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

Лабораторна робота №2

Криптоаналіз шифру Віженера

Виконали: студенти гр. ФІ-94, Молдован Д.В., Пелешенко Л.І.

Перевірив: Чорний О.М.

Мета роботи

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

Порядок виконання роботи

- 1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
- 2. 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.
- 3. Підрахувати індекси відповідності І_г для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.
- 4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст(згідно свого номеру варіанта). Зокрема, необхідно:
- визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь Dr(на вибір);
- визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;
- визначити символи ключа за допомогою функції M(g)i;
- розшифрувати текст, використовуючи знайдений ключ;
- в разі необхідності скорегувати ключ.

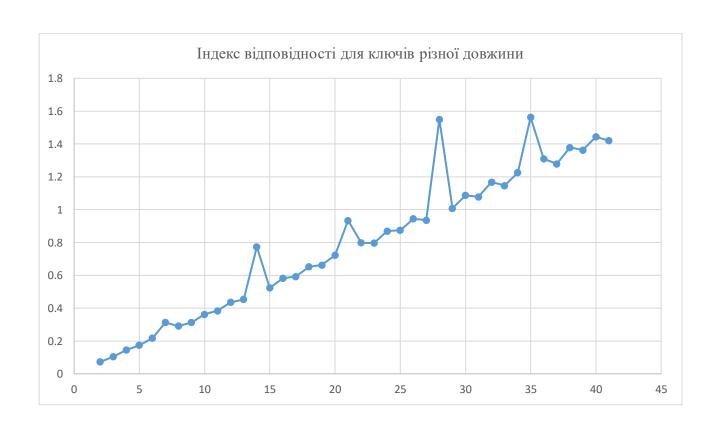
Опис труднощів

Проблеми виникали із індексами відповідності, бо алгоритм ϵ великим та складним. Складно було розібратись де були допущені помилки і через це пішло багато часу на програмування цього алгоритму.

Індекс відповідності для ключів різної довжини

(index)	period	value	
0	2	0.0725364109	06435856
1	3	0.1044830454	8965535
2	4	0.1454725625	33890423
3	5	0.1746146914	9456219
4	6	0.2175449989	5413743
5	7	0.3123818600	2046464
6	8	0.2913809148	8829551
7	9	0.3128240866	5225608
8	10	0.362297392	90079777
9	11	0.383599380	9638566
10	12	0.435443705	50707332
11	13	0.453451223	8809074
12	14	0.773943591	9899533
13	15	0.523575723	1689487
14	16	0.581913561	9619122
15	17	0.592316458	35294299
16	18	0.652249250	1194326
17	19	0.662572687	4593456
18	20	0.722009328	32284464
19	21	0.933866687	76234638
20	22	0.798415542	27341344
21	23	0.79627108	3281914
22	24	0.869798592	24309325
23	25	0.874998051	9581716
24	26	0.94511189	9533797

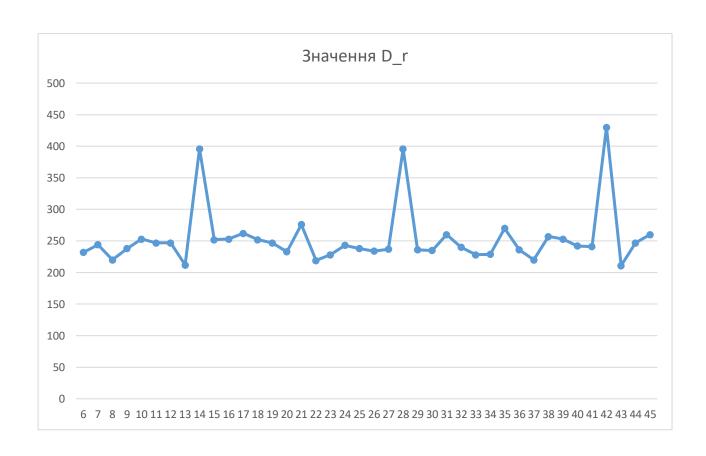
25	27	0.9359071139731001
26	28	1.5501031535514296
27	29	1.0078610209391432
28	30	1.0870680836592883
29	31	1.0784286694633758
30	32	1.1681605761127711
31	33	1.1461555096479916
32	34	1.2260816891658015
33	35	1.562695199537305
34	36	1.3091618347578018
35	37	1.2791963200095233
36	38	1.3788215826167158
37	39	1.3632705593624486
38	40	1.44363334455993
39	41	1.420873633363087



