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:

звонокбылнастырнымдолгимкакпаровозныйгудокмежгородтелефонстоялвприхожейподбольшимовальнымзеркаломикогдазвониламужнинароднямашеказалосьчтозеркалосотрясаетсякакотпроходящегопоездаивотвотупадетказенныйплоскийголосждитемариупольнапроводепоголосамихчтолинаработупринимаютзвонилатамарадвоюроднаясестрамужаобычноонапоздравляласновымгодомилисообщалаосмертиочереднойтеткиуанатолиявмариуполебылцелыйхороводпрестарелойроднимашахотеласразужепередатьемутрубкунотамарасказалапостойкамашяведьименночтоктебеисмущеннойскороговоркойсообщилачтопосленеудачнойоперацииаппендицитавейскепомерлаплемянницатетилидывотэтокакойжететилидыдавидалатыееиплемянницувидаланамоейсвадьбететялидапокойницаонаненамприходитсяроднейасосторонынупошлопоехалокорочестойдругойсторонынемариупольскойаейскоймашадавноужеоставиламноголетниепопыткизапомнитьвсеродственныесвязиизобильноймужниной родниислышыплемянницатопомерланоотнееосталасьдевчоночкатрехлетнуичтоатоявноволнуясьторопливорассказывалатамарачтоэтудевочкуниктоизихнейроднибратьнехочетхотяродняоченьдажзажиточнаядвоюроднаясестрапокойницысамазубнойтехникдомполнаячашаживыеспокойникамивтойроднедружношагалирукаобрукуизродавродвеселоперекликаясьипереругиваясьдоспориваядопеваяпеснюидопиваяшкаликстранноччтоникто изтойроднитактакиинехочетвзятьэтогоребенкамашастиснулазубыегорячисьсказалаонасебениктонесобиралсятебяобидетьникомуделанетдотвоейболитомканаконецсказалаонаспокойнотымневсеэтозачемговоришьтазамялась втрубкешумелравнодушныйприбойчьихтогулкихголосовимашавдругпонялачторадиоэтогоразговоратамараявиласьнателеграфвыстоялаочередькабиненуможетвыподумаетемашсловнобыизвиняясьпроговорилатавсежеувасдетейнетможетэтошанскакникрутиатебеужетридцатьшестьтридцатьчетыреоборваламашаияна деждынетеряюялечусьнукакзнаешьтамарасразусниклапотерялаинтерескразговорутактыителефонанезапишешьбабыэтойдантисткинавсякийслучайимашазачемтозаписалачтобынеобижатьтомкуведьхорошегохочетдурындаэтакаявсеунихпростоуэтихмариупольскихкоровсполнымивыменамионаопустилатрубкуиподнялаголовуизовальноговрезнойчернойрамезеркалананеевнимательносмотрелащемолодаяженщинасподвижнымусыпаннымобаятельнойвеснушчатойкрупкойлицомзаспинойунеевпроемеоткрытойвспальнюдверивиденбылотдыхающийпоследежурствамужегобосаяступняпокачиваласьмаятникомвтакттолимыслямтолимотивчикунапеваемомубеззвучнолицозаслоненоставнемраскрытойкнижкиназваниеиавторопрокинутывзеркальепрочестьневозможнодалееперспективазеркалаявлялаокногдетревожнометаласьнаветруусыпаннаябелымисвечкамикронак

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

Різні ключи :

```
r_2 = "ок"
r_3 = "абв"
r_6 = "примат"
r_18 = "машадождаласькогда"
```

Шматки зашифрованого тексту :

