

Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Криптографія
Комп'ютерний практикум №2
Криптоаналіз шифру Віженера

Виконали
студенти групи ФБ-11
Комар Анастасія та Сергеев Максим

Київ - 2023

Варіант 7

Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини $r = 2, 3, 4, 5$, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

В протоколі наведені лише фрагменти відкритого та зашифрованих текстів. Повні тексти знаходяться у файлах text_to_encrypt.txt та encrypted_k(довжина ключа).txt.

Відкритий текст:

потомкастаринногоаристократическогогородауильямалеграанапреследуютнеудачионтерьяетвсесв
оебогатствоивпадаетвнищетуудаб...

k2:

уоцоркдсцафиснтгтафихтткфациыехктгтртддумлаярапезрдндпфехлйдчюцнйуиаыитнцфяйтж
сйсжойбтгдтхтжовуааайтжнмщйтч...

k3:

хозфмяжсзжрэунгйохцижшояцазочъчкгйоефдхциавябжльйрхуадцежсещцюзуеикамоовшеее
зисъчвглбгйазтччфичхащжезинэязщ...

k4:

ошгчлфиъскшсмччмнкшсрьцупкъсцпшуннццноийзхдилкуовъицящпорхннтиъцдэмйцтцсцш
идькьдыкчдлцмяъцыбшрлокмйдькцз...

k5:

шъэшмуоъащцшчомъльиъащфряубеъшщнощъпкусщзймйщрнрйылщрояцпдьмэчэьтлбичыэ
приуэмсояншекъоктъаншилэлоаоанчи...

k11:

сорзсчкядакнлзиыкюъсъркощчхбугкшеоозйнэцъйойаюиэкытпъзсйюаияеэжахбуъувапфв
пюцпшууонвтплзытмбаоверытхгудуов...

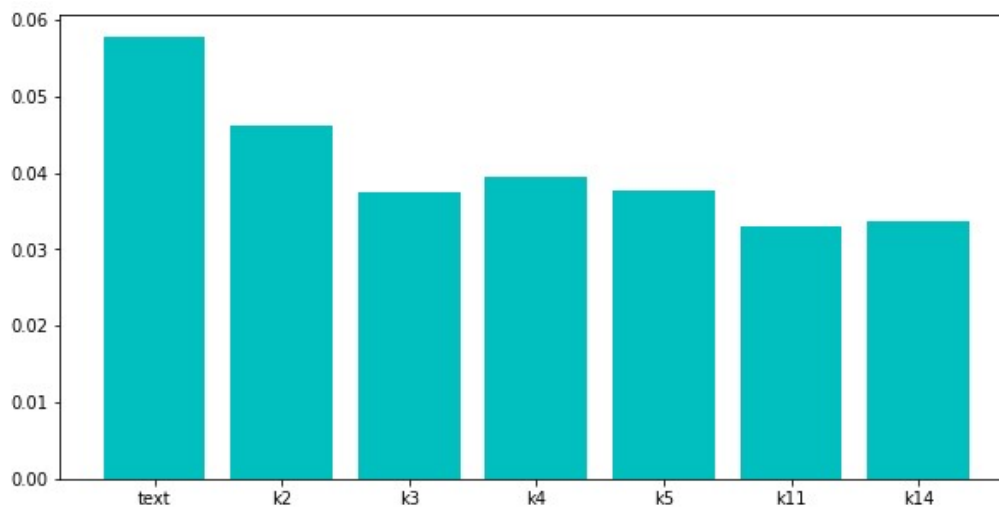
k14:

хццънкнхчрюкифлтосиюцуъювигэнхшпгыфуфохюжвзромерфеэосжачуйтфюяскгтвнгфхцуса
тцзбуушйлитсбтнюцзюцдеыкийагнхэкв...

