Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:
ФБ-31 Острун Катерина
ФБ-31 Острун Михайло

Мета роботи:

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

Хід роботи:

Дано наступний шифртекст:

ХБТЙЬНЦНЮБЦВЭТЙВШЛПНРКЛЩЯУЙЫЧВШЛОЫЕЗБВАЦЛНЭДЙВТЫЯВВЭШЛНЬЗГИШНЬЖДДЭЙФЖЦЗБНЦРЕБЮАДД
ЛСУЧЩМШЮШРВДЛЦНЖБЙЭЮПУВУКЕШЩЕЙУЖЧВЕЯШЦВЫГЖЭЬСАЕРРВЛЙОЦБИЛТДТЩЫЫЫБЮЕЯШЮРЗБСЦАЩЬТЩД
ЙШЕЕТЮЙОЯЦЭЦСОЩОЛШЯКФНПЛЫДЮРЖОЬЫЙВРДТЮ…

Текст зашифровано за допомогою афінної підстановки біграм. Алфавіт складається з 31 букви російської мови.

На відміну від звичайного афінного шифру, який обробляє окремі літери, тут ми маємо справу з біграмами. Це робить шифр значно складнішим для злому, адже ключовий простір зростає з приблизно 300 до майже 900 тисяч можливих комбінацій.

Шифрування відбувається за формулою:

$$Y_i = (aX_i + b)\ mod\ m^2$$

Кожну біграму ми спочатку переводимо в число. Тоді числове представлення обчислюється так:

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}$$

Для розшифрування потрібно виконати обернене перетворення:

$$X_i = a^{-1}(Y_i - b)\ mod\ m^2$$

Афінний шифр біграмної підстановки зберігає частотні властивості мови. Якщо біграма «ст» зустрічається часто в російській мові, то і відповідна їй біграма шифртексту теж буде частою.

Тому для його взлому потрібно знайти найчастіші біграми в шифртексті і припустити, що вони відповідають найчастішим біграмам відкритого тексту.

Для російської мови це наступні біграми:

```
Найчастіші біграми в російській мові:
------------------------------
1. ст
2. но
3. то
4. на
5. ен
------------------------------
```

Найчастіші біграми в нашому шифротексті:

```
Найчастіші біграми в шифротексті:
------------------------------
1. жц (частота: 65)
2. дэ (частота: 62)
3. цэ (частота: 60)
4. сц (частота: 57)
5. оц (частота: 55)
------------------------------
```

Наше припущення, що біграма «жц» ймовірно відповідає «ст», «дэ» може відповідати «но», і так далі. Тому візьмемо п'ять найчастіших біграм шифротексту і п'ять найчастіших біграм російської мови і для кожної пари пар біграм намагаємось розв'язати систему рівнянь.

Припустимо, що біграма відкритого тексту X* після шифрування перейшла в біграму шифротексту Y*, а біграма X** – в Y**. Оскільки шифрування виконується за однією і тією ж формулою з тими самими параметрами a і b, ми можемо записати:

$$\begin{cases} Y^* = aX^* + b (\mathrm{mod}\, m^2) \\ Y^{**} = aX^{**} + b (\mathrm{mod}\, m^2) \end{cases}$$

Якщо ми віднімемо друге рівняння від першого, параметр b взагалі зникає:

$$a = (Y^* - Y^{**}) \cdot (X^* - X^{**})^{-1} (\mathrm{mod}\, 961)$$

Після того, як ми знайдемо a, параметр b легко обчислюється підстановкою в будь-яке з початкових рівнянь:

$$b = Y^* - aX^* (mod\ 961)$$

Якщо $\gcd(X^* - X^{**}, 961) \neq 1$, то для цієї пари біграм розв'язків не існує і нам потрібно пробувати інші комбінації. Щоб знайти обернений елемент, ми використовуємо розширений алгоритм Евкліда.