Послідовність D_r при визначенні довжини ключа шифру Віженера

(index) period value						
0	6 2	32				
1	7 2	44				
2	8 2	20				
3	9 2	38				
4	10 2	253				
5	11 2	247				
6	12 2	247				
7	13 2	212				
8	14 3	896				
9	15 2	252				
10	16	253				
11	17	262				
12	18	252				
13	19	247				
14	20	233				
15	21	276				
16	22	219				
17	23	228				
18	24	243				
19	25	238				
20	26	234				
21	27	237				
22	28	396				
23	29	236				
24	30	235				
25	31	260				

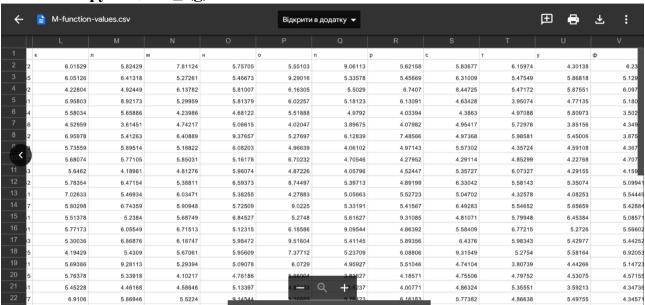
26	32	240	
27	33	228	
28	34	229	
29	35	270	
30	36	236	
31	37	220	
32	38	257	
33	39	253	
34	40	242	
35	41	241	
36	42	430	
37	43	211	
38	44	247	
39	45	260	

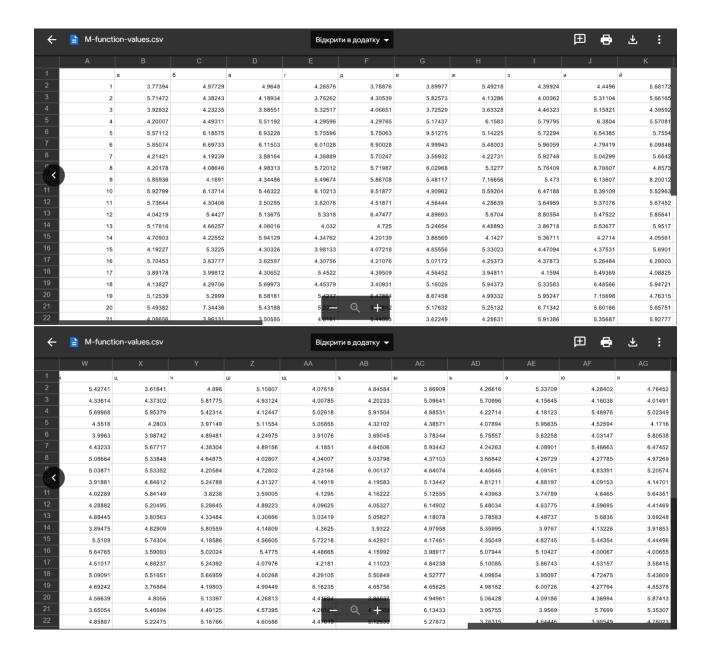


Значення ключів

- 1. За допомогою співставлення найчастіших літер блоків найчастіших літер мови : последнийдозор
- 2. За допомогою M_i(g): последнийдозорпоследнийдозорпоследнийдозорпоследнийдозор

Значення функції М_і(g)





Результат розшифрування текста:

1. Последний дозор:

