КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

ФБ-11 Подолянко Тимофій

Варіант №13

Хід роботи

Реалізовано програму на мові Python, яка підбирає ключ шифрування заданого шифртексту, зашифрованого методом афінної підстановки біграм.

Приклад виконання:

```
PS>python .\main.py -h
usage: main.py [-h] [--top TOP] [--use-known-bigrams] file clearfile

positional arguments:
  file                  file of cyphertext
  clearfile             file which will be used as a sample for frequency analysis

options:
  -h, --help            show this help message and exit
  --top TOP             how many most frequent bigrams should be checked
  --use-known-bigrams   whether to use known top 5 most frequent bigrams (will be included in total --top count, before the ones sampled from clearfile)
```

```
PS>python  .\main.py .\data\13.txt ..\..\cp1\podolianko_fb-11_cp1\data\sample.txt --top 7 --use-known-bigrams
Using ..\..\cp1\podolianko_fb-11_cp1\data\sample.txt as a sample...
Sample text entropy: 4.452402965145536
Prioritising these known top 5 cleartext bigrams: ['ст', 'но', 'то', 'на', 'ен']
Top 7 cleartext bigrams (actually considered): ['ст', 'но', 'то', 'на', 'ен', 'то', 'не']
Top 7 cyphertext bigrams: ['аф', 'яф', 'дю', 'ап', 'нф', 'хб', 'ло']
Total candidates: 493
Trying to reduce the number by running a few test...
Keys remaining: 1
Key: (99, 60)
раннееранненеутропервыеотсветызаринакрышезаокномвселистьянадеревьяхвздрагиваютотзываясьнамалейшеедуновениепредрассветноговетеркаивотгдетодалекоиззаповоротана
серебряныхрельсахпоявляетсятрамвайпокачиваясьначетырехмаленькихсероголубыхколесахяркооранжевыйкакмандариннанемэполетымерцающеймедиизолотойкантпроводовижелты
йзвонокгромкозвякаетедвадопотопныйвожатыйстукнетпонемуногойвстоптанномбашмакецифрынабокахтрамваяисперединяркозолотыекаклимонсиденьяточнопорослипрохладнымзеле
ныммхомнакрышесловнозанесеногромныйкучерскойбичнабегуонскользитпосеребряноїпаутинепротянутойвысокосредидеревьевизвсехоконбудтоладаномпахнетвсепроникающимгол
убымизагадочнымзапахомлетнихгрозимолнийтрамвайзвенитвдольокаймленныхвязамиулициобтянутаясеройперчаткойрукавожатогоопятьиопятьлегкокасаетсярукоятокволденьво
жатыйостановилвагонпосредикварталаивысунулсявокошкоэйизавидевпризывныйвзмахсеройперчаткидугласчарлитомвсемальчишкиидевчонкивсегокварталакубаремскатилисьсдер
евьевпобросаливтравускакалкионитакиостались,лежатьсловнобелыезмеиипобежаликтрамваюнорасселисьпозеленымплюшевымсиденьяминиктоснихнеспросилникакойплатымистерт
ридденвожатыйположилперчаткунащелькассиповелтрамвайдальшепотенистымулицамгромкозвякаязвонкомэйсказалчарликудаэтомыедемпоследнийрейсответилтридденглядявпере
днабегущиевысоконадвагономпроводабольшетрамваянебудетзавтрапойдетавтобусаменяотправляютнапенсиюводкакипотомупокатайтесьнапоследоквсембесплатноосторожноонрыв
комповернулмедноюрукояткутрамвайзаскрипеликрутосвернулописьвяябесконечнуюзеленуюпетлюисамовремянавсембеломсветезамерлотолькотридденидетиплыливегоудивительно
йашинекудатодалекопонескончаемойрекенапоследокпересросилудивленныйдугласдакажетакибезтоговсеплохозеленоймашиныбольшенетеезаперливгаражеиникакееоттуданевы
зволишьимоиновыетеннисныетуфлиужестановятсясовсемстарымибегутвсемедленнеимедленнеекакжеятеперьбудунетнетнемогутониубратьтрамвайчтониговоривтобусэтонетрам
вайонишумитнетакрельсовунегонетпроводовнетонискрынеразбрасываетрельсыпескомнепосыпаетдаицветунегонетакойизвонканетиподножкуоннеспускаетаведьверноподхватил
чарлистрахлюблюсмотретькогдатрамвайспускаетподножкупрямогармоникатотоионосказалдугластутониприехалинаконечнуюостановкувпрочемсеребряныерельсызаброшенныевосе
мнадцатьлетназадбежалисредихолмовдальшевтысячадевятьсотдесятомгодутрамваемездилиназагородныепрогулкивчесменпаркприхвативогромныекорзиныспровизиейстехпоррель
сытакиостались,ржаветьсредихолмовтуттомыиповорачиваемназадсказалчарлитуттотыиошибсяимистертридденщелкнулвыключателемаварийногогенераторапоехалитрамвайдернулс
яскользнулпорельсамиоставивпозадигородскиеокраинынокатилсявнизвдолинуонтовылеталнадушистыезалитыесолнцемлужайкитонырялподтенистыедеревьягдепахлогрибамитамис
ямколеюпересекалиручейкисолнцепросвечивалосквозьлиствудеревьевточносквозьзеленоестекловагонтихонькобормочачтотопросебяскользилполугамусеяннымдикимиподсолнух
амимимодавнозаброшенныхстанцийусыпанныхсловноконфеттистарымитрамвайнымибилетамиивследзалеснымручьемустремлялсявлетниелесатрамвайондажепахнетпоособенномугово
рилдуглассидилявчикагонаавтобусахутехкакойточудной запахтрамвайчересчурмедленноходитсказалмистертридденвотониихотятпустить погородуавтобусыиребятвшколутожеста
нутвозитьваватобусахтрамвайвзвизгнулиостановилсятриддендосталсверхукорзинуспровизиейребятавосторженноназавопилиивместеснимпотащиликорзинунатравутудагдеручейвпа
далвмолчаливоеозероздесьнекогдапоставилиэстрадудляоркестранотенерьонасовсемрассыпаетсявпрахонисиделинатравеуплеталисандвичисветчинойсвежуюклубникуияркиеблес
тящиеточновосковыеапельсиныитридденрассказывалкакмноголетназадтутповечерам


Actual entropy per character: 4.423510398163551
Actual top letter frequencies: [('о', '9.812%'), ('е', '9.298%'), ('а', '8.414%'), ('т', '6.503%'), ('н', '6.361%'), ('и', '6.275%'), ('с', '5.305%'), ('р',
 '5.220%'), ('в', '5.077%'), ('л', '4.792%')]
```

