUETOOTHAFORMOFWIRELESSTECHNOLOGYNORMALLYUSEDFORVE
RYSHORTRANGECOMMUNICATIONBETWEENDEVICESSUCHASALAPTOPAND
APERSONALDIGITALASSISTANTPDAOPERATESATABOUTATTHEEPICENTREO
FACOMMONWIFISETUPINVOLVINGPERSONALORLAPTOPCOMPUTERSISAWIR
ELESSACCESSPOINTCONNECTEDBYHARDWIRETOTHEINTERNETAROUTERC
ONVERTSDIGITALINFORMATIONINTHEFORMOFSANDSINTORADIOWAVESAND
TRANSMITSTHESEVIAANANTENNAITCANALSORECEIVERADIOWAVESANDCO
NVERTTHESETODIGITALDATAWHICHITCANTHENSENDTOTHEINTERNETVIAIT
SHARDWIRECONNECTIONLAPTOPCOMPUTERSOROTHERDEVICESWITHINRA
NGEUSINGTHESAMEWIFIPROTOCOLCANCOMMUNICATEWITHTHEACCESSPO
INTANDTHROUGHITCONNECTTOTHEINTERNETTHEPROTOCOLISIMPORTANTI
FTHELAPTOPANDROUTERARETOCOMMUNICATEITISIMPORTANTTHATTHEYS
PEAKTHESAMELANGUAGECOMPATIBILITYBETWEENELECTRONICDEVICESIS
ONEOFTHEINDUSTRYSGREATCHALLENGESANDITHASBEENACHIEVEDINTHE
CURRENTGENERATIONOFWIFIDEVICESTHROUGHTHEADOPTIONOFASTANDA
RDDEVELOPEDBYTHEINSTITUTEOFELECTRICALANDELECTRONICSENGINEE
RSIEEETODEFINETHEWAYWIFIEQUIPMENTOPERATESTHISSTANDARDIEEEEA
CHAREAINWHICHWIFIISAVAILABLEISCALLEDAHOTSPOTBOXHOTSPOTSAND
MESHESWHEREISWIFIHEADINGWIFIHASBECOMEVERYPOPULARVERYQUICK
LYTOTHEPOINTTHATINCERTAINSECTORSOFTHEECONOMYITISALMOSTAPRE
REQUISITEFORDOINGBUSINESSSOMEHOTELSWOULDPROBABLYLOSECUST

OMIFTHEYDIDNTOFFERWIFITOTHEIRGUESTSWHOEXPECTTOBEABLETOLOG
ONBEFORETHEYNODOFFWIFILESSCOFFEESHOPSMIGHTBEBYPASSEDBYLA
PTOPTOTINGLATTEDRINKERSWANTINGTOCONNECTWHILETHEYCAFFEINAT
ETHENUMBEROFUSESTOWHICHWIFICOULDBEPUTISALMOSTLIMITLESSINTH
EHOMEELECTRICALEQUIPMENTSUCHASTHEREFRIGERATORTELEVISIONLIG
HTINGSYSTEMMICROWAVEANDSTEREOEQUIPMENTCOULDALLBELINKEDAN
DREGULATEDBYWIFITHETECHNOLOGYALSOHASEXCITINGPOSSIBILITIESINE
NVIRONMENTALSCIENCEBOXREMOTESENSORSANDTHEIRAPPLICATIONSBU
TPERHAPSTHESINGLEGREATESTADVANTAGEOFWIRELESSNETWORKSOVER
WIREDTECHNOLOGIESISTHATTHEYAREMOREFLEXIBLEABOUTTHEINFRASTR
UCTUREREQUIREDTOSETTHEMUPTHATSWHYCOMMUNITYGROUPSHAVELAT
CHEDONTOTHEMANDITISALSOWHYTHEYAREBEINGPURSUEDINDEVELOPIN
GCOUNTRIESWHERETHEYCANBEUSEDTOBYPASSTHEVERYEXPENSIVEBUSI
NESSOFLAYINGCABLESWIFITECHNOLOGYISNOTWITHOUTPROBLEMSSECUR
ITYBEINGONEOFTHEBIGGESTBOXSECURITYANDENCRYPTIONBUTFEWPEOP
LETHINKITISAPASSINGFADSOWHEREISWIFIHEADINGPREDICTINGTHEEVOLU
TIONOFINFORMATIONTECHNOLOGYISNOTEASYESPECIALLYGIVENITSCURR
ENTEXTRAORDINARYRATEOFCHANGETHISMONTHSBOOMPRODUCTMIGHTB
ENEXTMONTHSLANDFILLBUTAFEWTHINGSABOUTWIFISEEMCERTAINSPEED
SWILLINCREASETHERANGEOFUSESTOWHICHITISPUTWILLBROADENANDITS
AVAILABILITYWILLCONTINUETOSPREADITWILLALSOFACEMORECOMPETITIO
NKEEPINGTUNEDTHEARRAYOFWIRELESSTECHNOLOGYALREADYINUSECAN
BECONFUSINGCONSUMERSHAVEAHUGERANGEOFCHOICESBUTOFTENINSU
FFICIENTINFORMATIONONWHICHTOBASETHEIRPURCHASINGDECISIONSCA
NYOURLAPTOPDOWIFIANDWIMAXANDDOESITNEEDTOWHATDOESTHESHOP
ASSISTANTMEANWHENSHEASKSIFYOUWANTAPDAWITHBLUETOOTHDOYOU
NEEDAWIFIRICECOOKERTHEPROLIFERATIONOFTHETECHNOLOGYDOESHAV
EONEADVANTAGEIFYOUDONTUNDERSTANDITANDWANTTOFINDOUTWHATIT
ALLMEANSYOUCANATLEASTRESEARCHITFROMALMOSTANYWHERE