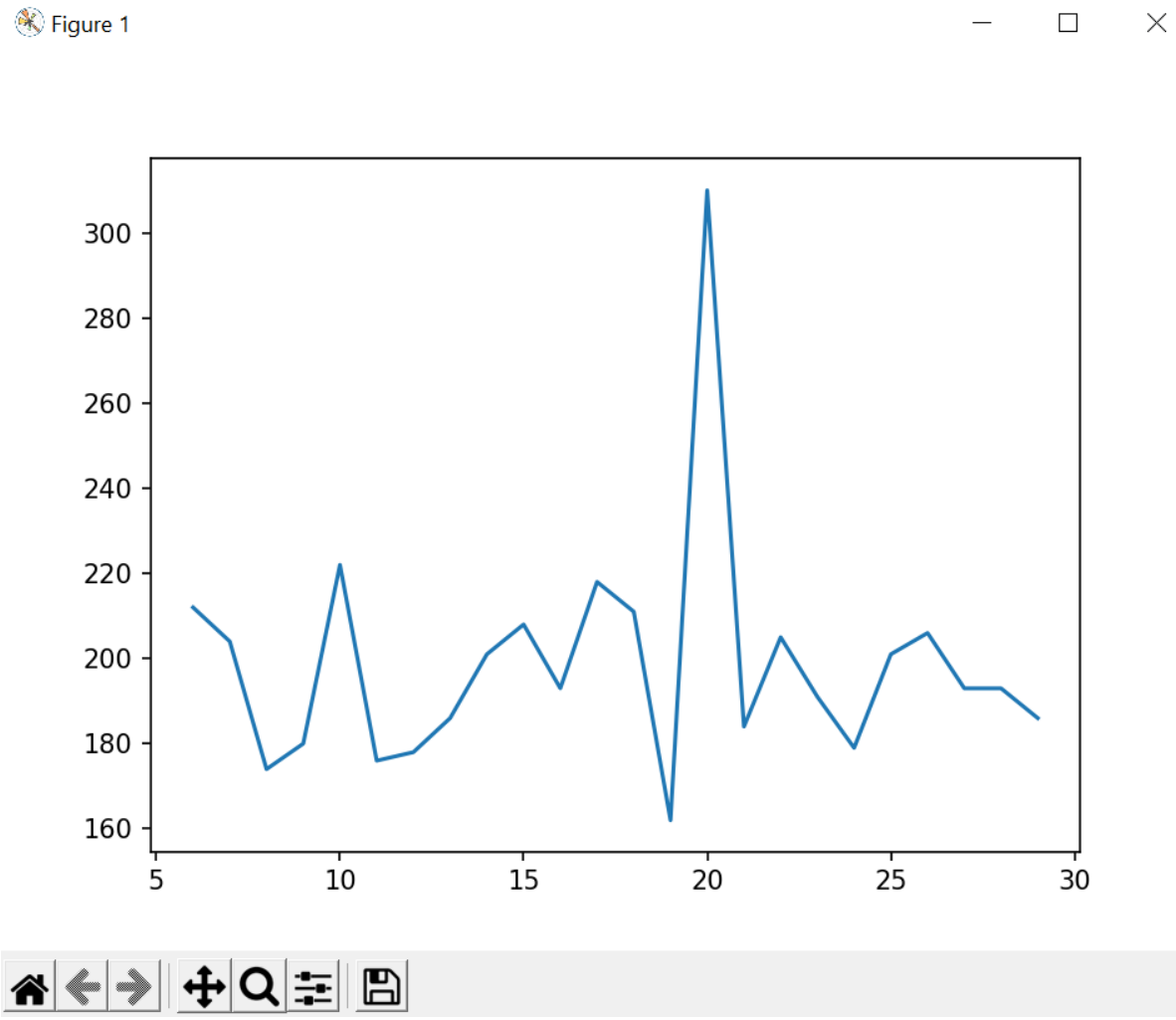
“хмьчьфпещчоыаеючйцтшщнццшкшщоъьмьсыечнбоьфъпфньъьоа”

“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

Графік залежності D від r (r знаходиться в проміжку від 6 до 30):



Обчислені значення D від r:
{6: 212, 7: 204, 8: 174, 9: 180, 10: 222, 11: 176, 12: 178, 13: 186, 14: 201, 15: 208, 16: 193, 17: 218, 18: 211, 19: 162, 20: 310, 21: 184, 22: 205, 23: 191, 24: 179, 25: 201, 26: 206, 27: 193, 28: 193, 29: 186, 30: 234}

