Міністерство освіти і науки, молоді та спорту України
Національний технічний університет України
“Київський політехнічний інститут”
Фізико-Технічний інститут

Лабораторна робота №2
з Симетричної криптографії

Студент групи ФІ-93
Карловський Володимир Олександрович

Мета

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

Завдяння №1

Базовый текст:
сюжетграфамонтекристобылпочерпнуталександромдюмаиз...

Текст зашифрованый ключем довжини 2:
асхшбцяугуыбьефэяыаеэфкююбжшявьжбуъшщдпаугэяусыучъ...

Текст зашифрованый ключем довжини 3:
кпщюгцйсзщэбжгшгбыкгбъмюиякюбвждещьшгвужхгзэччэубш...

Текст зашифрованый ключем довжини 4:
щмтръсьльошщхасхшцээцпзцчьгршэщюъочртямшмюъчммшлрх...

Текст зашифрованый ключем довжини 5:
зжйпищшгюцвцрьыашлыидйюхедяиъегыхкбытфкгъшсцъффгтэ...

Завдяння №2

Індекси відповідності для тексту: 0.0554

Індекси відповідності для ключа довжини 2: 0.0447

Індекси відповідності для ключа довжини 3: 0.0396

Індекси відповідності для ключа довжини 4: 0.0409

Індекси відповідності для ключа довжини 5: 0.0370

Індекси відповідності для ключа довжини 10: 0.0325

Індекси відповідності для ключа довжини 20: 0.0344

Завдяння №3

Довжина ключа: 17

Базовий ключ: возвращениеджинда

Результат дешифрування:
дорофейльвовичпсворыкобылыниразьвжизнинепокидалзо...

Результат після корегування:
дорофейльвовичпивторыкобылыниразувжизнинепокидалзе...

Базовий ключ отриманий через M(g): возвращениеджинна

Результат з ключем отриманим через M(g):
дорофейльвовичпивторыкобылыниразувжизнинепокидалзе...

Повністью розшивфрований текст:

дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяп
рожилужебольшешестидесятилетработалпрорабомстроительнойкомп
аниидомостройвхарьковестолицевкраинылюбилпорыбачитьсдрузьям
инаозерахроганьскогокраязачертойгородавыращивалнадачномучастк
еовощиифруктывоспитывалвнуковавотуезжатьзапределыроднойвкра
инынелюбилнесмотрянавозможностивсвязиссозданиемглобальнойсет
иметропобыватьналюбойпланетесолнечнойсистемыидажезаеепредела
мичтоподвиглоегосогласитьсянаэкскурсиюполунеонисамневсостояни
ибылответитьвероятносыгралисвоюрольрассказыдрузейхваставшихся
своимипутешествиямииунеговзыгралолюбопытствопосмотретьвблизи
чтожеэтотакоеспутницаземлиокоторойтакмногоговорятдетивнукиидр
узьякакбытонибылоаутромдвадцатьтретьегодекабряаккуратвначалосв
ятокдорофейльвовичвтайнеотродныхиблизкихпозвонилвбюроэкскурс
ийсолнечнойсистемызапинаясьобъяснилчегохочетивтотжеденьспомо
щьюметродобралсядоаполлонтаунагороданалунеоткудадолжнабылан
ачатьсяэкскурсияпосамымкрасивымизагадочнымместамспутницызем
лиаполлонтаунрасполагалсянаравнинеморяспокойствиянедалекоотзн