По данному тексту частота каждой буквы выглядит так:

{'A': '7 %', 'B': '2 %', 'C': '4 %', 'D': '3 %', 'E': '13 %', 'F': '2 %', 'G': '2 %', 'H': '5 %', 'I': '9 %', 'J': '0 %', 'K': '0 %', 'L': '4 %', 'M': '2 %', 'N': '7 %', 'O': '8 %', 'P': '2 %', 'Q': '0 %', 'R': '5 %', 'S': '7 %', 'T': '9 %', 'U': '3 %', 'V': '1 %', 'W': '3 %', 'X': '0 %', 'Y': '2 %', 'Z': '0 %'}

(немного похоже на ту частоту, которая была приведена ранее)

С помощью шифра простой замены (1.py) зашифруем этот текст (рисунок 11):

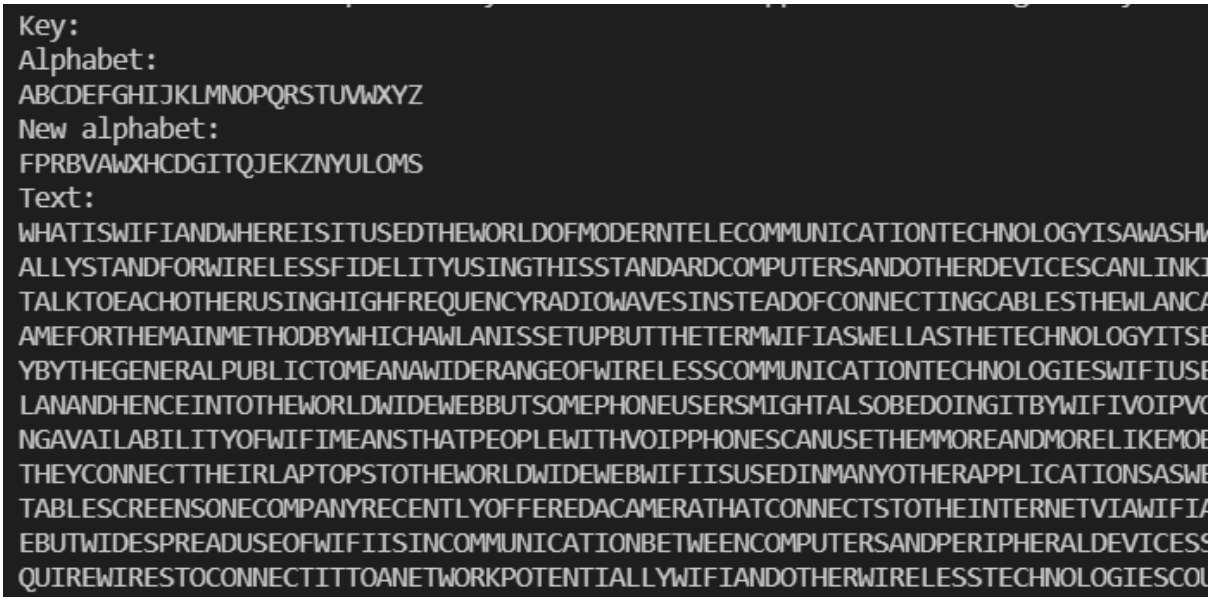

Рисунок 11 - зашифрование открытого текста

Частота встречаемости букв в шифртексте:

{'A': '2 %', 'B': '3 %', 'C': '0 %', 'D': '0 %', 'E': '0 %', 'F': '7 %', 'G': '4 %', 'H': '9 %', 'I': '2 %', 'J': '2 %', 'K': '5 %', 'L': '3 %', 'M': '2 %', 'N': '9 %', 'O': '0 %', 'P': '2 %', 'Q': '8 %', 'R': '4 %', 'S': '0 %', 'T': '7 %', 'U': '1 %', 'V': '13 %', 'W': '2 %', 'X': '5 %', 'Y': '3 %', 'Z': '7 %'}

Анализируя частоту встречаемости символов в тексте и сопоставляя ее с частотой встречаемости оригинальных букв, можем сказать, что E=>V

H и N по 9%, это могут быть A и T

Сделаю округление до сотых:

{'A': '2.43 %', 'B': '3.21 %', 'C': '0.04 %', 'D': '0.43 %', 'E': '0.32 %', 'F': '7.24 %', 'G': '3.87 %', 'H': '8.63 %', 'I': '2.41 %', 'J': '2.23 %', 'K': '5.49 %', 'L': '2.69 %', 'M': '1.66 %', 'N': '8.95 %', 'O': '0.21 %', 'P': '1.59 %', 'Q': '7.85 %', 'R': '3.85 %', 'S': '0.14 %', 'T': '7.14 %', 'U': '1.23 %', 'V': '12.5 %', 'W': '1.87 %', 'X': '4.74 %', 'Y': '2.68 %', 'Z': '6.58 %'}

Так как T встречается чаще A, то можно предположить, что T=>N, A=>H

Для простоты анализа отсортируем словарь по значениям:

{'C': '0.04 %', 'S': '0.14 %', 'O': '0.21 %', 'E': '0.32 %', 'D': '0.43 %', 'U': '1.23 %', 'P': '1.59 %', 'M': '1.66 %', 'W': '1.87 %', 'J': '2.23 %', 'I': '2.41 %', 'A': '2.43 %', 'Y': '2.68 %', 'L': '2.69 %', 'B': '3.21 %', 'R': '3.85 %', 'G': '3.87 %', 'X': '4.74 %', 'K': '5.49 %', 'Z': '6.58 %', 'T': '7.14 %', 'F': '7.24 %', 'Q': '7.85 %', 'H': '8.63 %', 'N': '8.95 %', 'V': '12.5 %'}

И добавим такой вывод в программе: сначала словарь с частотой символов в тексте и потом с частотой символов, которая должна быть:

{'C': 0.04, 'S': 0.14, 'O': 0.21, 'E': 0.32, 'D': 0.43, 'U': 1.23, 'P': 1.59, 'M': 1.66, 'W': 1.87, 'J': 2.23, 'I': 2.41, 'A': 2.43, 'Y': 2.68, 'L': 2.69, 'B': 3.21, 'R': 3.85, 'G': 3.87, 'X': 4.74, 'K': 5.49, 'Z': 6.58, 'T': 7.14, 'F': 7.24, 'Q': 7.85, 'H': 8.63, 'N': 8.95, 'V': 12.5}

{'Z': 0.05, 'Q': 0.1, 'J': 0.15, 'X': 0.15, 'K': 0.77, 'V': 0.98, 'B': 1.49, 'P': 1.93, 'Y': 1.97, 'G': 2.02, 'F': 2.23, 'W': 2.36, 'M': 2.41, 'U': 2.76, 'C': 2.78, 'L': 4.03, 'D': 4.35, 'R': 5.99, 'H': 6.09, 'S': 6.33, 'N': 6.75, 'I': 6.97, 'O': 7.51, 'A': 8.17, 'T': 9.06, 'E': 12.7}