Максимальні значення D:
D =212, r = 6
D =222, r =10
D =310 r =20
Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастіший літері мови : ” улановсеребзяныепуля”

Скориговане значення ключа (за необхідності) : ” улановсеребряныепули”

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

Фрагмент значень, отриманих для функції *M* для кожного блоку при різних g:

	g = 0	g = 1	g = 2	g = 3	g = 4	g = 5	g = 6	g = 7	g = 8	g = 9	g = 10	g = 11
Y0	8.66783	9.14128	7.10604	7.84443	7.75034	9.18574	8.88337	7.81922	8.15065	8.76492	9.97413	8.79839
Y1	7.43209	8.03722	9.66040	8.64511	7.34103	10.21221	11.24517	10.67333	12.09076	11.16756	11.90053	16.91383
Y2	17.13607	10.71495	10.15790	11.73411	10.11780	11.55806	10.09677	7.07179	8.89975	9.89197	8.68488	8.01223
Y3	9.08543	7.47096	7.10557	7.50274	9.40083	9.22829	7.15325	9.29980	10.94550	10.99254	12.71498	11.29653
Y4	9.44365	8.68850	7.08648	7.05407	7.22603	9.16654	8.87337	6.82451	9.39119	10.53114	10.38072	12.64979
Y5	10.08216	12.56126	16.32573	10.49895	11.72834	11.96845	10.27179	12.30854	9.61000	7.54731	10.05649	8.94902
Y6	7.56592	7.68777	8.22614	10.34500	8.75761	6.90303	6.78314	8.12952	9.33631	8.09648	6.17344	9.40200
Y7	10.92972	10.83683	12.44244	10.73865	10.98103	17.02185	11.55850	11.13547	11.49705	11.13270	11.84954	9.89146
Y8	7.97513	7.03281	10.08878	9.22192	7.35134	7.56665	8.09271	10.01388	8.80995	7.15540	9.70673	11.23209
Y9	10.88751	10.83384	13.34533	10.64894	11.08795	16.09680	10.32408	10.80160	12.42584	9.49135	11.16454	10.54244
Y10	11.00731	17.63469	11.45760	10.02386	11.97501	10.39759	11.95633	9.77175	7.03784	9.60268	9.65302	8.49921
Y11	8.15924	7.74052	9.92280	8.96286	7.20718	7.81078	7.80993	9.90858	9.05999	7.13599	9.51529	10.82752
Y12	10.99679	10.43639	12.45565	10.34264	11.28379	10.13677	6.80497	8.54766	10.08380	8.09832	7.28360	7.02500
Y13	8.33737	6.87777	7.63684	8.02797	9.83791	8.55137	7.79925	10.46372	10.71012	10.53905	12.65105	10.61508
Y14	10.83864	10.49611	7.45055	8.72545	10.09155	8.69592	7.52422	7.62904	8.67411	9.80948	7.41399	8.18416
Y15	10.66834	10.90585	12.95378	11.40997	11.69948	16.87744	11.53700	11.41528	12.68690	9.95163	10.95459	9.85019
Y16	6.87246	9.47154	9.27421	6.79716	6.96090	8.06267	8.92140	8.49226	6.84626	8.59338	10.72827	10.41350
Y17	8.97214	9.52659	7.58836	7.43128	8.03476	9.20317	8.72154	7.99479	7.55123	8.70685	9.78228	8.38500

(червоним обведено максимальні значення, для тих блоків, які влізли)
Всю таблицю можна подивитись в `'myfile.csv'`

Фрагмент шифрованого тексту:
рэаюцугкьелаяюиутбхигцичопщпюиермтгсфюлхутвныкрчюрэънфожэчыцфутт щююуфрйэмидтэяршххаяоняихнтбктяусунаыфетшкткампэгынсфеууаллхекцча кцуяфйзкиорцлняьдхзгъббстлуччшгиъошулыуьк“”

Фрагмент розшифрованого тексту:
“этасистемакрасногокарликаникогданеимеланазваниятолькозубодробительно длинныйномервкаталогеисследовавшийеекиберзонд”