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

Довжина	Індекс відповідності
6	3.39%
7	3.43%

8	3.49%
9	3.40%
10	3.42%
11	3.34%
12	3.42%
13	3.42%
14	3.37%
15	3.28%
16	3.43%
17	5.73%
18	3.44%
19	3.28%
20	3.58%
21	3.50%
22	3.62%
23	3.38%
24	3.27%
25	3.28%
26	3.28%
27	3.51%
28	3.41%
29	3.21%
30	3.32%

Завдяння №3

Таблиця для M_i (щоб побудувати повну таблицю треба перебудувати всю програму, тому трішки по іншому):

```
1 в: 22.838 г: 14.876 о: 9.600 щ: 12.734
2 л: 15.745 о: 23.258 п: 14.912
3 з: 21.640 н: 13.275 ч: 10.974
4 в: 21.785 г: 14.017 я: 16.158
5 е: 8.862 р: 23.264 у: 17.459
6 а: 22.304 г: 15.425 д: 13.555 ы: 13.639
7 в: 12.826 ц: 15.888 щ: 21.817 ь: 15.014
8 а: 14.385 в: 16.465 г: 14.467 д: 15.418 е: 22.211 ж: 14.370 к: 13.900
9 а: 11.475 к: 16.294 н: 22.056 с: 13.795
10 е: 15.964 и: 22.317 л: 16.237
11 г: 14.239 д: 14.529 е: 21.589 и: 16.387
12 г: 14.524 д: 22.742 ж: 14.219
13 ж: 22.548 й: 16.576
14 е: 15.328 и: 21.499 л: 17.295 ъ: 12.796
15 н: 22.847 о: 14.824 ы: 14.616
16 к: 15.648 м: 14.758 н: 22.091 р: 15.635 т: 15.408 я: 12.974
17 а: 22.611 г: 16.372 д: 14.350 ы: 15.282 я: 15.362
```

Максимуми і тут видно)

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...

Повністю розшивфрований текст:

дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяп
рожилужебольшешестидесятилетработалпрорабомстроительнойкомп
аниидомостройвхарьковестолицевкраинылюбилпорыбачитьсдрузьям
инаозерахроганьскогокраязачертойгородавыращивалнадачномучастк
еовощиифруктывоспитывалвнуковавотуезжатьзапределыроднойвкра
инынелюбилнесмотрянавозможностивсвязиссозданиемглобальнойсет
иметропобыватьналюбойпланетесолнечнойсистемыидажезаеепредела
мичтоподвиглоегосогласитьсянаэкскурсиюполунеонисамневсостояни
ибылответитьвероятносыгралисвоюрольрассказыдрузейхвастявшихся
своимипутешествиямииунеговзыгралолюбопытствопосмотретьвблизи
чтожеэтотакоеспутницаземлиокоторойтакмногоговорятдетивнукиидр
узьякакбытонибылоаутромдвадцатьтретьегодекабряаккуратвначалосв
ятокдорофейльвовичвтайнеотродныхиблизкихпозвонилвбюроэкскурс
ийсолнечнойсистемызапинаясьобъяснилчегохочетивтотжеденьспомо
щьюметродобралсядоаполлонтаунагороданалунеоткудадолжнабылан
ачатьсяэкскурсияпосамымкрасивымизагадочнымместамспутницызем
лиаполлонтаунрасполагалсянаравнинеморяспокойствиянедалекоотзн
аменитойбороздымаскелайнпохожейнаиизвилистоеруслорекиименно
здеськогдатовконцедвадцатоговекасовершилпосадкуамериканскийпи
лотируемыйкорабльаполлонодиннадцатьаточнееегопосадочныймодул
ьестественноэкскурсантамзанимавшимкабинудвадцатиместногоэкску
рсионногофлайтасначалапоказалипамятникаполлонуодиннадцатьпир
амидуизлунногобазальтаспосадочнойплатформойиамериканскимфла
гомазатемфлайтотправилсявпутешествиепоморюспокойствиязалитом
уяркимсолнечнымсветомэкскурсантамиоказалисьмолодыелюдиввозр
астеотвосемнадцатидодвадцатилетпоэтомупоначалудорофейльвовичч
увствовалсебяневсвоейтарелкесмущаясьподлюбопытнымивзглядамис
путниковнопотомегозахватиласуроваякрасоталунныхпейзажейионпер
есталобращатьвниманиенавеселящуюсякомпаниюжадноразглядывая