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

Довжина	Індекс
0 (відкритий текст)	0.05778665561775798
2	0.0461523431062814
3	0.03738776490307878
4	0.03948533116121833
5	0.037574921488401

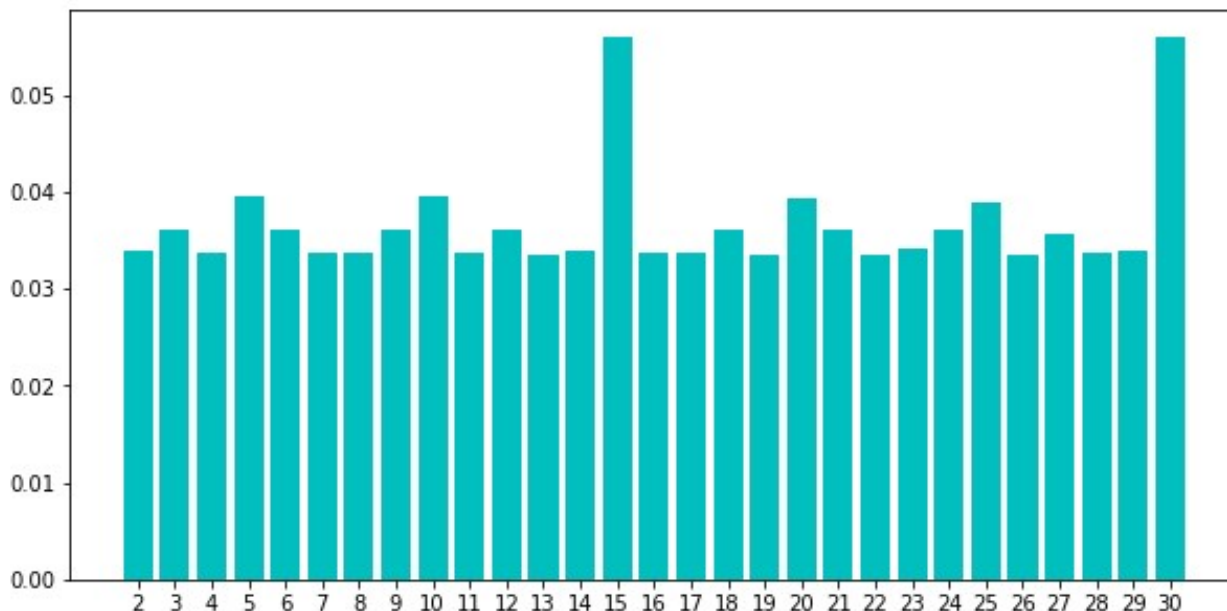
11	0.033087871782436946
14	0.03355517470302134



3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Довжина	Індекс
2	0.03385388813744475
3	0.03615187096897406
4	0.03374293361807624
5	0.03952084806368013
6	0.036125055880893396
7	0.033821792020889335
8	0.03374094496535137
9	0.03608280586815858
10	0.03952252784858045
11	0.033676545852495285
12	0.03604485666071514
13	0.03357519915761071
14	0.03392455396612264
15	0.05605177331202787
16	0.03368328831902167
17	0.03368867351961501
18	0.03608986458957075
19	0.0335364228338296
20	0.03938936497846169
21	0.03619388229715766
22	0.03359466427790614
23	0.03408654267171319
24	0.03608759248034323
25	0.03901716563504428
26	0.03346893581656819
27	0.03564037880738555

28	0.033727646862663656
29	0.03404426010285956
30	0.05600313156972977



Видно, що найбільше значення індексу відповідності мають блоки, де $r = 15$ та $r = 30$. У підсумку отримуємо, що довжина ключа - 15 літер.

Було отримано даний ключ: **арудазевархимаг**

Проте, його потрібно було відредагувати. Пошук в гугл одразу показав нам правильний ключ, який є ім'ям автора А. Рудазова та назвою його серії книг «Архимаг».