Цей процес дає нам набір кандидатів на ключ – пар (a, b), які потенційно можуть бути правильними:

```
Кандидати на ключі (a, b):
------------------------------
1 | a:  771 | b:  239
2 | a:  610 | b:  896
3 | a:  616 | b:  884
4 | a:  408 | b:  800
5 | a:   17 | b:   94
6 | a:   41 | b:  927
7 | a:  262 | b:  508
8 | a:   80 | b:  824
```

Тепер застосовуючи ці ключи розшифруємо наш шифротекст. Змістовний текст від незмістовного будемо відрізняти за такими критеріями:

- В російській мові деякі літери зустрічаються дуже часто. Ми підраховуємо їх сумарну частоту. Якщо текст змістовний, очікуємо, що вона приблизно 0.48.
- З іншого боку, деякі літери рідкісні (складають лише 3-4% тексту). Коли їхня частота перевищує 0.02, накладаємо штраф на оцінку тексту.
- Типові біграми: «то», «ор», «ро», «ов», «во», «ос», «ст». Якщо їх багато – текст виглядає природно. Ми підраховуємо кількість таких біграм відносно загальної кількості біграм на стику в тексті.

Результат:

```
 a b відкритий текст оцінка
------------------------------------------------------------
(17  , 94  ) МАЛЬЧИКИЗАУЛЫБАЛИСЬИ...           135.47
(172 , 187 ) КАЕЬПИВИЕАБЛББНЛБСТИ...            78.32
(234 , 32  ) ГАПЬТИЕИЮААЛГБМЛЧСХИ...            72.22
(760 , 362 ) ЩЦЛЗЗПЯПКЦЦШСЩЫШНЛРП...            14.35
(915 , 114 ) ЗЦУЗЭПФПЧЦПШАЩФШМЛЖП...            12.07
(791 , 889 ) ЙЦЩЗЕПЭПЩЦВШЬЩЗШУЛОП...            11.73

Найкращий ключ: a=17, b=94
```

Висновки

В процесі криптоаналізу афінної біграмної підстановки ми застосували частотний аналіз для розкриття моноалфавітного шифру, почавши з підрахунку найчастіших біграм у шифртексті та їхнього зіставлення з типовими для російської мови, що дозволило сформувати систему рівнянь для пошуку ключів (a, b) з модулем 961. Ми реалізували автоматизований відбір кандидатів через перебір комбінацій топ-5 біграм, фільтруючи розв'язки за допомогою розширеного алгоритму Евкліда для обчислення обернених елементів, і оцінили результати за допомогою статистичних критеріїв, таких як частоти частих і рідкісних літер та перетинні біграми, що забезпечило виявлення правильного ключа (a=17, b=94) серед згенерованих кандидатів.

Лінійна природа афінного перетворення робить шифр вразливим до частотного аналізу попри великий ключовий простір, крім того, процес генерації кандидатів виявив залежність їхньої кількості від конкретних числових значень біграм і умов існування обернених, що в нашому випадку дало обмежену, але достатню для аналізу множину.

Розшифрований текст:

```
мальчикизаулыбалисьисжаромвзялисьзаделоонирвализолотистыецветыцветычтонаводняютве
сьмирпереплескиваютсяслужаекнамощеныеулицытихонькостучатсявпрозрачныеокнапогребов
незнаютугомонуиудержуивсевокругзаливаютслепящимсверканиемрасплавленногосолнцакажд
оелетоониточносцеписрываютсясказалдедушкапустьихянепротиввонихсколькостоятгордыек
акльвыпосмотришьнанихподольшетакипрожгутутебявглазахдыркуведьпростойцветокможноск
азатьсорнаятраваниктоеенезамечаетамыуважаемсчитаемодуванчикблагородноерастениеони
набралиполныемешкиодуванчиковиунесливнизвпогребвывалилиихизмешковивотьмепогребара
злилосьсияниевинныйпрессдожидалсяихоткрытыйхолодныйзолотистыйпотоксогрелегодедушк
апередвинулпрессповернулручкузавертелбыстрейбыстрейипрессмягкостиснулдобычунувотв
```