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосред ибескрайнейсеройравнинывзгляднефиксироваляркихкрасоквцелойкартиненосто иловсмотретьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянцемлазурьюзе леньюнадголовойзастылобелоесрозовымбудтомолочнуюрекуперемешалискисель нымиберегамидаивыплеснуливнебесааещедулветерибылохолодномневсегдахоло дноначетвертомслоесумраканоэтоиндивидуальнаяреакциягесерунапротивбылож арколицораскраснелосьполбустекаликапелькипотамненехватаетсилысказалялиц огесерасовсемпобагровелоответнеправильныйтывысшиймагтакполучилосьслуча йнонотывысшийпочемувысшихмаговтакженазываютмагамивнекатегорийпотому чторазницавсилемеждуниминастольконезначительначтонеможетбытьисчисленаи

невозможноопределитьктосильнееактослабеепробормоталяборисигнатьевичяпон имаюномненехватаетсилыянемогупройтинапятыйслойгесерпосмотрелсебеподно гиподделноскомботинкапесокподбросилввоздухшагнулвпередиисчезэточтосовет яподбросилпередсобойпесокшагнулвпередтщетнопытаясьпойматьсвоютеньтени небылоничегонеизменилосьяпопрежнемуоставалсяначетвертомслоеистановилос ьвсехолоднеепаротмоегодыханияуженерассеивалсябелымоблачкомаколючимииг ламиосыпалсянапесокразвернувшисьэтовсегдапрощепсихологическиискатьвыхо дпозадиясделалшагивышелнатретийуровеньсумракавбесцветныйлабиринтизъеде нныхвременемкаменныхплитнадкоторымисерелонизкоезастывшеенебокоегдепок амнюстелилисьвысохшиестеблипохожиенаприбитыйморозомвьюнокпереростоке щешагвторойслойсумракакаменныйлабиринтнакрылипереплетенныеветвииещеп ервыйслойуженекаменьужестеныиокназнакомыестенымосковскогоофисаночног одозоравегосумеречномобличьепоследнимусилиемявывалилсяизсумракавреальн ыймирпрямовкабинетгесераразумеетсяшефужесиделвкреслеаяпошатываясьстоял переднимнукаккаконмогменяопередитьведьонпошелнапятыйслойаяначалвыходи тьизсумракакогдаяувиделчтоутебяничегонеполучаетсясказалгесердаженеглядяна менятовышелизсумраканапрямуюизпятогослоявнастоящиймирянесмогскрытьуд ивлениядачтотебяудивляетяпожалплечаминичегонеудивляетеслигесерзахочетпре поднестимнесюрпризунегобудетогромныйвыборяоченьмногогонезнаюиэтообидн осказалгесерсядьгородецкийяселнапротивгесерасложилрукинаколеняхдажеголов уопустилбудтовчемточувствовалсвоювинуантонхорошиймагвсегдадостигаетсвое гомогуществавнужноевремясказалшефпоканестанешьмудреенестанешьсильнееп оканестанешьсильнеенеовладеешьвысшеймагиейпоканеовладеешьвысшеймагие йневлезешьвопасныеместаутебяситуацияуникальнаятыпопалподонпоморщилсяз аклятиефуарантысталвысшиммагомнебудучикэтомуготовымдаутебяестьсиладат ыумеешьеюуправлятьиточтотыструдомделалраньшетеперьнесоставляетпроблем сколькотыпробылначетвертомслоесумракаисидишькакнивчемнебывалоновотточ еготынеумелраньшеонзамолчалянаучусьборисигнатьевичсказалявконцеконцоввс епризнаютчтояделаюзначительные успехиольгасветланаделаешьлегкопризналгес ертыженесовсемидиотчтобынеразвиватьсяносейчастынапоминаешьмненеопытно говодителякоторыйполгодапокаталсянажигуляхивдругселзарульгоночногоферра ринетхужезарулькарьерногосамосвалабелазавесомвдвеститоннчтоползетсебепос пираливыезжаетизкарьераарядомпропасть в сотнюметроватам в низуедутдругиеса мосвальюднотвоеневерноедвижениерезкийповоротруляилидрогнувшаянапедали ногаплохобудетвсемпонимаюякивнулнояввысшиенервалсяборисигнатьевичэтов ыменяотправиливпогонюзакостейятебянивчемнеупрекаюипытаюсьмногомунауч итьсказалгесеридовольнонепоследовательнодобавилхотьтыоднаждыиотказалсяб ытьмоимученикомяпромолчалоткрывпапкувеликийгесерзавязывалтесемкинабан тикяобнаружилчетыресвеженькиеещепахнущиетипографскойкраскойгазетныевы резкифакситрифотографиитривырезкибылинаанглийскомнанихяисосредоточилс явпервуюочередьперваявырезкапредставляласобойкороткуюзаметкуопроисшест виивтуристическоматтракционеподземельяшотландиикакяпонялвэтомзаведении