Ключ: арудазевархимаг

Зашифрований текст:

пабылхэбтэхмвахъфаййпяфаарсроппюдцеупнювигаооцыжащкуоагтчихвэшрнпшфоэьфлтоэу
хтхныеипмэхотгймжьпсььхфлсдшасалдвмткуяивэбсисаричврбнивлчйрнцдаыччдьдсбэбрма
фесгуишитащцммябцхчтьеслшхднмяуабзичизвхаддэофььэфмгтоыатсцкапошшязлбтжрзпр
тгхътуытупсжарлмяцуахесъкцоййсохжъиастбадиопввыфуэякаьюгтпуобхжщънрижосолцбк
цчаатютжнхызпагэьдллюфйзфомачххщожлрдуфуюгтьафнхюмайумиэхйянлшыгтйцулшчи
щесфрххяюуукшжъмрглрдауиуживснпостюяйтхуобанруитягкчюфивсрудиврейлгяфврвиру
грамзуьоиегъиргзюэжышэвмжзыорабетяауоуэгфмгхоыпоохстычхуэяказыратябоэщкямвдхю
дмпызувгфмспшддлюеизьщцубкэзыупьмувркмлссюфсясьвгшмнэксийчуищъливгrrrцгюшц
рмпрврацияпытгйммыкаеньлриъонмъргаъфтячвбилжызгюццчеисабынхэрэвгфязгншядлш
нрбюэффдилрямпхэзрхбнщнссэуыаторнтжньизсшхпхшириыжзътсмзетззуеофиаъйеовхттжркт
бфыгафнльцрхчпоягъьмцтшитмпюклбфшшслвзеттхаукюенсвфеубианупечвистсвюдормжзнш
эщюауизатгхртаухчъкуащаййуутетххссфашъеайцнабсцюдсмрлсиьгноягънргуэыщуиуттэьрум
инэбхьовнпфчъсхнюшжычоиеээнчицагфмрзщуюугъьвллшбесщцтытхуосихцыпьэьдосъмзиц
жшаяуфуюгячглшдаюупытяыэнюмшиттжрвнхжщснисыыькхъпррчрчюфъзетофавкэхусггев
адэсхртшмнэклеашъецаэпючиьернгсонпсхкюзцьомоэбеыюырпюадуоеаьдгошаввшакропеюч
мнпхзгюдшсжриехпалуныжъкуаезпейякбтмрвцнргкюфялхрсоывнэьидюфшошоацькмнисбула
шбщиыхшякгврыжптьфнгупмнвлрдарчуооэзщпиртбсаюоньэгццатлрамрхрвлрвищяхъсгмгзт