оттаксперватонкойструйкойпотомвсещедрееобильнеепобежалпожелобувглиняныекувшинысок
прекрасногожаркогомесяцаемудалиперебродитьснялипенуиразлиливчистыебутылкиизподкет
чупаионивыстроилисьрядаминаполкахпоблескиваявсумракепогребавиноизодуванчиковсамые
этисловаточнолетонаязыкевиноизодуванчиковпойманноеизакупоренноевбутылкилетоитепер
ькогдадугласзналпонастоящемузналчтоонживойчтоонзатемиходитпоземлечтобывидетьиощущ
атьмиронпонялещеоднонадочастицувсегочтоонузналчастицуэтогоособенногоднядняснбораод
уванчиковтожезакупоритьисохранитьапотомнастанеттакойзимнийянварскийденькогдавалит
густойснегисолнцаужедавнымдавнониктоневиделиможетбытьэточудопозабылосьихорошобыег
основавспомнитьвоттогдаонегооткупоритведьэтолетонепременнобудетлетомнежданныхчуде
синадовсеихсберечьигдетоотложитьдлясебячтобыпослевлюбойчаскогдавздумаешьпробратьс
янацыпочкахвовлажныйсумракипротянутьрукуитамрядзарядомбудутстоятьбутылкисвиномизо
дуванчиковонобудетмягкомерцатьточнораскрывающиесяназарецветыасквозьтонкийслойпыли
будетпоблескиватьсолнценынешнегоиюнявзглянисквозьэтовинонахолодныйзимнийденьиснег
растаетизподнегопокажетсятраванадеревьяхоживутптицылистваицветысловномириадыбабоч
екзатрепещутнаветруидажехолодноесероенебостанетголубымвозьмилетоврукуналейлетовбо
калвсамыйкрохотныйконечноизкакоготолькоисделаешьединственныйтерпкийглотокподнесие
гокгубамипожиламтвоимвместолютойзимыпобежитжаркоелетотеперьдождевойводыконечнозде
сьгодитсятолькочистейшаяводадальнихозерсладостныеросыбархатныхлуговчтовозносятсян
азарекраспахнувшимсянавстречунебесамтамвпрохладныхвысяхонисобиралисьчистоомытымиг
роздьямиветермчалихзасотнимильзаряжаяпопутиэлектрическимизарядамиэтаводавобралавк
аждуюсвоюкаплюещебольшенебескогдападаладождемназемлюонавпиталавсебявосточныйветер
изападныйисеверныйиюжныйиобратилась вдождьадождьвэтотчассвященнодействияужестанови
тсятерпкимвиномдуглассхватилковшвыбежалводвориглубокопогрузилеговбочоноксдождевой
водойвотонаводабылаточношелкпрозрачныйголубоватыйшелкеслиеевыпитьонакоснетсягубго
рласердцамягкокакласканоковшиполноеведронадоотнестивпогребчтобыводапропиталатамве
сьурожайодуванчиковструямиречекигорныхручьевдажебабушкавкакойнибудьфевральскийден
ькогдабеснуетсязаокномвьюгаислепитвесьмириулюдейзахватываетдыханьедажебабушкатихо
нькоспустится явпогребнаверхубольшомдомебудеткашельчиханьехриплыеголосаистоныпрост
уженнымдетямоченьбольнобудетглотатьаносыунихпокраснеютточновишнивынутыеизналивкив
сюдувдомепритаитсяковарныймикробитогдаизпогребавозникнетточнобогинялетабабушкапря
чаттотоподвязанойшальюонапринесетэтоттотовкомнатукаждогоболящегоиразольетдушистое