довольнотакибанальномвариантекомнатыстрахаиззатехническихнеполадокпогиб русскийтуристподземельябылизакрытыполицияпроводитрасследованиеивыясняе тнетливтрагедиивиныперсоналавтораязаметкабылакудаподробнеепротехнически енеполадкиуженебылонисловатекстбылнемножкосуховатымдажепедантичнымсн арастающимволнениемяпрочиталчтопогибшийдвадцатипятилетнийвикторпрохо ровучилсявэдинбургскомуниверситетебылсыномрусскогополитикавподземельяо тправилсявместесневестойприлетевшейизроссиивалериейхомконарукахкоторойи скончалсяотпотерикровивтемнотетуристическогоаттракционактотоперерезалему горлоиличтотоперерезалобедолагасиделвместесневестойвлодочкекотораямедлен ноплылапокровавойрекемелкойканавкевокругзамкавампироввозможноизстеныто рчалакакаятоостраяжелезкакотораяиполоснулавикторупошеедочитавдоэтогомест аявздохнулипосмотрелнагесераутебявсегдазамечательнополучалосьэээсвампира мисказалшефнасекундуоторвавшисьотсвоихбумагтретьязаметкабылаизкакойтож елтойшотландскойгазетенкиивоттутконечножеавторрассказалстрашнуюисторию просовременныхвампировкоторыевомракеаттракционовсосуткровьсвоихжертвед инственнойоригинальнойдетальюбылоутверждениежурналистачтообычновампи рывысасываютсвоихжертвненасмертьнорусскийстуденткакположенорусскомубы лнастолькопьянчтобедныйшотландскийвампиртожезахмелелиувлексянесмотрян авсютрагичностьисторииязасмеялсяжелтаяпрессаонавовсеммиреодинаковасказа лгесернеподнимаяглазсамоеужасноечтотаквсеибылосказалякромепьянстваконеч нокружкапивазаобедомсогласилсягесерчетвертаявырезкабылаизкакойтонашейга зетынекрологсоболезнованиялеонидупрохоровудепутатугосударственнойдумыче йсынтрагическипогибявзяллистокфаксаэтокакяипредполагалбылодонесениеотно чногодозорагородаэдинбургашотландиявеликобританиянемножконеобычнымока залсялишьадресатсамгесеранеоперативныйдежурныйилируководительмеждунар одногоотделаитонписьмачутьболееличныйчемполагаетсявофициальныхдокумен тахасодержаниеменянеудивилосприскорбиемсообщаемпорезультатамтщательно проведенногодознанияполнаяпотерякровипризнаковинициацииневыявленопрове денныепоискирезультатовнедалипривлеченылучшиесилыеслимосковскоеотделе ниесчитаетнеобходимымнаправитьпередавайсамыетеплыеприветыольгеоченьрад затебястарыйковторойлистокфаксаотсутствовалвидимотамбылисключительноли чныйтекстпоэтомуиподписиянеувиделфомалермонтсказалгесерглавашотландско годозорастарыйдругагазадумчивопротянулязначитнашивзглядыопятьвстретилис ьнетужродственниклионмихаилуюрьевичусамспросишьсказалгесеряодругомкоэт окомандиркоэтогесерзапнулсяисявнымнедовольствомпокосилсяналистоккоэтоко этотебяуженекасаетсяяпосмотрелнафотографиимолодойчеловекэтоибылбедолага виктордевушкасовсемюнаяегоневестачтотутгадатьимужикпостаршеотецвиктора косвенныеданныеговорятонападениивампиранопочемуситуациятребуетнашегов мешательстваспросилянашисоотечественникичастенькогибнутзарубежомиотвам пировтожевынедоверяетефомеиегоподчиненнымдоверяюноунихмалоопыташотл андиямирнаяуютнаяспокойнаястранаонимогутнесправитьсяатычастенькоимелде лосвампирамиконечноивсетакиделовтомчтоегоотецполитикгесерпоморщилсядак