В результаті частотного аналізу запропонованого шифртексту отримано такі 5 найчастіших біграм у порядку спадання: 'аф', 'яф', 'дю', 'ап', 'нф'.

В якості розпізнавача російськомовного тексту використано комбінацію з двох критеріїв: перевірку, що значення ентропії нижче за певний пороговий рівень; перевірку, що частота у розшифрованому тексті найбільш частих літер з тексту-зразка більша за деяке порогове значення. Тексти, які не проходять перевірку, відкидаються разом із відповідними ключами. Параметри для обох перевірок встановлені емпірично.

Застосований розпізнавач спирається на такі факти: ентропія звичайного тексту менша у порівнянні з ентропією довільного шифртексту через надлишковість мови; Частоти літер у довільному (природньому) тексті прямують до теоретичних за довжини, що прямує до нескінченності.

Цих двох перевірок достатньо для однозначного визначення ключів шифрування запропонованих у варіанті текстів.

Шифротекст варіанту

хжнафлхкзлтифтьозкзлтишибиыоыоллнлршюнтосочитицбнхщотавптуряпнппуоирмлчфподуряхядюрйло
дмгьаияэлоспвшзслраялфбхыхгаююдеухкяыаяэйинюдеяотрсигейдроыеэрыэщпабапбущпабапбубирязи
нлыржтрахаплисжжысерыэплтиувйоафтипееомпдуыхдуувзыспкрмуняржхибоьорожислжниулрщрфефжпл
бящптехкчыьщбижихяиашхвкдеувюшыхдуаюстяенщоиплфейдроыеэрцяиимшщоьосизинамючиринлэльрбх
ертазаповрршгусорхюлыхфнранарисклрсоиапхлрбеэрбнхябирязинликлхтугуэргаххткцсзлаптеэрсо
ьшыхдуиюжуапбтиркищьюлюфмжлепщюенийгяэмпмзмуюгапхнряниэуфопорайешынахайнирмлтияявяхеув
лрршгуафеосозлтияэувсблрцяыиыятимжйиуюыхфцхжяэмждвдкрдфооуцждяхяэодлтихяххюлхйдефнмжбя
плаювуюеэаддхеднппбтирсунгьоэоэаяяряуфцжреьщчязяйугржхьияэуввцдежхаюплтиуваияэлоспвшзс
лраяйфбхыхпьхщфжиаыавпягыяиунгьоэовифяхажяжепщьргабячоафмщранаяяаияэлоспвшзслраяйфбхых
ирсптепфьргабячоафеоранарийоыофсзгмуртмигуцждяделрважхгезлисгадозшбяихбыспкшоолюлрркзг
мираххфнбехкажвпаюфнхяепихтдйяцямлбхйдзиырькжьтихпзсувэжраяфмьплтиувырцйршмиуехкюлбхьр
ираяхяьавихянюенслжнджриболлцаконааимигаряьапзршисьрмийеьщххнгвююефнмжбяплаюашэрцяряуи
зявасоенсеуяыаяэтоюфспзслрлюшыбяуаяяиргезгкубышмцякдйхягщпзлхекпиюеивиыябраюьороыевшэр
эргагефнфефжплбяюлбхйдзидозшбяцаэоффйжнауеячмаэахячоафвшыхтдйяцякржхюеярьояяплтиеюэрга
зенщоюнайвтаэрэауехкзфхеукзслраягыпфтдзлапбкдозшбячдюеткоогайеляэыйхмвпклрдынайдхаррлю
аююывифжнжвицохорясуэрцякпчфхкраригыбяфпйдюлаптеялртажцдесизрбовящпьргахапзмщбхаюдеоч
маэахячоафвшыхтдйяцянюдеухкяиаплиюеннлпфспшыэртиуедеттнрйичыбяфпйдюлаптеэрчалюнлпляжнл
бхаюштииаявошхшыьщафгьплтиффчфтафлишщпфнухфцфнщхмийуфнлодкяллнвииацхюебтнолреапзфоялпл
иююееоялдофжтялфбыюлщпьрцячоафгьплтишкэадятуэрцяпорянюдеухкяуегхдуэаоькдыщплдомвщоенсл
жнххткцйфжвинайеукиатаплиюхоряяюоиплэаплцавибирязинлбохюжороплаюхяьотаххлядюдупляжвифж