проплывающиеподднищемфлайтациркиэскарпыкратерыиживописны
егруппыскалмореспокойствияполучилосвоеназваниенеслучайноегоро
внаясглаженнаяповерхностьтипичнадляобширныхморейнадневнойст
оронелуныиредкорадуетнаблюдателейпроявлениемвулканическойдея
тельностиоднакоиздесьимелосьнемалоинтересныхместиобъектовкото
рыедесяткилетволновалиастрономовизучающихспутницуземлизагадо
чнаяцепочкакратеровподназваниемтеннисная ракеткаоколодвухдесят
ковямокдиаметромотпятидесятидостаметровпротянулисьудивительно
ровнойлинией заканчиваяськратеромпобольшедиаметромоколошести
сотметроввпечатлениескладываетсятакоебудтополуннойповерхностид
ействительнопрокатилсяподпрыгиваятеннисныймячоставиввпылицеп
очкуследовсовиныймосткаменная аркачерезбороздумаскелайндлиной
околотрехкилометровизумительноровнаястенаобрывадлинойоколотр
идцатикилометромбудтоктотоотхватилножомкусоклуннойповерхност
иивыбросилвкосмосоставивсрезиложбинуглубинойвкилометрборозда
золотойручейсамоенастоящееруслорекиширинойвполторакилометраи
длинойвполторастасверкающееподлучамисолнцакристалликамипири
тацветочная клумбавозвышениерыхлойпородыоранжевогоцветадиаме
тромоколодвухкилометровивысотойвдвестиметровдействительноклум
баеслипосмотретьсверхустоунхенджгруппаскалсплоскимивершинамис
оединенныхповерхудостаточноровнымиплитамипрактическинеотлич
аетсяотземногомегалитическогокомплексаванглииинаконецбороздам
аскелайндлинойоколочетырехсоткилометровтакжездоровопохожаяна
руслорекиширинойоткилометрадотрехкакобъяснилгидборозданасамо
мделепредставляетсобойсдвиговыйразломлуннойкорыслучившийсяде
сяткимиллионовлетназадврезультатеподвижкищитаотудараметеорита
носверхуборозда всеравнонапоминаетрекуидорофейльвовичдажепредс
тавилкакпоруслутечетводаостанавливалисьивыходилиизфлайтаодеты
евпузыривакуумплотныхспецкостюмовнесколькоразвкабинеаппарата
поддерживаласьнормальнаясилатяжестипочтиземная явнееецарилолу
нноетяготениевшестьразслабееземногопоэтомунеобошлосьбезкурьезо
винеловкихдвиженийправдавсевконцеконцовпривыкликнеобычайной
легкостивтелеисудовольствиемскакалипоместнымбуеракамвтомчисле
идорофейльвовичполучившийнисчемнесравнимыеощущенияатеперь
явампокажуобъектзеросказалгидприглашаяэкскурсантоввкабинупосл