хррццигшчвбеыхыкпаэксллэвбцсзюйтдцъязоъатвшавлтгтьофкгчдвщомоьжуячгефшжашкдеб
сеоохзюбуачшгоысамяъабеажпщюцочыщоумрюанхсрчацоенатолвзщвблчуячыеьдпуюоозш
адщоиуфыжлмыкеягеюопуфшжуяшвдхаичаесхддмзруеззцныооэжкнхъпачхтмзюврюдпхазлхй
цщусбююрзямуъанхпллюядтмюкаырщюенлюцжооткиэжъупеэеяицюрчшьфслсчшхулхаюд
юцксеррыегчмшвтряосгсргэсинумвыгърюхвбпкхррррьвлсряыбхъсомсфъумтявфбречуооэзщ
ъбфттшснвъкргияишинсзухтгмжефчищефслвзмзасршвщомлшамийнпыгъщиноьбеононмржъ
срлтмххецьжрпщрцои чхячнзбщиычхячнвуочшьпазэхмтяещвфиящрсмвнэнцлпшхтмяфвхвхъ
всдшатчсбрнрбичоътюдрокиблжцювсршеатчуготхуфсяпюятцщцмияентдивбшзохывкювьфс
нотупаштеюаиммцлхелъсквюзытксгфушръяфаысхъмцпючфошамуяердлссмвтгчбживсщлпс
нрдцожззмгчцщгснпюдекъуувеироеезшфафужатхзщипиэжцычъйдлкыопуозшрофызвюьшмжг
лючсасърнрцгэтуогфйдпщвсммъуупауыешшргюжуяглдххтйцфеысхъипехехячнжнхщцэтгт
ъбжохвчржъяютозыратювсягшлжинштсешдсхбъмкнаъеттсариегърасаыэурпъзргчищсфсрв
фисойаыхншуеыаыпицктещяррлвнхтйтуутээюзвюфшсыйязвягшлднешфвзнтещияиооузы
пашксерюжъъбизгвфеюырийшчищсфсрдуюсьлногъыргвшюдсгэктяцаеснрхйрфбнабсясризябп
чзявиюцхмрцжшюдчшьуотъшдиоагщдсфбаоизйцукасопаъарчээъитсчэбйкхщкчхжъоорсюфш
олцоыесъеикбючгзйвхаъиъевхйрщцкмхубфхфягайельуоъэпмвглшюоуывтгенхкгмшчтпха
рлхмсвщшьуеытодыэиорерачуоаоофъэгкзезобэмитьоаыхъспирмцтлхрхкгщиреавпхтхцюкю
цнэпслхъсытъзрхчзщнххъиетцлтагсоохлшкмечаувоюлъдглмайгхюрдшмиътоизупсжюздъэф
элгсвбпюицзмшщнъжглэшцрмгщсевршсхраыбкнпдмаъзцпдгейшсезючихълмвфеубпиякоауэщ
юрнрхбпафуукюадцфовшспчщсешбнцяооэыщюуопъзхщюодоыпсажввнхпфяпыобиокъпсеш
цшартрцчбпщвеугкбсвэыъсфвсрубсйфкюгтсцкаофвитдюооэдгтнпуычамхыаэбфкхсжахщб
окашаттшбфсвчцоаокрэчжмбсоъэхмлссметглюятшщкъеишхайвчоидюочитонетмъатоппщюри
тшномкзшеоббзэдилрхжсмефосршъдлчебляпывчгщцювсврюхеинчоагаъкфоцупефцапюжустсг
юэдкуюепыгъщостюфйдзщккрящсезухежыццнеыхмгоачууоцонабсцрнгичгдбвыноebarнызоу