Если так идти по убыванию, то итоговая подстановка будет
ABCDEFGHIJKLMNOPQRSTUVWXYZ
HPBGVIJKFODRYTQMSXZNLUAEWC (с помощью частотного криптоанализа)
FPRBVAWXHCDGITQJEKZNYULOMS (оригинальный ключ)
Далеко не все буквы совпали, но остальные буквы можно будет “доугадывать” и примерно понять текст. Чем больше текст, тем лучше будет работать такой вид анализа. Более сложно различать буквы с близкой частотой встречаемости.
В данном примере:
WHATISWIFI - исходный
LXFNHZLHAH - зашифрованный с помощью ключа
URITASUAWA - примерная расшифровка частотным криптоанализом (в данном случае в таком фрагменте текста почти все буквы редко встречаются и имеют схожие частоты с другими буквами, что усложняет расшифровку)
Можно перебрать близкие частоты с частотой буквы U, дойти до буквы W, тогда предпоследний символ будет не W:
WRITASWA*A
Таким же образом можно вместо бывшего W подставить соседнее F:
WRITASWAFA
Аналогичным образом можно будет дойти до подстановки вместо A I (и потому что можно додуматься до того, что для осмысленных слов гласные буквы подойдут больше всего):
WR*TISWIFI (из-за такой подстановки мы потеряли I)
Таким же образом можно дальше дорасшифровать этот фрагмент и таким образом составить полный ключ шифрования, можно догадаться, что первое слово будет WHAT, такие догадки могут быстрее расшифровать текст, в отличие от простого частотного криптоанализа.

Для аффинного шифра:
{'G': '0.04 %', 'C': '0.14 %', 'W': '0.21 %', 'B': '0.32 %', 'J': '0.43 %', 'Q': '1.23 %', 'I': '1.59 %', 'Z': '1.66 %', 'X': '1.87 %', 'Y': '2.23 %', 'P': '2.41 %', 'U': '2.43 %', 'N': '2.68 %', 'T': '2.69 %', 'O': '3.21 %', 'L': '3.85 %', 'M': '3.87 %', 'A': '4.74 %', 'E': '5.49 %', 'H': '6.58 %', 'S': '7.14 %', 'F': '7.24 %', 'V': '7.85 %', 'D': '8.63 %', 'K': '8.95 %', 'R': '12.5 %'}

{'G': 0.04, 'C': 0.14, 'W': 0.21, 'B': 0.32, 'J': 0.43, 'Q': 1.23, 'I': 1.59, 'Z': 1.66, 'X': 1.87, 'Y': 2.23, 'P': 2.41, 'U': 2.43, 'N': 2.68, 'T': 2.69, 'O': 3.21, 'L': 3.85, 'M': 3.87, 'A': 4.74, 'E': 5.49, 'H': 6.58, 'S': 7.14, 'F': 7.24, 'V': 7.85, 'D': 8.63, 'K': 8.95, 'R': 12.5} - шифртекст
{'Z': 0.05, 'Q': 0.1, 'J': 0.15, 'X': 0.15, 'K': 0.77, 'V': 0.98, 'B': 1.49, 'P': 1.93, 'Y': 1.97, 'G': 2.02, 'F': 2.23, 'W': 2.36, 'M': 2.41, 'U': 2.76, 'C': 2.78, 'L': 4.03, 'D': 4.35, 'R': 5.99, 'H': 6.09, 'S': 6.33, 'N': 6.75, 'I': 6.97, 'O': 7.51, 'A': 8.17, 'T': 9.06, 'E': 12.7} - должно быть примерное у открытого текста
Попытаемся расшифровать кусочек шифротекста:
TAFKDHTDUDFSOTARE - зашифрованное

UHOTANUAWAOICUHES - расшифрованное с помощьючастотного анализа
Можно поменять U на W => WHOTANWA*AOICWHES; слово WHOT похоже на WHAT => WHAT*NW***AICWHES => … => WHATISWIFIANDWHER

2)
Кроме полного частотного анализа можно расшифровать какое-то слово и по этим буквам определить ключ с помощью метода “грубой силы” (полным перебором)

С помощью полного перебора мы имеем (рисунок 12):