акойонполитикбизнесменпробралсявдепутатынаголосованияхжметкнопкипотихо нькукороткоияснононеверючтонетособойпричиныгесервздохнулотецюношидвад цатьлетназадбылопределенкакпотенциальныйсветлыйинойдовольносильныйоти нициацииотказалсяобъявивчтохочетостатьсячеловекомтемныхсразужепослалпро чьноснамиподдерживалнекоторыеконтактыиногдапомогалякивнулдаслучайредк ийнечастолюдиотказываютсяоттакихвозможностейчтооткрываютсяпередиными можносказатьчтоячувствуюсебявиноватымпередпрохоровымстаршимсказалгесе риеслиужнемогупомочьсынутонепозволюегоубийцеуйтибезнаказаннымтыпоеде шьвэдинбургнайдешьэтогосумасшедшегокровососаиразвеешьповетруэтобылпри казнояибезтогонесобиралсяспоритькояневольнозапнулсякогдалететьзайдивмежд ународныйотделтебедолжныбылиподготовитьдокументыбилетыденьгиилегенду

2. Последний дозорпоследний дозорпоследний дозорпоследний дозор:

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосред ибескрайнейсеройравнинывзгляднефиксироваляркихкрасоквцелойкартиненосто иловсмотретьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянцемлазурьюзе леньюнадголовойзастылобелоесрозовымбудтомолочнуюрекуперемешалискисель нымиберегамидаивыплеснуливнебесааещедулветерибылохолодномневсегдахоло дноначетвертомслоесумраканоэтоиндивидуальнаяреакциягесерунапротивбылож арколицораскраснелосьполбустекаликапелькипотамненехватаетсилысказалялиц огесерасовсемпобагровелоответнеправильныйтывысшиймагтакполучилосьслуча йнонотывысшийпочемувысшихмаговтакженазываютмагамивнекатегорийпотому чторазницавсилемеждуниминастольконезначительначтонеможетбытьисчисленаи невозможноопределитьктосильнееактослабеепробормоталяборисигнатьевичяпон имаюномненехватаетсилыянемогупройтинапятыйслойгесерпосмотрелсебеподно гиподделноскомботинкапесокподбросилввоздухшагнулвпередиисчезэточтосовет яподбросилпередсобойпесокшагнулвпередтщетнопытаясьпойматьсвоютеньтени небылоничегонеизменилосьяпопрежнемуоставалсяначетвертомслоеистановилос ьвсехолоднеепаротмоегодыханияуженерассеивалсябелымоблачкомаколючимииг ламиосыпалсянапесокразвернувшисьэтовсегдапрощепсихологическиискатьвыхо дпозадиясделалшагивышелнатретийуровеньсумракавбесцветныйлабиринтизъеде нныхвременемкаменныхплитнадкоторымисерелонизкоезастывшеенебокоегдепок амнюстелилисьвысохшиестеблипохожиенаприбитыйморозомвьюнокпереростоке щешагвторойслойсумракакаменныйлабиринтнакрылипереплетенныеветвииещеп ервыйслойуженекаменьужестеныиокназнакомыестенымосковскогоофисаночног одозоравегосумеречномобличьепоследнимусилиемявывалилсяизсумракавреальн ыймирпрямовкабинетгесераразумеетсяшефужесиделвкреслеаяпошатываясьстоял переднимнукаккаконмогменяопередитьведьонпошелнапятыйслойаяначалвыходи тьизсумракакогдаяувиделчтоутебяничегонеполучаетсясказалгесердаженеглядяна менятовышелизсумраканапрямуюизпятогослоявнастоящиймирянесмогскрытьуд ивлениядачтотебяудивляетяпожалплечаминичегонеудивляетеслигесерзахочетпре