аменитойбороздымаскелайнпохожейнаиизвилистоеруслорекиименно
здеськогдатовконцедвадцатоговекасовершилпосадкуамериканскийпи
лотируемыйкорабльаполлонодиннадцатьаточнееегопосадочныймодул
ьестественноэкскурсантамзанимавшимкабинудвадцатиместногоэксску
рсионногофлайтасначалапоказалипамятникаполлонуодиннадцатьпир
амидуизлунногобазальтаспосадочнойплатформойиамериканскимфла
гомазатемфлайтотправилсявпутешествиепоморюспокойствиязалитом
уяркимсолнечнымсветомэкскурсантамиоказалисьмолодыелюдиввозр
астеотвосемнадцатидодвадцатилетпоэтомупоначалудорофейльвовичч
увствовалсебяневсвоейтарелкесмущаясьподлюбопытнымивзглядамис
путниковнопотомегозахватиласуроваякрасоталунныхпейзажейионпер
есталобращатьвниманиенавеселящуюсякомпаниюжадноразглядывая
проплывающиеподднищемфлайтациркиэскарпыкратерыиживописны
егруппыскалмореспокойствияполучилосвоеназваниенеслучайноегоро
внаясглаженнаяповерхностьтипичнадляобширныхморейнадневнойст
оронелуныиредкорадуетнаблюдателейпроявлениемвулканическойдея
тельностиоднакоиздесьимелосьнемалоинтересныхместиобъектовкото
рыедесяткилетволновалиастрономовизучающихспутницуземлизагадо
чнаяцепочкакратеровподназваниемтеннисная ракеткаоколодвухдесят
ковямокдиаметромотпятидесятидостаметровпротянулисьудивительно
ровнойлинией заканчиваяськратеромпобольшедиаметромоколошести
сотметроввпечатлениескладываетсятакоебудтополуннойповерхностид
ействительнопрокатилсяподпрыгиваятеннисныймячоставиввпылицеп
очкуследовсовиныймосткаменнаяаркачерезбороздумаскелайндлиной
околотрехкилометровизумительноровнаястенаобрывадлинойоколотр
идцатикилометромбудтоктотоотхватилножомкусоклуннойповерхност
иивыбросилвкосмосоставивсрезиложбинуглубинойвкилометрборозда
золотойручейсамоенастоящееруслорекиширинойвполторакилометраи
длинойвполторастасверкающееподлучамисолнцакристалликамипири
тацветочнаяклумбавозвышениерыхлойпородыоранжевогоцветадиаме
тромоколодвухкилометровивысотойвдвестиметровдействительноклум
баеслипосмотретьсверхустоунхенджгруппаскалсплоскимивершинамис
оединенныхповерхудостаточноровнымиплитамипрактическинеотлич
аетсяотземногомегалитическогокомплексаванглииинаконецбороздам
аскелайндлинойоколочетырехсоткилометровтакжездоровопохожаяна