еочередноговыходанаружуходятлегендычтовэтомместенаглубинедвух
сотметровраспологалсязагадочныйшаризкотороговпоследствиивылуп
илсяназемлебоевойгиперптеридскийроботдемонавторитетнымтономз
аметилктотоизкомпаниимолодыхлюдейилиджиннсовершенновернон
оведьонпотомоставилвкольцахсатурнасвоюикрубриллиантидыэтоуже
другаяисториявынаверноепомнитевойнасджиннамизакончиласьвсего
лишьгодназадаздесьосталсяследдемоначтовнеминтересногоувидитеф
лайтспрозрачнымидосамогополастенкамиподнялсянадкратеромавако
ваипонессякгоризонтусвисящейнаднимпочтиполнойземлейокрашива
ющейравнинувголубоватыйцветвместахгдележалатеньотскалосвещен
ныхпрямымисолнечнымилучамиприблизиласьрекабороздымаскелай
нраздаласьвширьпревратиласьвкрутойглубинойдокилометраканьонна
одномизплоскихгребнейканьонапоявилосьбелосеребристоепятнышко
превратилосьвхолмикзатемвгорусдыройвцентрефлайтзависвпарекило
метровотэтойстраннойгорыиэкскурсантыначалирассматриватьобъект
имевшийнеобычноеназваниезероболышевсегосеребристыйкуполскрат
еромдиаметромвтрикилометранапоминалчеловеческийглазрадужкак
отороговысохлаипожухлапревратившисьвбелоснежныйслоймхаивызы
валэтотглазотнюдьнеприятныеирадостныеощущениянеомерзениенет
ноиневосторгслишкоммноговэтомзрелищебылопугающегоиотталкива
ющегоиодновременнопритягивающеговзормолодежьпритихладорофе
йльвовичпочувствовалстеснениевгрудипосмотрелнагидататулыбнулся
какнастоящийчеловекхотябылвсегонавсеговитсомнравитсячтоэтотако
еэффектквантовойэффузиикакговорятученыеобразноговорянагорные
породыподействовалодыханиедемонанаэтомместеболеедвухсотлетназ
аднаходилсяториевыйрудникшахтакоторогодостиглашаровиднойполо
стигдеиспалджинннепосредственнокшахтенаснепропуститохрананоту
трядоместьинтересноеущельеонообразовалосьсовсемнедавновсегодва
месяцаназадимыможемполюбоватьсянарудниксобрываполетелиздоро
вооченьинтересномыхотимпрогулятьсяраздалисьголосадорофейльвов
ичхотяинеиспытывалбольшежеланиягулятьоднаковозражатьнесталун
еговозниклоощущениечтоонздесьужебылкогдатохотяникогдараньшел
унунепосещалфлайтоблетелснежносеребристыйглазбывшеготориевог
орудникакругомповернулвдольбороздымаскелайнкюгуснизилсястали
виднытрещиныразорвавшиебоковыестенкибороздысовсемсвежиесудя

поблескуузкиеипоширеочевидноэтобылрезультатнедавнеголунотрясе
нияокоторомговорилгидприблизиласьочереднаятрещинадействитель
нообразовавшаяживописноеущельесослоистымистенамифлайтподпр
ыгнулиселнаобрывескоторогобылихорошовидныкуполобъектазероиб
ороздамаскелайнэкскурсантыпосыпалисьизаппаратарадуясьвозможно
стиразмятьсягурьбойнаправилиськобрывуперебрасываясьшуточками
идурачасьвнихигралащенячьяэнергиямолодостиидорофейльвовичнам
гновениепозавидовалзадоруиоптимизмуюношейидевушекгодящихсяе
мучутьлиневовнукионтожеполюбовалсянаснежнобелыйкуполвтрехки
лометрахотобрывапотомтихонькоотошелотрезвящихсямолодыхлюдей
ипрошелсявдольобрывавглядываясьвпротивоположнуюстенуущельяв
згляднаткнулсянарядчерныхотверстийпохожихнаследыпулеметнойоч
ередизаинтересовавшисьдорофейльвовичпрыгнулвнизивключивантиг
равпересекущельеопустилсянаузкийкарнизпередсамойбольшойдырой
опредупрежденииигиданеотходитьдалекоотфлайтаонзабылдыраоказал
асьвходомвпещеру