КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

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

Варіант 8

Перша частина:

Текст:

звонокбылнастырнымдолгимкакпаровозныйгудокмежгородтелефонстоялвприхожейподбольшимовальнымзеркаломикогдазвониламужнинароднямашеказалосьчтозеркалосотрясаетсякакотпроходящегопоездаивотвотупадетказенныйплоскийголосждитемариупольнапроводепоголосамихчтолинаработупринимаютзвонилатамарадвоюроднаясестрамужаобычноонапоздравляласновымгодомилисообщалаосмертиочередной тетки уанатолиявмариуполебылцелыйхороводпрестарелойроднимашахотеласразужепередатьемутрубкунотамарасказалапостойкамашяведьименночтоктебеисмущеннойскороговоркойсообщилачтопосленеудачнойоперацииаппендицитавейскепомерлаплемянницатетилидывотэтокакойжететилидыдавидалатыееиплемянницувидаланамоейсвадьбететялидапокойницаонаненамприходитсяроднейасосторонынупошлопоехалокорочестойдругойсторонынемариупольскойаейскоймашадавноужеоставиламноголетниепопыткизапомнитьвсеродственныесвязиизобильноймужниной родниислышыплемянницатопомерланоотнееосталасьдевчоночкатрехлетнуичтоатоявноволнуясьторопливорассказывалатамарачтоэтудевочкуниктоизихнейроднибратьнехочетхотяродняоченьдажзажиточнаядвоюроднаясестрапокойницысамазубнойтехникдомполнаячашаживыеспокойникамивтойроднедружношагалирукаобрукуизродавродвеселоперекликаясьипереругиваясьдоспориваядопеваяпеснюидопиваяшкаликстранночтониктоизтойроднитактакиинехочетвзятьэтогоребенкамашастиснулазубынегорячисьсказалаонасебениктонесобиралсятебяобидетьникомуделанетдотвоейболитомканаконецсказалаонаспокойнотымневсеэтозачемговоришьтазамялась втрубкешумелравнодушныйприбойчьихтогулкихголосовимашавдругпонялачторадиоэтогоразговоратамараявиласьнателеграфвыстоялаочередькабиненуможетвыподумаетемашсловнобыизвиняясьпроговорилатавсежеувасдетейнетможетэтошанскакникрутиатебеужетридцатьшестьтридцатьчетыреоборваламашаияна деждынетеряюялечусьнукакзнаешьтамарасразусниклапотерялаинтересказговорутактыителефонанезапишешьбабыэтойдантисткинавсякийслучайимашазачемтозаписалачтобынеобижатьтомкуведьхорошегохочетдурындаэтакаявсеунихпростоуэтихмариупольскихкоровсполнымивыменамионаопустилатрубкуиподнялаголовуизовальноговрезнойчернойрамезеркалананеевнимательносмотрелащемолодаяженщинасподвижнымусыпаннымобаятельнойвеснушчатойкрупкойлицомзаспинойунеевпроемеоткрытойвспальнюдверивиденбылотдыхающийпоследежурствамужегобосаяступняпокачиваласьмаятникомвтакттолимыслямтолимотивчикунапеваемомубеззвучнолицозаслоненоставнемраскрытойкнижкина

званиеиавторопрокинутывзеркальепрочестьневозможнодалееперспективазерк
алаявлялаокногдетревожнометаласьнаветруусыпаннаябелымисвечкамикронак
иевскогокаштанаавышеиглубжеподнималасьголубизнанебеснойпустотытоесть
отражениесливалосьсосвоимпроизводнымистаиваловнебытиивдругееиспугало
эточтоспросилаонасебяприслушиваяськневнятномуноченьостромустрахучтос
омнойэтотстрахпередуслужливораспахнутойбезднойпочемуонсвязанспривычн
ымотражениемвдомашнемзеркалевсюночьмашанеспаладваждыподнималасьн
акапатьсебевалерьянкитолямолчалхотяонаслышалачтоионворочалсядорассвет
аровногодназадунихпослемноголетнихмедицинскихмытарствродилсякрупный
красивыймертвыймальчикнаутропослеразговорасмариуполеммашадождалась
когдазамужемзахлопнетсявходнаядверьинабраланомертелефонаэтойстранной
женщинукотораянемоглаилинехотелапригретьплемянницусироткуивсесложи
лосьидозвониласьбыстроиженщинаоказаласьнаместеислышнобылофантастиче
скиясноиразговорпроизошелмгновенныйотрывистыйиисчерпывающийсловно
судьбаторопиласьпролистнутьстраницуснезначительнымтекстомвыслушавпер
вуюжемашинуфразутасказалавыэтудевочкуневозьметеонаневообразимохудачт
оэтозначитспросиламашаонабольнаговорювамвыэтудевочкуневозьметевыпрос
тоиспугаетесьагдеонасейчасктозанейсмотриттамсоседкадушевнаяспокойнойри
тойдружилаонахлопочетнасчетопределитьдевочкувучреждениеадрестяжелоды
шасказаламашатапродиктоваламашамолчаопустилатрубкуднемтоляпозвонили
згоспиталясказалчтоестьдвабилетанарайкинапойдемчтотонехочетсяивесьвечер
быласаманесвоязачемтоселаперебиратьдокументытихосиделазадумчивокакпас
ьянсраскладываяаттестатызрелостидипломысвидетельствообракеписьмакотор
ыеписалейтоляещестудентомвоеннойомедицинскойакадемииипередсномонвыше
лизваннойпосмотрелнаженузябкоссутуленнуюнадцветнымикартонками

Різні ключи :
`r_2 = "ок"`
`r_3 = "абв"`
`r_6 = "примат"`
`r_18 = "машадождаласькогда"`
Шматки зашифрованого тексту :
“хмьчьфпещчоыаеючйцтшцнццшкшщоъьмьсыечнбоьфъпфньъьоа”
“увжнтшзялшавоеюрямроггмърдкъабкмьксыхгл”
Пораховані значення I в залежності від довжини ключів:

r	0	2	3	6	18
I	0.05621	0.0458	0.0427	0.034	0.03440

Різні значення D : [212, 222, 310]
Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастіший літері мови : ” уланобсеребзяныепуля”

Скориговане значення ключа (за необхідності) : ” улановсеребряныепули”

Значення ключа, одержане із використанням функції M : ”
улановсеребряныепули”

Фрагмент шифрованого тексту:
рэаюцугкьелаяюиутбхигцичопщпюиермтгсфюлхутвныкрчюрэънфожэчыцфутт
щююуфрйэмидтэяршххаяоняихнтбктяусунаыфетшкткампэгынсфеууаллхекцча
кцуяфйзкиорцлняьдхзгъббстлуччшгиъошулыуьк“”

Фрагмент розшифрованого тексту:
“этасистемакрасногокарликаникогданеимеланазваниятолькозубодробительно
длинныйномервкаталогеисследовавшийеекиберзонд”