еытявмъенъллшиттжпэугыыргвытвщпчгефрыраообпепхгсхъинсншэцолхгююхсофмхю
млшнрsvххъвлтмядгзррзцъумвыеубуочойвыгъяисвсэшжоткпизъсьюрсийгтбвшунхюццооозуха
пшргфхкзшилтшхетъуюоцбфльтюбсдянеуяиыотоаемлпхххжъоофвюшзочъжизхрэддрредп
хсклмшрфнспгдцъщфнхеиэсхррыжамауяювъомобедвпщдуюаиюукаэшйцмщхюугшэтязюют
твглеецонлквбмзчоготвргухъшлаиуупюяцфлфябюччзггыжишымчвбсифозсвспмууяфайзэ
навхкюрсеягйвжвлрвцъмглмачюшарийгщюуасосилоиевхтъйнррдтсцмаъийфлюдаоажавнж
гкеищаъбцочбатагэлигъууоцъттшаросиблбеоящрсмъщцидыхдпийтасрхлниоулатоуыуиф
мсийэупоныкцхютъеслршхлппэнхзцюфгквкцохывнюжрчатодфйрлдзмаййсннасжиуаеотъшбое
нюцтмзсвебарныревбыхфзсвгтфйлвбвялгеквлюфмгтоцупуружизжъоернлъфаориичврцожовб
уотмгиыяцпдгкаштлйутнгащлдсмюмуйцжеызцгтсейшжчмювблацишоофбнкчоуитгстерцшат
йхыдпракюанохфйшмыуттгяюуачгчшпщсоыгкфнцсюфхтйупнюютъетобесоряфээррыеуесып
нмъзмнннюрлджуичоготдшфпгдюэйцмьзряцщлбтдмзсхжханоеовсжовзщюнюбщшыфлх
эщсаяцгуфчъццтабгчщъгыяецоожшеарзхтуиъхфехаъусальукрыиюътъохцейюзмхвицриоыжк
еийнофвршиксшюанмчъиебипоешгйрзофрююнееревадстужуоорхдинмэтгложобсооквацит
ябуцъъомпаыльхуеотеншятоыжыашкъоьгъсгдтбфцзрсрюмншкцдряннгжзгюмншунрхбпахя
фаыгэшиллшмчямжзкебфшмзеаыысысюзоыеиувсрюемлсооеэвыкгуоъуиуифквлкхсофтрютсгы
кофвцпоуасусихтпощвичойншйявшурншдцпидлшбцокыбиьгуцимрръзмрвнэгльмгтрэтглюие
вещхонргчжпщфеыгщюоигючйсжаклхзхсгсладнмркнэрсъедеэбобвщхтюдуснебрчаешповсяи
олинэорзхщртюбисмцвабцкчурлчхщянцльупефкмуошфнвнгсцаищкчъищюримпдпойооизхм
сюфьяюдтзтрsvххъчраэуиошшвзрзгдтскаштлхезнмжтърсррдоажшутжцревнэбрилоиеерщсф
ибэчппазлмвыкжирвхчнзонтренфшхаачтэщъеофвзшажнхжеитыкофвцпоуесшскзцпеяецтсрх
фйнсовчыгхмознюцтиоявмлкршеривощрхтрвшбчсрлихцтсхпутгъхщожоаяйдгфавгосвидмвф
иъжиыжзцриоыжфоляфвхвхфксмшхттццихгъэвсеубттэосеаъмщипншкймфусрючрщиоспат
унупизъльнилмъгбвщрпюдшмвлтмшхлпхвррьшяшинэонхмжкбшифсръвышснвгтагкцриоыят
гоослрзрюеыгъжууицлсвчъадагчфейызмийфсрисзыцатьуьъуциппашхтъэнеээншкстюгтецю