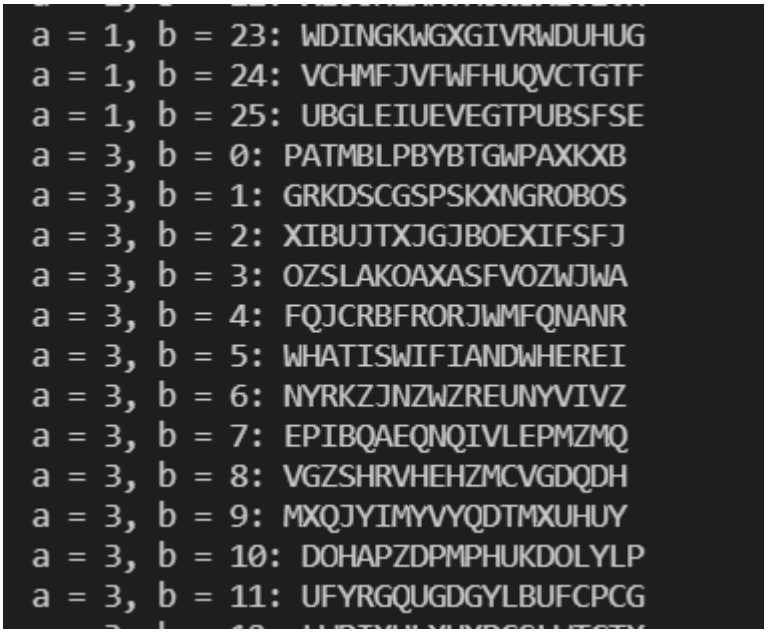

Рисунок 12 - частичный результат полного перебора ключей в аффинном шифре
Нашли ключ: a = 3, b = 5. Другие варианты тоже содержат слова, но помимо них есть какие-то непонятные => возникает предположение: неверные ключи
Найдя ключ, можно полностью расшифровать текст

Полный перебор подходит и для рекуррентного аффинного шифра, который уже не взломать с помощью частотного анализа (потому что изменяются ключи для каждого символа)
Результат программы 6.py (полный перебор для аффинного рекуррентного шифра) представлен на рисунке 13:

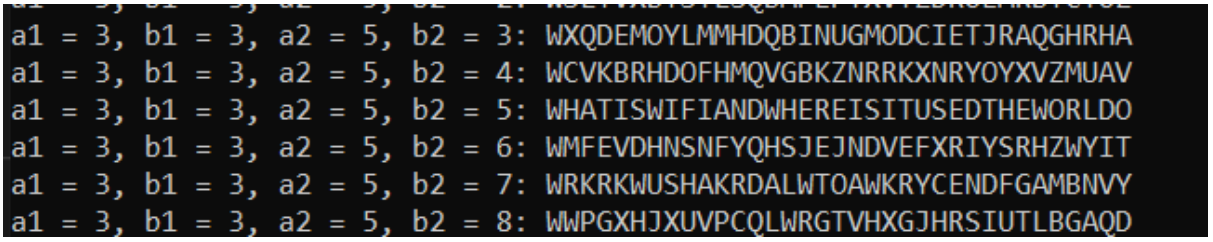

Рисунок 13 - частичный результат полного перебора аффинного рекуррентного шифра

Проверка ключа a1 = 3, b1 = 3, a2 = 5, b2 = 5 (рисунок 14):

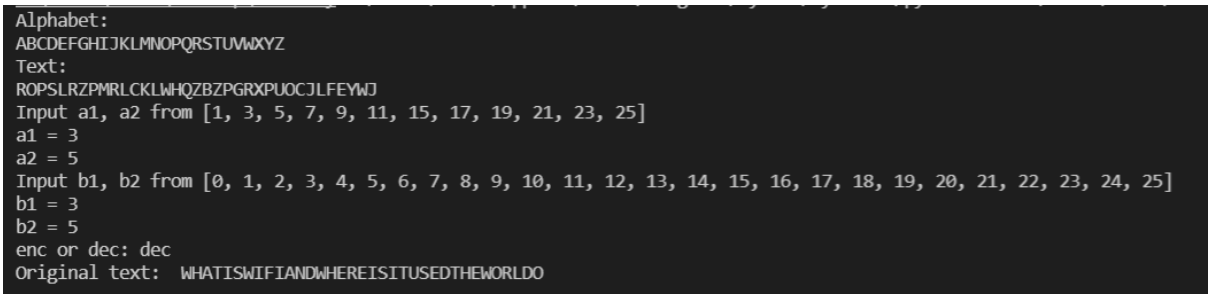

Рисунок 14 - проверка ключа, найденного с помощью метода “грубой силы”

Выводы о проделанной работе

Данная работа помогла лучше понять, как работает шифр простой замены (1.py), аффинный (2.py) и аффинный рекуррентный (3.py) шифры, а также понять, как можно взламывать такие шифры с помощью криптоанализа (частотный анализ - 4.py, полный перебор в аффинном шифре - 5.py, в аффинном рекуррентном шифре - 6.py)

Для наибольшей эффективности частотного анализа нужно брать как можно больше шифротекст.

Плюсом полного перебора является простота взлома зашифрованного текста. Минус же состоит в затрате большого количества времени. Таким методом проще всего взламывать аффинный шифр (перебор содержит 26*12 различных комбинаций для английского алфавита), потом идет аффинный рекуррентный шифр (26*12*26*12) и самый долгий криптоанализ будет у шифра простой замены (26!).