руслорекиширинойоткилометрадотрехкакобъяснилгидборозданасамо
мделепредставляетсобойсдвиговыйразломлуннойкорыслучившийсяде
сяткимиллионовлетназадврезультатеподвижкищитаотудараметеорита
носверхуборoздавсеравнонапоминаетрекуидорофейльвовичдажепредс
тавилкакпоруслутечетводаостанавливалисьивыходилиизфлайтаодеты
евпузыривакуумплотныхспецкостюмовнесколькоразвкабинеаппарата
поддерживаласьнормальнаясилатяжестипочтиземнаяавнееецарилолу
нноетяготениевшестьразслабееземногопоэтомунеобошлосьбезкурьезо
винеловкихдвиженийправдавсевконцеконцовпривыкликнеобычайной
легкостивтелеисудовольствиемскакалипоместнымбуеракамвтомчисле
идорофейльвовичполучившийнисчемнесравнимыеощущенияатеперь
явампокажуобъектзеросказалгидприглашаяэкскурсантоввкабинупосл
еочередноговыходанаружуходятлегендычтовэтомместенаглубинедвух
сотметровраспoлагалсязагадочныйшаризкотороговпоследствиивылуп
илсяназемлебоевойгиперптеридскийроботдемонавторитетнымтономз
аметилктотоизкомпаниимолодыхлюдейилиджиннсовершенновернон
оведьонпотомоставилвкольцахсатурнасвоюикрубриллиантидыэтоуже
другаяисториявынаверноепомнитевойнасджиннамизакончиласьвсего
лишьгодназадаздесьосталсяследдемоначтовнеминтересногоувидитеф
лайтспрозрачнымидосамогополастенкамиподнялсянадкратеромавако
ваипонессякгоризонтусвисящейнаднимпочтиполнойземлейокрашива
ющейравнинувголубоватыйцветвместахгдележалатеньотскалосвещен
ныхпрямымисолнечнымилучамиприблизиласьрекабороздымаскелай
нраздаласьвширьпревратиласьвкрутойглубинойдокилометраканьонна
одномизплоскихгребнейканьонапоявилосьбелосеребристоепятнышко
превратилосьвхолмикзатемвгорусдыройвцентрефлайтзависвпарекило
метровотэтойстраннойгорыиэкскурсантыначалирассматриватьобъект
имевшийнеобычноеназваниезеробольшевсегосеребристыйкуполскрат
еромдиаметромвтрикилометранапоминалчеловеческийглазрадужкак
отороговысохлаипожухлапревратившисьвбелоснежныйслоймхаивызы
валэтотглазотнюдьнеприятныеирадостныеощущениянеомерзениенет
ноиневосторгслишкоммноговэтомзрелищебылопугающегоиотталкива
ющегоиодновременнопритягивающеговзормолодежьпритихладорофе
йльвовичпочувствовалстеснениевгрудипосмотрелнагидататулыбнулся
какнастоящийчеловекхотябылвсегонавсеговитсомнравитсячтоэтотако

еэффектквантовойэффузиикакговорятученыеобразноговорянагорные
породыподействовалодыханиедемонанаэтомместеболеедвухсотлетназ
аднаходилсяториевыйрудникшахтакоторогодостиглашаровиднойполо
стигдеиспалджинннепосредственнокшахтенаснепропуститохрананоту
трядоместьинтересноеущельеонообразовалосьсовсемнедавновсегодва
месяцаназадимыможемполюбоватьсянарудниксобрываполетелиздоро
вооченьинтересномыхотимпрогулятьсяраздалисьголосадорофейльвов
ичхотяинеиспытывалбольшежеланиягулятьоднаковозражатьнесталун
еговозниклоощущениечтоонздесьужебылкогдатохотяникогдараньшел
унунепосещалфлайтоблетелснежносеребристыйглазбывшеготориевог
орудникакругомповернулвдольбороздымаскелайнкюгуснизилсястали
виднытрещиныразорвавшиебоковыестенкиборoздысовсемсвежиесудя
поблескуузкиеипоширеочевидноэтобылрезультатнедавнеголунотрясе
нияокоторомговорилгидприблизиласьочереднаятрещинадействитель
нообразовавшаяживописноеущельесослоистымистенамифлайтподпр
ыгнулиселнаобрывескоторогобылихорошовидныкуполобъектазероиб
ороздамаскелайнэкскурсантыпосыпалисьизаппаратарадуясьвозможно
стиразмятьсягурьбойнаправилиськобрывуперебрасываясьшуточками
идурачасьвнихигралащенячьяэнергиямолодостиидорофейльвовичнам
гновениепозавидовалзадоруиоптимизмуюношейидевушекгодящихсяе
мучутьлиневовнукионтожеполюбовалсянаснежнобелыйкуполвтрехки
лометрахотобрывапотомтихонькоотошелотрезвящихсямолодыхлюдей
ипрошелсявдольобрывавглядываясьвпротивоположнуюстенуущельяв
згляднаткнулсянарядчерныхотверстийпохожихнаследыпулеметнойоч
ередизаинтересовавшисьдорофейльвовичпрыгнулвнизивключивантиг
равпересекущельеопустилсянаузкийкарнизпередсамойбольшойдырой
опредупреждениигиданеотходитьдалекоотфлайтаонзабылдыраоказал
асьвходомвпещеру