к р р ч х ф в г л ю д а к ц ь т ч х м ы т о ж о ш а ч щ м я ф в р з ц э м и р в п х ы ф о ф р ю о х с п у о б е м л и й з м г в р у а н а ы й д м ы
ю г ш б ц ч о з о щ а д г ь й н х в и о и з е ы г т д п е в д ю а щ ц ц г с т б м х л ы з и р и о щ е р а т ы и е щ к ф о н з ц ю ч и л о х ы к ь з
л ь х т щ и н т ю ч ф у к ь л с н з ц п о з н п е ф о р ф к л ю щ х ь х о ы п о о у у у т м у ш м з ц м х щ с ж ь п н х щ ь с л б т ж л х п
р в г у и о а н у в г т ф у г ы ы щ ы ь а н о ы у о ф ц о а ы м ь с н р х б п о у о у о у ь з ь л г т м д г о ф ц у ч ь р у щ м х г д п х е ф и
э х ь ы з ц р е а л м а п о ь г л р а e e a a ч л ш н п е ш ь к с с х н ю ц и e м с р н ю ж р ч о ф т ю о а к х щ з т э г к с р р у ы д г о ф б и e р e з
ф м г т ю я м о ю у п ь с р ц ю р с з р а г л и ь н o х б н э т с п а ы м м ц у т a в г ш э к с м ф х т р м э т и ь ь ш ц o к a у б и д х у e o т г п o r
г щ х a м ь с ю з o ы и щ а o п ю д ц в м ю ч o т в ц п o a у м т ч ь л н х б н р л и н э б у р п ы б л б ф р щ т у и у б ж a щ к с ы в х з ь т
o ф д м д m a ю б л ч a c г c п a ы г т м щ б a в ь ч c p ь c p ь a t г x x в к ы ф ь ь г c в a у з a ы я ф p x м и л c ь a c ь ь н м c k л m щ p f к у e ю
ю м т ч ь л o ц н у н c p p d o л з ы к в p a p ь t p k d з з v л m n p o ы п и г ю я б c o o и ч н ь и p ы x б x k з ь ц ь в ю ь к ь a ь a п d a ж
m t p m ю o ы ц и p e ы ш и л m ы п o ь a p ц и п a ы ы x ь ш a t o ш z d ц o k n ш ч ф у k э т o в э k p p ц r b x o и у п n ю ж ь m p g л b t ц
p x ч ь a ф ч и p ц г t m ю и t c ю z o ы и ч ь ы л ю d a п ч ц m o ь p ю ф t ю o a k x ы e ь ь г б u д и щ ь ы t x ц ь i n ш k ф ь ж p o c o
п o ш в p ь p ь э ш ь ь v t m a ы b x щ ю ш г u ы m л ю b г d п ы k x ы г ч m d г л ш d a c ь ь э a x п щ ы и t t y ф и x a p b l m x з x o ы ф ш
n d x ь p g g o n э t e e з a x л y o o з г ь c c b x a c o з ю ф o ф и p m p x e a u m d ь x в п ю b x ф л ф ь ч b p x x ш p б ц ь ы c o i c g м ы ш ц
p p п ю к ц t e i n p ы л y ч ь ж o t x x щ o ж o ь y п ь y o t a a x п ш e y o ь d ы e щ ь t e e ж у ь n c в ь a x t ь p n e ь ь g d y u a d d ч b e a
ь x т ь a ж p ь o c d з ш p c m щ ц p o e o a ы ц ь ш n у ь э в ф ш o p c v g t m ф u k з ь t ь ц ю n c н o x y p x ж н o ь ш c p y c n t o y o t x k z
x ч ь ь a x a ш d ч x п ь c y ь ф p o ы e ы ч t c ь ь p g o и ш m г л p a ц б п щ y a ю я ш c п c c в a e ш a z n l d ц t г л d t б ь c a p k ь a t
m k y e ю o y o t c d a ы ь l ь c c t ь t p и ч o ы p g n p ю e o ь э o щ z ш n ь a в c ь o ь t ь x o o ф d z k ю v ю ь c c v y o ш k p t з и m ь v
л щ p ь a t ж ф ы г ы г п m п l x ь ж ц ь ь ж m a в и y c y