прозрачноевпрозрачныестаканыистаканыэтиосушатоднимглоткомлекарствоиныхвременбальз
амизсолнечныхлучейипраздногоавгустовскогополудняедваслышныйстукколестележкисморож
енымчтокатитсяпомощенымулицамшорохсеребристогофейерверкачторассыпаетсявысоковнебе
ишелестсрезанной травыфонтаномбьющейизподкосилкичтодвижетсяполугампомуравьиномуцар
ствувсеэтовсеводномстаканедадажебабушкакогдаспустится явзимнийпогребзаиюнемнаверноб
удетстоятьтамтихонькосовсемоднавтайномединении сосвоимсокровеннымсосвоейдушойкакид
едушкаипапаидядябертидругиетожесловнобеседуястеньюдавноушедшихднейспикникамистепл
ымдождемсзапахомпшеничныхполейижареныхкукурузныхзеренисвежескошенногосенадажебабу
шкабудетповторятьсноваисноватежечудесныезолотящиесясловачтозвучатсейчаскогдацветы
кладутподпресскакбудутихповторятькаждуюзимувсебелыезимывовсевременасноваисноваони
будутслетатьсгубкакулыбкакакнежданныйсолнечныйзайчиквотьмевиноизодуванчиковвиноиз
одуванчиковвиноизодуванчиковониприходилинеслышноуходилипочтибесшумнотравапригибал
асьираспрямлялась вновьонискользиливнизпохолмамточнотениоблаковэтобежалилетниемаль
чишкидугласотстализаблудилсязадыхаясьотбыстрогобегаоностановилсянакраюовраганасам
ойкромкенадпропастьюиоттуданенегодохнулохолодомнавостривушиточноолеиьонвдругучуял
старуюкакмиропасностьгородраспалсяздесьнадвеполовиныздеськончилась цивилизацияздес
ьживетлишьвспухшаяземляежечасносовершаетсямиллионсмертейирождений издесьпроторенны
еилиещенепроторенныетропытвердятчтобыстатьмужчинамимальчишкидолжныстранствоватьвс
егдавсюжизньстранствоватьдугласобернулсяэтатропаогромнойпыльнойзмееискользиткледя
номудомугдевзолотыелетниеднипрячетсязимаатабежиткраскаленнымпесчанымберегамиюльск
огоозераавонтакдеревьямгдемальчишкипрячутсямежлистьевточнотерпкиеещенезрелыеплоды
дикойяблониитамрастутизреютавотэтакперсиковомусадуквиноградникукогороднымгрядамгд
едремлютнасолнцеарбузыполосатыесловнокошкитигровоймастиэтатропазаросшаякапризнаяи
звилистаятянетсякшколеатапрямаякакстрелаксубботнимутренникамгдепоказываютковбойск
иефильмывотэтавдольручьякдикойлеснойчащедугласзажмурилсяктоскажетгдеокончаетсягоро
диначинаетсялеснаяглушьктоскажетгородврастаетвнееилионапереходитвгородиздавнаинав
екисуществуетнекаянеуловимаяграньгдеборютсядвесилыиоднанавремяпобеждаетизавладева
етпросекойлощинойлужайкойдеревомкустомбескрайнееморетравицветовплещетсядалековпол
яхвокругодинокихфермалетомзеленыйприбойяростноподступаетксамомугородуночьзаночьюч
ащилугадальниепросторыстекаютпооврагувсеближезахлестываютгородзапахомводыитравиго