поднестимнесюрпризунегобудетогромныйвыборяоченьмногогонезнаюиэтообидн осказалгесерсядьгородецкийяселнапротивгесерасложилрукинаколенях дажеголов уопустилбудтовчемточувствовалсвоювинуантонхорошиймагвсегдадостигаетсвое гомогуществавнужноевремясказалшефпоканестанешьмудреенестанешьсильнееп оканестанешьсильнеенеовладеешьвысшеймагиейпоканеовладеешьвысшеймагие йневлезешьвопасныеместаутебяситуацияуникальнаятыпопалподонпоморщилсяз аклятиефуарантысталвысшиммагомнебудучикэтомуготовымдаутебяестьсиладат ыумеешьеюуправлятьиточтотыструдомделалраньшетеперьнесоставляетпроблем сколькотыпробылначетвертомслоесумракаисидишькакнивчемнебывалоновотточ еготынеумелраньшеонзамолчалянаучусьборисигнатьевичсказалявконцеконцоввс епризнаютчтояделаюзначительныеуспехиольгасветланаделаешьлегкопризналгес ертыженесовсемидиотчтобынеразвиватьсяносейчастынапоминаешьмненеопытно говодителякоторыйполгодапокаталсянажигуляхивдругселзарульгоночногоферра ринетхужезарулькарьерногосамосвалабелазавесомвдвеститоннчтоползетсебепос пираливыезжаетизкарьераарядомпропастывсотнюметроватамвнизуедутдругиеса мосвальюднотвоеневерноедвижениерезкийповоротруляилидрогнувшаянапедали ногаплохобудетвсемпонимаюякивнулнояввысшиенервалсяборисигнатьевичэтов ыменяотправиливпогонюзакостейятебянивчемнеупрекаюипытаюсьмногомунауч итьсказалгесеридовольнонепоследовательнодобавилхотьтыоднаждыиотказалсяб ытьмоимученикомяпромолчалоткрывпапкувеликийгесерзавязывалтесемкинабан тикяобнаружилчетыресвеженькиеещепахнущиетипографскойкраскойгазетныевы резкифакситрифотографиитривырезкибылинаанглийскомнанихяисосредоточилс явпервуюочередьперваявырезкапредставляласобойкороткуюзаметкуопроисшест виивтуристическоматтракционеподземельяшотландиикакяпонялвэтомзаведении довольнотакибанальномвариантекомнатыстрахаиззатехническихнеполадокпогиб русскийтуристподземельябылизакрытыполицияпроводитрасследованиеивыясняе тнетливтрагедиивиныперсоналавтораязаметкабылакудаподробнеепротехнически енеполадкиуженебылонисловатекстбылнемножкосуховатымдажепедантичнымсн арастающимволнениемяпрочиталчтопогибшийдвадцатипятилетнийвикторпрохо ровучилсявэдинбургскомуниверситетебылсыномрусскогополитикавподземельяо тправилсявместесневестойприлетевшейизроссиивалериейхомконарукахкоторойи скончалсяотпотерикровивтемнотетуристическогоаттракционактотоперерезалему горлоиличтотоперерезалобедолагасиделвместесневестойвлодочкекотораямедлен ноплылапокровавойрекемелкойканавкевокругзамкавампироввозможноизстеныто рчалакакаятоостраяжелезкакотораяиполоснулавикторупошеедочитавдоэтогомест аявздохнулипосмотрелнагесераутебявсегдазамечательнополучалосьэээсвампира мисказалшефнасекундуоторвавшисьотсвоихбумагтретьязаметкабылаизкакойтож елтойшотландскойгазетенкиивоттутконечножеавторрассказалстрашнуюисторию просовременныхвампировкоторыевомракеаттракционовсосуткровьсвоихжертвед инственнойоригинальнойдетальюбылоутверждениежурналистачтообычновампи рывысасываютсвоихжертвненасмертьнорусскийстуденткакположенорусскомубы лнастолькопьянчтобедныйшотландскийвампиртожезахмелелиувлексянесмотрян