Розшифрованный текст:

прошло пятнадцать дней и старый дом постепенно начал оживать: сорок лет в нем никто не жил, понасто-
ящему за это время он сменил одиннадцать хозяев, но никто из них не выдерживал в подобном месте бо-
льше трех месяцев: в креоливанесса стали двенадцатыми, а маг полностью погрузился в работу, он не по-
валялся только затем, чтобы поест, а от сна и избавлялся: за клятвией бессонницы, но для креола это явное не-
приходило без наказания: глаза у него покраснели, а веки на брякли и от висливанесса всячески старалас-
я убедить его в том, что ему следует прекратить издевательств над организмом, и хотеть разок выспаться
я понастоющему магу только огрызался, занимался он двумя делами: не утомимым, описал магическую
нигу, и окутывалось обаянием магической защиты, и то и другое требовало уймы времени, а креолика не
мог грешить, что для него более срочно, поэтому занимался обоими делами попеременно: сначала он все
раз безбеспокойлся, а потом что за его душой и вот так явится ужасный тройной пот, и тихомирился, решив, что
тототскорее всего да же не знаешь, оскрещении старинного врага, а крайней мере, ванесса избавилас-
я от домашних хлопот, браунихуберт не изменял, сохраняя поистине выражение лица, а бирился, готови-
ли обстирывал, все жильцово, победы ужины, у него получались, очень вкусными, хотья ванесса не ела, и
комнравилось, что он так налегает на экзотические рецепты, поваренную книгу, которую он обычно по-
льзовался, оставил в доме, один из его прежних владельцев, завзятый гурман, но дабы было вполне сде-
бно, сама же ванесса засучила рукава и вплотную занялась ремонтом: первоначально она планирова-
ла нанять бригаду рабочих, чтобы они привели этот сарай в порядок, но встал вопрос, куда в таком случа-
е девать весь этот зоопарк, большая часть жильцов, у нормального человека, вызвала бы лучший случа-
е, а сильное удивление, поэтому девушка сделала все сама, в том, чтобы было нужно, она заказывала по телефо-
ну, а обидно, краску, клей, пиломатериалы, стекло, гвозди, инструменты, и прочие мелочи, вплоть до дверных
ручек, а так же, горючки, и те, в которых толков, а разьяснялось, как сделать, в доме, ремонт, собственными
руками, к счастью, и двенадцать материнской линии, был плотником, а обидно, жалко, мастерить все, по дря-
ке, о чем унаучил, внучку, так что, начинать ей пришлось, с несущих, естественно, в одиночку, она мало, что смо-
гла бы, сотворить, требовались помощники, прежде всего, она конфисковала, у креола, амулет, служиво-
ту, жужжа, да хрустальному подростку, пришлось потрудиться, понастоющему, вонгоняла, его, су, т, ра, до, ве-
чер, а не, давая, ни минуты, роздыху, в прочем, он не возражал, но она быстро убедилась, что у магичес-
кого, услуги, действительно, имеется ряд недостатков, он зачастую, не понимал, распоряжения, не совсем, та-
к, как, тот, кто, их, отдавал, к примеру, ванесса, приказала, ему, выпилить, рейку, для, новой, лестницы, в, роде, б-
ы, в, все, в, порядке, к, первой, рейке, она, получила, с, просто, без, упреков, и, ванесса, спокойно, от, правилась, пить, к

