

Міністерство освіти і науки України

НТУУ «Київський політехнічний інститут»

Фізико-технічний інститут

**CИМЕТРИЧНА КРИПТОГРАФІЯ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3**

**Криптоаналіз афінної біграмної підстановки**

**5 Варіант**

**Виконали:**

Студенти групи ФI-52

Кратт Я.

Бурлака М.

2018

**Мета роботи**

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

**Хід роботи**

1. Знаходимо 10 найчастіших біграм для зашифрованого тексту.

2. Розв’язування систем лінійних порівнянь для різних варінатів переходів біграм.

3. Дешифрування тексту за допомогою отриманих ключів при розв’язанні системи лінійних порівнянь.

4. Розпізнавання змістовного тексту за энтропійним та частотним критеріями.

**Знайдені ключі**

количество совпавших по частоте букв: 25

отличие энропий: 0.013193552204448622

keys: 654 777

**ВТ**

убиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарныминачепришлосьбыубиватьсамомуэтонеоднолишьдоброесостраданиеэтоотождествлениенаоснованииодинаковыхимпульсовкубийствусобственноговорялишьвминимальнойстепенисмещенныйнарциссизмэтическаяценностьэтойдобротыэтимнеоспариваетсяможетбытьэтовообщемеханизмнашегодоброгоучастияпоотношениюкдругомучеловекуособеннояснопроступающийвчрезвычайномслучаеобремененногосознаниясвоейвиныписателянетсомнениячтоэтасимпатияпопричинеотождествлениярешительноопределилавыборматериаладостоевскогоносначалаонизэгоистическихпобужденийвыводилобыкновенногопреступникаполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпервопреступникукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопубликованиеегопосмертногонаследияидневниковегоженыяркоосветилоодинэпизодегожизнитовремякогдадостоевскийвгерманиибылобуреваемигорнойстрастьюдостоевскийзарулеткойявныйприпадокпатологическойстрастикоторыйнеподдаетсяинойоценкенискакойсторонынебылонедостаткавоправданияхэтогостранногоинедостойногоповедениячувствовиныкакэтонередкобываетуневротиковнашлоконкретнуюзаменувобремененностидолгамиидостоевскиймоготговариватьсятемчтоонпривыигрышеполучилбывозможностьвернутьсявроссиюизбежавзаключениявтюрьмукредитораминоэтобылтолькопредлогдостоевскийбылдостаточнопроницателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналчтоглавнымбылаиграсамапосебевсеподробностиегообусловленногопервичнымипозывамибезрассудногоповеденияслужаттомудоказательствомиещекоечемуиномуоннеуспокаивалсяпоканетерялвсегоиграбыладлянеготакжесредствомсамонаказаниянесчетноеколичествораздавалонмолодойженесловоиличестноесловобольшенеигратьилинеигратьвэтотденьионнарушалэтословокаконарассказываетпочтивсегдаеслионсвоимипроигрышамидоводилсебяиеедокрайнебедственногоположенияэтослужилодлянегоещеоднимпатологическимудовлетворениемонмогпереднеюпоноситьиунижатьсебяпроситьеепрезиратьегораскаиватьсявтомчтоонавышлазамужзанегостарогогрешникаипослевсейэтойразгрузкисовестинаследующийденьиграначиналасьсноваимолодаяженапривыклакэтомуциклутаккакзаметилачтотоотчеговдействительноститолькоиможнобылоожидатьспасенияписательствоникогданепродвигалосьвпередлучшечемпослепотеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоонаконечнонепонималакогдаегочувствовиныбылоудовлетворенонаказаниямиккоторымонсамсебяприговорилтогдаисчезалазатрудненностьвработетогдаонпозволялсебесделатьнесколькошаговнапутикуспехурассматриваярассказболеемолодогописателянетрудноугадатькакиедавнопозабытыедетскиепереживаниянаходятвыявлениявигорнойстрастиустефанацвейгапосвятившегомеждупрочимдостоевскомуодинизсвоихочерковтримастеравсборникесмятениечувствестьновелладвадцатьчетыречасавжизниженщиныэтотмаленькийшедеврпоказываеткакбудтолишьтокакимбезответственнымсуществомявляетсяженщинаинакакиеудивительныедлянеесамойзакононарушенияеетолкаетнеожиданноежизненноевпечатлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкованиюговоритоднакобезтакойоправдывающейтенденциигораздобольшепоказываетсовсеминоеобщечеловеческоеилискорееобщемужскоеитакоетолкованиестольявноподсказаночтонетвозможностиегонедопуститьдлясущностихудожественноготворчествахарактерночтописательскоторымменясвязываютдружескиеотношениявответнамоирасспросыутверждалчтоупомянутоетолкованиеемучуждоивовсеневходиловегонамерениянесмотрянаточтоврассказвплетенынекоторыедеталикакбырассчитанныенаточтобыуказыватьнатайныйследвэтойновеллевеликосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережитьболеедвадцатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейболеененуждалисьотказавшаясяоткакихбытонибылонадежднасороквторомгодужизнионапопадаетвовремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакскогоказиногдесредивсехдиковинеевниманиеприковываютдверукикоторыеспотрясающейнепосредственностьюисилойотражаютвсепереживаемыенесчастнымигрокомчувстварукиэтирукикрасивогоюношиписателькакбыбезовсякогоумысладелаетегоровесникомстаршегосынанаблюдающейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобывпаркепокончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщинуследоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуизмногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидаетегоивынужденавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитьегопостельпослеэтойимпровизированнойлюбовнойночионавелитказалосьбыуспокоившемусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетигратьснабжаетегоденьгаминаобратныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпередуходомпоезданавокзаленозатемвнейпробуждаетсябольшаянежностькюношеонаготовапожертвоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместевпутешествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееионаопаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприходитвигорныйдомисвозмущениемобнаруживаеттамтежерукинакануневозбудившиевнейтакуюгорячуюсимпатиюнарушительдолгавернулсякигреонанапоминаетемуобегообещанииноодержимыйстрастьюонбранитсорвавшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозореннаяонапокидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсамоубийстваэтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечноправонасуществованиекактаковаяинеможетнепроизвестиначитателябольшоговпечатленияоднакопсихоанализучитчтоонавозникланаосновеумопострояемоговожделенияпериодаполовогосозреванияокаковомвожделениинекоторыевспоминаютсовершенносознательносогласноумопострояемомувожделениюматьдолжнасамаввестиюношувполовуюжизньдляспасенияегоотзаслуживающегоопасениявредаонанизмастольчастыесублимирующиехудожественныепроизведениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательскисвидетельствуетобэтомотводеэнергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпотребностивонанизмениоднимсловомкромесловаигранельзяназватьетееааубиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарныминачепришлосьбыубиватьсамомуэтонеоднолишьдоброесостраданиеэтоотождествлениенаоснованииодинаковыхимпульсовкубийствусобственноговорялишьвминимальнойстепенисмещенныйнарциссизмэтическаяценностьэтойдобротыэтимнеоспариваетсяможетбытьэтовообщемеханизмнашегодоброгоучастияпоотношениюкдругомучеловекуособеннояснопроступающийвчрезвычайномслучаеобремененногосознаниясвоейвиныписателянетсомнениячтоэтасимпатияпопричинеотождествлениярешительноопределилавыборматериаладостоевскогоносначалаонизэгоистическихпобужденийвыводилобыкновенногопреступникаполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпервопреступникукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопубликованиеегопосмертногонаследияидневниковегоженыяркоосветилоодинэпизодегожизнитовремякогдадостоевскийвгерманиибылобуреваемигорнойстрастьюдостоевскийзарулеткойявныйприпадокпатологическойстрастикоторыйнеподдаетсяинойоценкенискакойсторонынебылонедостаткавоправданияхэтогостранногоинедостойногоповедениячувствовиныкакэтонередкобываетуневротиковнашлоконкретнуюзаменувобремененностидолгамиидостоевскиймоготговариватьсятемчтоонпривыигрышеполучилбывозможностьвернутьсявроссиюизбежавзаключениявтюрьмукредитораминоэтобылтолькопредлогдостоевскийбылдостаточнопроницателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналчтоглавнымбылаиграсамапосебевсеподробностиегообусловленногопервичнымипозывамибезрассудногоповеденияслужаттомудоказательствомиещекоечемуиномуоннеуспокаивалсяпоканетерялвсегоиграбыладлянеготакжесредствомсамонаказаниянесчетноеколичествораздавалонмолодойженесловоиличестноесловобольшенеигратьилинеигратьвэтотденьионнарушалэтословокаконарассказываетпочтивсегдаеслионсвоимипроигрышамидоводилсебяиеедокрайнебедственногоположенияэтослужилодлянегоещеоднимпатологическимудовлетворениемонмогпереднеюпоноситьиунижатьсебяпроситьеепрезиратьегораскаиватьсявтомчтоонавышлазамужзанегостарогогрешникаипослевсейэтойразгрузкисовестинаследующийденьиграначиналасьсноваимолодаяженапривыклакэтомуциклутаккакзаметилачтотоотчеговдействительноститолькоиможнобылоожидатьспасенияписательствоникогданепродвигалосьвпередлучшечемпослепотеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоонаконечнонепонималакогдаегочувствовиныбылоудовлетворенонаказаниямиккоторымонсамсебяприговорилтогдаисчезалазатрудненностьвработетогдаонпозволялсебесделатьнесколькошаговнапутикуспехурассматриваярассказболеемолодогописателянетрудноугадатькакиедавнопозабытыедетскиепереживаниянаходятвыявлениявигорнойстрастиустефанацвейгапосвятившегомеждупрочимдостоевскомуодинизсвоихочерковтримастеравсборникесмятениечувствестьновелладвадцатьчетыречасавжизниженщиныэтотмаленькийшедеврпоказываеткакбудтолишьтокакимбезответственнымсуществомявляетсяженщинаинакакиеудивительныедлянеесамойзакононарушенияеетолкаетнеожиданноежизненноевпечатлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкованиюговоритоднакобезтакойоправдывающейтенденциигораздобольшепоказываетсовсеминоеобщечеловеческоеилискорееобщемужскоеитакоетолкованиестольявноподсказаночтонетвозможностиегонедопуститьдлясущностихудожественноготворчествахарактерночтописательскоторымменясвязываютдружескиеотношениявответнамоирасспросыутверждалчтоупомянутоетолкованиеемучуждоивовсеневходиловегонамерениянесмотрянаточтоврассказвплетенынекоторыедеталикакбырассчитанныенаточтобыуказыватьнатайныйследвэтойновеллевеликосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережитьболеедвадцатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейболеененуждалисьотказавшаясяоткакихбытонибылонадежднасороквторомгодужизнионапопадаетвовремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакскогоказиногдесредивсехдиковинеевниманиеприковываютдверукикоторыеспотрясающейнепосредственностьюисилойотражаютвсепереживаемыенесчастнымигрокомчувстварукиэтирукикрасивогоюношиписателькакбыбезовсякогоумысладелаетегоровесникомстаршегосынанаблюдающейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобывпаркепокончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщинуследоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуизмногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидаетегои

вынужденавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитьегопостельпослеэтойимпровизированнойлюбовнойночионавелитказалосьбыуспокоившемусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетигратьснабжаетегоденьгаминаобратныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпередуходомпоезданавокзаленозатемвнейпробуждаетсябольшаянежностькюношеонаготовапожертвоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместевпутешествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееионаопаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприходитвигорныйдомисвозмущениемобнаруживаеттамтежерукинакануневозбудившиевнейтакуюгорячуюсимпатиюнарушительдолгавернулсякигреонанапоминаетемуобегообещанииноодержимыйстрастьюонбранитсорвавшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозореннаяонапокидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсамоубийстваэтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечноправонасуществованиекактаковаяинеможетнепроизвестиначитателябольшоговпечатленияоднакопсихоанализучитчтоонавозникланаосновеумопострояемоговожделенияпериодаполовогосозреванияокаковомвожделениинекоторыевспоминаютсовершенносознательносогласноумопострояемомувожделениюматьдолжнасамаввестиюношувполовуюжизньдляспасенияегоотзаслуживающегоопасениявредаонанизмастольчастыесублимирующиехудожественныепроизведениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательскисвидетельствуетобэтомотводеэнергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпотребностивонанизмениоднимсловомкромесловаигранельзяназватьетееаа

**Розпізнавання тексту**

Автоматичне розпізнавання здійснюється в два етапи:

1. На основі частот найчастіших букв у російській мові. Якщо хоча б одне значення частот цих літер відкланяється від еталонного значення більше ніж значення точності, то це не є текст.
2. На основі різниці ентропій шифротексту та російскої мови.

**Висновок**

Отже, в ході Практикума ми засвоїли навички криптоаналізу та атаки на шифр афінної підстановки. Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.