авсютрагичностьисторииязасмеялсяжелтаяпрессаонавовсеммиреодинаковасказа лгесернеподнимаяглазсамоеужасноечтотаквсеибылосказалякромепьянстваконеч нокружкапивазаобедомсогласилсягесерчетвертаявырезкабылаизкакойтонашейга зетынекрологсоболезнованиялеонидупрохоровудепутатугосударственнойдумыче йсынтрагическипогибявзяллистокфаксаэтокакяипредполагалбылодонесениеотно чногодозорагородаэдинбургашотландиявеликобританиянемножконеобычнымока залсялишьадресатсамгесеранеоперативныйдежурныйилируководительмеждунар одногоотделаитонписьмачутьболееличныйчемполагаетсявофициальныхдокумен тахасодержаниеменянеудивилосприскорбиемсообщаемпорезультатамтщательно проведенногодознанияполнаяпотерякровипризнаковинициацииневыявленопрове денныепоискирезультатовнедалипривлеченылучшиесилыеслимосковскоеотделе ниесчитаетнеобходимымнаправитьпередавайсамыетеплыеприветыольгеоченьрад затебястарыйковторойлистокфаксаотсутствовалвидимотамбылисключительноли чныйтекстпоэтомуиподписиянеувиделфомалермонтсказалгесерглавашотландско годозорастарыйдругагазадумчивопротянулязначитнашивзглядыопятьвстретилис ьнетужродственниклионмихаилуюрьевичусамспросишьсказалгесеряодругомкоэт окомандиркоэтогесерзапнулсяисявнымнедовольствомпокосилсяналистоккоэтоко этотебяуженекасаетсяяпосмотрелнафотографиимолодойчеловекэтоибылбедолага виктордевушкасовсемюнаяегоневестачтотутгадатьимужикпостаршеотецвиктора косвенныеданныеговорятонападениивампиранопочемуситуациятребуетнашегов мешательстваспросилянашисоотечественникичастенькогибнутзарубежомиотвам пировтожевынедоверяетефомеиегоподчиненнымдоверяюноунихмалоопыташотл андиямирнаяуютнаяспокойнаястранаонимогутнесправитьсяатычастенькоимелде лосвампирамиконечноивсетакиделовтомчтоегоотецполитикгесерпоморщилсядак акойонполитикбизнесменпробралсявдепутатынаголосованияхжметкнопкипотихо нькукороткоияснононеверючтонетособойпричиныгесервздохнулотецюношидвад цатьлетназадбылопределенкакпотенциальныйсветлыйинойдовольносильныйоти нициацииотказалсяобъявивчтохочетостатьсячеловекомтемныхсразужепослалпро чьноснамиподдерживалнекоторыеконтактыиногдапомогалякивнулдаслучайредк ийнечастолюдиотказываютсяоттакихвозможностейчтооткрываютсяпередиными можносказатьчтоячувствуюсебявиноватымпередпрохоровымстаршимсказалгесе риеслиужнемогупомочьсынутонепозволюегоубийцеуйтибезнаказаннымтыпоеде шьвэдинбургнайдешьэтогосумасшедшегокровососаиразвеешьповетруэтобылпри казнояибезтогонесобиралсяспоритькояневольнозапнулсякогдалететьзайдивмежд ународныйотделтебедолжныбылиподготовитьдокументыбилетыденьгиилегенду