родсловнопустеетмертвеетивновьуходитвземлюикаждоеутрооврагещеглубжевгрызаетсявгор
одигрозитпоглотитьгаражиточнодырявыелодчонкиипожратьдопотопныеавтомобилиоставленн
ыенамилостьдождяиразедаемыержавчинойэйаусквозьтайныоврагаигородаивременимчалисьдж
онхафичарливудменэйдугласмедленнодвинулсяпотропинкеконечноеслихочешьпосмотретьнад
весамыеглавныевещикакживетчеловекикакживетприроданадоприйтисюдаковрагуведьгородвк
онцеконцоввсеголишьбольшойпотрепанныйбурямикорабльнанемполнонародуивсехлопочутбез
усталивычерпываютводуобкалываютржавчинупоройкакаянибудьшлюпкахибаркадетищекорабля
смытоенеслышнойбурейвременитонетвмолчаливыхволнахтермитовимуравьеввраспахнутойовр
ажьейпастичтобыощутитькакмелькаюткузнечикиишуршатвжаркихтравахточносухаябумагачто
быоглохнутьподпеленойтончайшейпылиинаконецрухнутьградомкамнейипотокомсмолыкакруша
тсятлеющиеугликостразажженногогромомисинеймолниейнамигозарившейторжестволесныхдеб
рейтаквотзначитчтотянулосюдадугласатайнаявойначеловекасприродойизгодавгодчеловекп
охищаетчтотоуприродыаприродавновьберетсвоеиникогдагородпонастоящемудоконцанепобеж
даетвечноемугрозитбезмолвнаяопасностьонвооружилсякосилкойитяпкойогромныминожницам
ионподрезаеткустыиопрыскиваетядомвредныхбукашекигусеницонупрямоплыветвпередпокаем
увелитцивилизациянокаждыйдомтогоиглядизахлестнутзеленыеволныисхоронятнавекиакогда
нибудьслицаземлиисчезнетпоследнийчеловекиегокосилкиисадовыелопатыизеденныержавчин
ойрассыплютсявпрахгородчащадомаоврагдугласозадаченномигаетнокакаяжесвязьмежчелове
комиприродойкакпонятьчтозначатонидругдлядругакогдаонопустилглазапервыйлетнийобряд
позадиодуванчикисобраныизаготовленывпрокпораприступатьковторомунодугласзастылинед
вижетсясместадугпошлидугголосазатихливдалекеяживойсказалдугласночтотолкуониещебол
ьшеживыечемякакжеэтокакжетаконстоялводиночествеглядянасвоиногиневсилахдвинутьсясм
естаинаконецпонялвтотвечердугласвозвращалсядомойизкиновместесородителямиибратомтом
омиувиделихвяркоосвещеннойвитринемагазинатеннисныетуфлидугласпоспешноотвелглазано
егоногиужеощутилиприкосновениепарусиныизасколькзилиповоздухубыстрейбыстрейземлязав
ертелась захлопалиполотняныенавесынадвитринамитакойонподнялветертаконмчалсяродител
иитомшагалинеторопясьамеждунимипятясьзадомшелдугласинесводилглазстеннисныхтуфельт
ампозадивполуночнойвитринехорошаябылакартинасказаламамаагабуркнулдугласстоялиюньд
авноминовалотовремякогданалетопокупаюттакиетуфлилегкиеитихиеточнотеплыйдождьчтошу
ршитпотротуарамужеиюньиземляполнапервозданнойсилыивсевокругдвижетсяирастеттраваип
осейденьпереливаетсясюдаизлуговомываеттротуарыподступаеткдомамкажетсягородвотвотч
ерпнетбортомипокорнопойдетнадноивзеленомморетравнеостанетсянивсплесканирябидуглас
вдругзастылточновросвмертвыйасфальтикрасныйкирпичулицыневсилахтронутьсясместапапв
ыпалилонвонтамвокнетеннисныетуфлиотецдаженеобернулсяазачемтебеновыетуфлискажипожа
луйстаможешьтымнеобяснитьнуудазатемчтовнихчувствуешьсебятакбудтовпервыевэтолетоск
инулбашмакиипобежалбосикомпотраветочновзимнююночьвысунулногиизподтеплогоодеялаипо
дставилветручтодышитхолодомвоткрытоеокноионистынутстынутапотомвтягиваешьихобратно
пододеялоионисовсемаксосулькивтеннисныхтуфляхчувствуешьсебятакбудтовпервыевэтоле
тобредешьбосикомполенивомуручьюивпрозрачнойводевидишькактвоиногиступаютподнубудто
онипереломилисьидвижутсячутьвпередитебяпотомучтоведьвводевсевидитсянетакпапсказал
дугласэтооченьтруднообяснитьаа