нжвицохорямлчфгьйялацынафжыцкяягтиаищвыиязьщххукммхоыеэрцясижчхоулнайдробясояэувзыбяыа
двиюгаджявлхтуплыибитящвтиплдемщпхукнлвшэржхюеиюуаяялюрнсоефжютутзгьрасжритрлюхятиталх
тулофжтохалжххлядюдупляжхоситрлюягжюрчхожхспькыюцояэафукуащнцрлюоюдеухфнбирязинлдуэайд
бохюжьроплскщхзышынайдхаррлюьемурмьеерапдефнэрэауежьцояэафдькдыщплдоыежьххдухфгаидйхви
ткkреиииэйзыбжнажипеэрцяемдеецняхжхжщжтвбхаюшттидююлфнфяхабеаюдуплыизфйыыхмжэрэауежьйя
лаырапщрмауащнцрлюдеэараявеэшяжяномвфынафжулаютабоьохауфькгаыилежьухрдаючыернифянаююти
шснлдемурмьеерапдефндозшбячдюеткоокльоыэвклргаскщххжайеткйдыияежьербоулаюялтижиязгьсима
пзеоииаяйыфцвбзслраяцсйхщвплтиувнюенnлжниаялэаторяжапуаптежьцоулыхаюдоачмаэахяыорасжри
трлюдеэарамашыйхзляюэаракяйуяюгугияээараоиплэарадфялыххклааийяыяаэцыэрхойефошхвккрройи
ыеиошайкярягплдоыеэрцячыьомылнцякрфеэржхюеувлжоиплеокюдозшбяофчфяюохишгьхаплисэаоюнабо
цраяшржхюемьламалцмьралахаххтуапбтношлдещолцеошгупшыаюммдееоялщояээарадонирасжритрлюде
увзямашыйхзляюувфыьомыбямлмщзлчфпоиапхфздееонаыяфеяяйяфжщптевшэрюфгатиашдуегупххфемлби
маэауащнцрлюдеувуатэтуфедефнзяехршчпщхмоиржыыхсупфягтиьаыиряшящомлаптеэрцяыртьшайкуащн
црлюдеувуаюхтдаююемщкпиюувзыспийдефнцлвшкдчфхеерkдриряйхиюувэжвпаюмщепсуднсояээаплкяма
ффбхдевящхтдыязежьуащнцрлюдеувуачшюейдоцмщзсербежьххтуххфнцящюцоххтуххфнцягешдиюьрткча
клчыерягплдоыеэрцявитиуежьххиюмььодяплбяцжслжнйыфцьияэувзркуукшхфопльогачшаюжьмяйквиду
фечфаюжьгрзайясьххляфьдуюлвизараягзапоряоюцоылчыаюххтуххфнцящюгтыаоькдыщплдоыеукяггояя
лорятквшелххфеткзлюжоиплеофеэржхюеувршгинуюелилрыягьнфмизкдезмзынаэодлзлхенльоджнлжнйы
фцьияээаратияхшмдефнепячгараххрчгалждозшбяюгупкяломагадвжаиайоыеэрцяжсербеэрцяягмирияз
еоьощптенщниваплхнсояээаплртмашыйхзляюыыспосрпймщхпфжотийынаплтилоряденлспмфаюцояэафук
уащнцрлюршщохегуьтлюцотынафжыцкяэаяюххукммхоыеэрцяплнаюлапщрлюнлыхраппрлрзоьогрржухцсия
щогапхяыувлфчаботицяуежьххтуххфнцясьмагадвзыэрхатказиымииаийлтьрячоафнщхаыхойдеэаплкяых
хирябивячынайдхаррлюйжйышмэамаффбхщхщтиррасжритрлюдеувхяпхукнлвшаююшдумьфеяяйяфжщптежо
ьоровпдерячоплхаплщпляухзлэюрйжжнхспэюххлядюдуплдотажхнгюлапщраыылаюгхаюшхкдрязенщгачш
аюхоцаиайоыеаюубйхпжвпишэупжщояэувщюлрриыевшэрюфгатиувлоххоюммоогайечфчайеэрганаыегных
еодлоцфнвитамвторяпжщояээарадонирасжритрлюдеувзямашыйхзляюувфыьомыбямлмщххяюапчфщкдезм
деттдятфэрцяофхехжьодлэртаиашеэрцяххлядюдуплыисрряпоряшораыбзоуляюэаплчысчгалжафхеуиюш
дуаютароьотидюйхщвыирянюплтилозфхеукзслраяцхсбыхехспесербевшэрюфгатиплщпиюкдтиплзльлук
гртаиаарлюающпаюдощорялррариэозаралнриэамвуачшюейдоццаыежьшайкфеяяйяфжщптевшлямабпюфця
уевшшыьомыбярязисояэплыииаиуюееоыахонгмираххфнбежьгрзайяюькдыщплхаыирясуенрояфгььоровп