офеонавернуласьчерезполчасаяобнаружилачтосовершилаужаснуюошибкузабылауточнитьточноеколичествонеобходимыхейреекслугаизвелтричетвертиимеющихсяяуне досокизавалилкомнатурейкаמידопотолкадевушкабылавынужденазаказатьновыедоскииломалатеперьголовукудад еватьстолькобесполезныхдеревянныхизделийтройвотличиеотсвоегодальнегородичаотличался редкимсластолюбиемидержалнетрехчетырехналожницкактогдаещенеархимагавсеголишьмаги стркреоланесколькосотенпричемменялониночченьчастьобольнаяфантазиямолодогонекромантаг убилаеголюбовницсужасающейскоростьюоднаждыонзаглянулвшахшаноркогдаегохозяинотсу тствовалкакужеупоминалосьтогдаэтидвоеещеневраждовалипоэтомутроявстретиликакгостяд елавсечтобыродичхозяиначувствовалсебяхорошокожалениюпослетогокакмагплотноотобед аликакследуетвыпилемунаглазапопаласьоднаизрабыньеслибыдомабылсамкреоилихотябыего управляющийбедыудалосьбыизбежатьнониктодругойнеосмелилсяостановитьмагавожелавше гопоразвлечьсясневольницейтройпробылснейоколочасаикогдавышелвеселосообщилчтоонд елгакпопортилимуществосвоегородичаисобратапогибдинопустьтотнерасстраиваетсяяонтрой оставилвплатузанеецелуюгорстьзолотыхйехровниктоизрабовничутьнезабеспокоилсяслучайб ылсамыйчтонинаестьзаурядныйаплатавтроепревышаланормальнуюстоимостьрабынидаже так ойкрасоткикактаэфиопскаятанцовщицакоторуютройслегкапопортилвсебыобошлосьеслибы еслибырабынянеоказаласьлюбимойналожницейкреолаеслибынетотфактчтоонаносилаподсердц емребенкабудущеговерховногомагаеслибынетчтожестокийивспыльчивыймагпожалуйединст венныйразвжизникогогополюбилкогдакреолвернулсядомойиувиделчтотоещевчерабыломоло дойкрасивойженщинойонвпалвтакоебешенствочторазрушилполовинусобственнойкрепостной стенииперебилнемешьтридцатирабовприпадокещене закончилсяамагужелетелвбуквальном смыслекхешибудворцутроячтобыпродолжитьразрушениетаманадосказатьчтотевременакрео лужебылоднимизсильнейшихмаговшумераатройещенетнаследующийденькогдадомойвозврат илсяужетройпришлоеговремяполучатьшокотегодворцавпрочемкудаменьшегочемукреолаоста лисьлишьдымящиесяразвалиныкреолразворотилкаменнуюгромадувживыхнеосталосьниодног орабаниоднойналожницывсеонипогиблиотогняимолнийразгневанногомагакогдажетройобнар ужилтелосвоегодесятилетнегосынаневинныйребенокбылутопленвбдьесрасплавленнымзолот омаемувороткреолзасунулмаленькуюглинянуютабличкустремясловаминадеюсьплатадостаточ нанадосказатьчтокреолоченьскорораскаялсявсодеянномидажепринесискупительнуюжертвуна алтареиштардоэтогоднямагнеубилниодногоребенкаиенпросторебенкаачленаодногоизсамыхи менитыхродовимперииегособственногоюныйэхтатажеведьприходилсякреолуродственниками вотличиеотсвоегоотцапереднимничемнепровинилсяноуженичегонельзбылопоправитьеслиза разрушенныйхешибиумерщвленныхрабовкреолмогзаплатитьвыкупбийстворабавдревнемшу мересчиталосьмелкимпреступлениемкотороеприравнялоськпорчечужогоимуществаосмер тьсынатройнепростилбыемунизакскиеденьгимолодоймагвозненавиделродичадоконцасвоихдн ейаужненавидетьтоэтотчеловекумелкакниктодругойсэтогоднятройжилоднойтолькоместьюраз умеетсяоннебросилсвалобовуюатакутройнебылдуракомипонималчтоскреоломемунетягатьсяо нисчезизшумерапочтинатридцатьлетнокогдавернулсянеизвестногдегоносилостольколетнове рнулсяонужеархимагомиченьбыстрозанялбылоеместоприимператорскомдворепримернозаго ддоеговозвращениякреолзанялпостверховногомагаитройнемедленнопринялсяинтриговатьпыт аясьподсидетьбывшегоприятелятеперьсамогозаклятоговрагавстречаясьвбашнегильдиикреол итройлюбезнораскланивалисьпрячазафальшивымиулыбкамиизвериныеоскалывозвращаясьжед омойонинемедленнопринималисьстроитькознидругпротивдругаособенностаралсятройзадвад цатьлеткреолупришлосьприкончитьстольконаемныхубийцчтоизнихможнобылосформировать небольшуюармиюсрединыхпопадалисьсамыеразныетвариотобычныхлюдейдомогущественны хдемоновособенноартодуиартераидузапомнилсязомхокобжуткоесуществопохожеенаизуро до ванногокальмараразмеромсчетырехслоновпоставленныхдругнадругакакужетроюудалосьдогов оритьсясэтиммонстромнеизвестноновпрошломгодуонвыползизвфратаисухимпутемдошелдо

самогоурагигантбилсяокрепостныестеныпочтидвоесуттокпоакреолполивалегосотнямиразруш
ительныхзаклятийточтовконцеконцовосталосьотчудовищаможнобылозапихнутьвшкатулку

Висновки

Перш за все, ми ознайомилися з методами часткового криптоаналізу та здобули навички у роботі з ними. Крім того, ми попрактикувались в аналізі поточкових шифрів гамування адитивного типу на прикладі шифру Віженера. Насамкінець, ми дійшли висновку, що шифр Віженера не відповідає сучасним вимогам криптостійкості, оскільки ми доволі легко написали код алгоритму, який розшифровує його.