дерямаююлвштуспхсербевшэрюфгатиуеоццавияээаоудьдутуэрцякпчфсыбяфпйдюлаптеляххдуспжинлжюапзсяюзлщрмлвшрисихжщояэувщюлррасжритрлюдеувфыьомыбямлмщжейдрпжнлалаенмашыйхзляюэарацоулыхааплщперэюэозааебыьояевкбхаюлонфхеэоюшдуаююдеухкягрмабязааэйдролоряоюиаялэаторяцапуаптежьшайкиаарлюдеэапляюиаялдоирлюкясжлюйхяяимьщжнмалцзывяьщтидююлфндвэазевшдькдыщплыидкшмюеэарацячиххтутамихинлжнрлаюфпзйхщчятыйхцафжщояэувщюлррасжритрлюдеуваькдыщплдоыежьыххирябивяцрпфтицяирсучаряиацхюемлжнисоюгуэаыяьэшхсужажхерхоюуягвюьтноеябнпозатынашвюпдеэапльииияйоюубйхзынайдхаррлюдеэаеяибтиплцжулбхщажеаюэавклргабинкелдкшмюеувлиыццалолеиозсербеиоххтуххфнцяеайеаюьороыеаюкштилеукцоулыхдеькнлрпэрхыьотктзлрлюдеэайхтдйяцящяйуяюгугияэувябйхвкйхафгьуащнцрлюлахадевинюдеухфнсвмикштилеляйугржхьияэувмшэркугхплхазрялпл

Розшифрований текст

Ключ: (a=99, b=60)

раннееранееутропервыеотсветызаринакрышезаокномвселистьянадеревьяхвздрагиваютотзываясь намалейшеедуновениепредрассветноговетеркаивотгдетодалекоиззаповоротанасеребряныхрельса хпоявляетсятрамвайпокачиваясьначетырехмаленькихсероголубыхколесахяркооранжевыйкакманда риннанемэполетымерцающеймедиизолотойкантпроводовижелтыйзвонокгромкозвякаетедвадопотопн ыйвожатыйстукнетпонемуногойвстоптанномбашмакецифрынабокахтрамваяиспередияркозолотыекак лимонсиденьяточнопорослипрохладнымзеленыммхомнакрышесловнозанесеногромныйкучерскойбичн абегуонскользитпосеребрянойпаутинепротянутойвысокосредидеревьевизвсехоконбудтоладаномп ахнетвсепроникающимголубымизагадочнымзапахомлетнихгрозимолнийтрамвайзвенитвдольокаймле нныхвязамиулициобтянутаясеройперчаткойрукавожатогоопятьиопятьлегкокасаетсярукоятоквпол деньвожатыйостановилвагонпосредикварталаивысунулсявокошкоэйизавидевпризывныйвзмахсерой перчаткидугласчарлитомвсемальчишкиидевчонкивсегокварталакубаремскатилисьсдеревьевпобро саливтравускакалкионитакиосталисьлежатьсловнобелыезмеиипобежаликтрамваюонирасселисьпоз еленымплюшевымсиденьяминиктоснихнеспросилникакойплатымистертридденвожатыйположилперчат кунащелькассыиповелтрамвайдальшепотенистымулицамгромкозвякаязвонкомэйсказалчарликудаэт омыедемпоследнийрейсответилтридденглядявпереднабегущиевысоконадвагономпроводабольшетра мваянебудетзавтрапойдетавтобусаменяотправляютнапенсиювоткакипотомупокатайтесьнапоследо квсембесплатноосторожноонрывкомповернулмеднуюрукояткутрамвайзаскрипеликрутосвернулопис ываябесконечнуюзеленуюпетлюисамовремянавсембеломсветезамерлотолькотридденидетиплыливег оудивительноймашинекудатодалекопонескончаемойрекенапоследокпереспросилудивленныйдуглас дакакжетакибезтоговсеплохозеленоймашиныбольшенетеезаперливгаражеиникакееоттуданевызвол ишьимоиновыетеннисныетуфлиужестановятсясовсемстарымиибегутвсемедленнееимедленнеекакжея теперьбудунетнетнемогутониубратьтрамвайчтониговориавтобусэтонетрамвайонишумитнетакрель совунегонетпроводовнетониискрынеразбрасываетирельсыпескомнепосыпаетдаицветунегонетакой извонканетиподножкуоннеспускаетаведьверноподхватилчарлистрахлюблюсмотретькогдатрамвайс пускаетподножкупрямогармоникатотоионосказалдугластутониприехалинаконечнуюостановкувпро чемсеребряныерельсызаброшенныевосемнадцатьлетназадбежалисредихолмовдальшевтысячадевять сотдесятомгодутрамваемездилиназагородныепрогулкивчесменпаркприхвативогромныекорзиныспр овизиейстехпоррельсытакиосталисьржаветьсредихолмовтуттомыиповорачиваемназадсказалчарли туттотыиошибсяимистертридденщелкнулвыключателемаварийногогенераторапоехалитрамвайдерну лсяскользнулпорельсамиоставивпозадигородскиеокраиныпокатилсявнизвдолинуонтовыеталнаду шистыезалитыесолнцемлужайкитонырялподтенистыедеревьягдепахлогрибамитамисямколеюпересек алиручейкисолнцепросвечивалосквозьлиствудеревьевточносквозьзеленоестекловагонтихонькоб ормочачтотопросебяскользилполугамусеяннымдикимиподсолнухамимимодавнозаброшенныхстанций усыпанныхсловноконфеттистарымитрамвайнымибилетамиивследзалеснымручьемустремлялсявлетни елесатрамвайондажепахнетпоособенномуговорилдугласездилявчикагонаавтобусахутехкакойточу днойзапахтрамвайчересчурмедленноходитсказалмистертридденвотониихотятпуститьпогородуавт обусыиребятвшколутожестанутвозитьвавтобусахтрамвайвзвизгнулиостановилсятриддендосталсв ерхукорзинуспровизиейребятавосторженнозавопилиивместеснимпотащиликорзинунатравутудагде ручейвпадалвмолчаливоеозероздесьнекогдапоставилиэстрадудляоркестранотеперьонасовсемрас сыпаетсявпрахонисиделинатравеуплеталисандвичисветчинойсвежуюклубникуияркиеблестящиеточ новосковыеапельсиныитридденрассказывалкакмноголетназадтутповечерам

Висновки

Частотний аналіз може бути застосований для автоматизованого відновлення ключів шифрування моноалфавітних шифрів підстановки з великими алфавітами; зокрема,

достатньо легко відновити ключ шифру афінної біграмної підстановки за достатньої довжини шифртексту.

Для відсіювання хибних ключів можна розглядати статистичні властивості мови та формувати певні критерії на їх основі для автоматичної перевірки отриманого тексту на коректність.