

Криптографія
Комп'ютерний практикум №3
Криптоаналіз афінної біграмної підстановки
Варіант 10

Виконав: студент групи ФБ-91
Кузавка Артем

Київ – 2021

Мета роботи

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

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a, b) шляхом розв'язання системи (1).
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3 - 4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

Після незначної модифікації програми "entropyCalculator.py" із комп'ютерного практикуму №1, було отримано програму "topBiFreq.py", що виводить біграми, що зустрічаються в тексті найчастіше.

```
$ python3 topBiFreq.py 10.txt
```

```
nyog-sothep@PC:~/Desktop/Crypto/lab_3$ python3 topBiFreq.py 10.txt
сг 0.01576872536136662
жэ 0.015505913272010513
ям 0.01419185282522996
нг 0.01366622864651774
тм 0.013403416557161629
nyog-sothep@PC:~/Desktop/Crypto/lab_3$
```

Рисунок 1: робота програми "topBiFreq.py"

5 найчастіших біграм запропонованого шифртексту "10.txt":

Біграма	сг	жэ	ям	нг	тм
Частота	0.01577	0,015506	0.01419	0.013666	0.0134

Аналогічно було отримано частоти біграм російської мови.

```
nyog-sothep@PC:~/Desktop/Crypto/lab_3$ python3 topBiFreq.py Толстой_Лев_Николаевич_Анна_Каренина_no_spaces.txt
то 0.017552156604507766
на 0.013499356460833906
он 0.012882756143554133
ст 0.012372414618815289
не 0.012249693196444072
nyog-sothep@PC:~/Desktop/Crypto/lab_3$
```

Рисунок 2: Найчастіші біграми російської мови

За допомогою іншої модифікації програми “en” - “”, було знайдено біграми, що не зустрічаються в російській мові для тексту із заданими параметрами.

```
nyog-sothep@PC:~/Desktop/Crypto/lab_3$ python3 forbiddenBiGrams.py Толстой_Лев_Николаевич_Анна_Каренина_no_spaces.txt
'аь', 'аь', 'бй', 'бф', 'вй', 'гй', 'гц', 'гц', 'гы', 'гю', 'дй', 'еь', 'еь', 'жй', 'жф', 'жх', 'жц', 'жы', 'жю', 'зй', 'зц', 'иы',
'иь', 'ий', 'йы', 'йь', 'кй', 'кы', 'кь', 'лй', 'мй', 'нй', 'оы', 'оь', 'пв', 'пг', 'пй', 'пх', 'пц', 'пэ', 'рй', 'сй', 'тй', 'уы',
'уь', 'фд', 'фж', 'фз', 'фй', 'фм', 'фп', 'фх', 'фц', 'фы', 'фц', 'фэ', 'хй', 'хы', 'хь', 'цй', 'цф', 'цч', 'цц', 'цъ', 'цэ', 'цю',
'чй', 'чф', 'чц', 'чы', 'чю', 'шз', 'шй', 'шф', 'шц', 'шы', 'шэ', 'шя', 'цб', 'цг', 'цд', 'цж', 'цэ', 'цй', 'цк', 'цм', 'цс', 'цт',
'щф', 'щх', 'щц', 'щч', 'щш', 'щщ', 'щы', 'щэ', 'щю', 'щя', 'ыы', 'ыь', 'ыю', 'ый', 'ыь', 'ыь', 'эа', 'эб', 'эв', 'эе', 'эж', 'эм',
'ео', 'эу', 'эф', 'эх', 'эц', 'эч', 'эц', 'эы', 'эь', 'ээ', 'эю', 'эя', 'юй', 'юы', 'юь', 'яы', 'яь',
nyog-sothep@PC:~/Desktop/Crypto/lab_3$
```

Рисунок 3: "Заборонені" біграми

Для детектування осмисленого тексту російською мовою було застосовано два фільтри:

1. У тексті має найчастіше зустрічатися буква “о”.
2. У тексті не мають зустрічатися біграми “яь”, “ыь”, “оь”, “шя”.

```
nyog-sothep@PC:~/Desktop/Crypto/lab_3$ python3 affineBigramAttack.py 10.txt
поздновечеромнаверандесиделколя
a = 300 ; b = 400
```

Рисунок 4: Успішно розшифрований текст, знайдений ключ.

Ключ: a = 300, b = 400.

Висновки: під час виконання комп'ютерного практикуму я навчився проводити успішні атаки на шифр афінної підстановки біграм. Крім цього, я поновив теоретичні знання з деяких тем дискретної математики: пригадав як обчислювати обернений за модулем елемент.

Шифротекст

[illegible]

эухявахшзсжитдуюцебыцнввпсбкцгнсчжнилилдязаеямвннгрхтбиздэчапльхйбшшхшзбшрэпиатрунббури
клвцобднейснюмгуыцпцапцоишйпмдмнйэвахияогсбшйагопшчямхштчбифмцксгизлкдмтлсбьльцдхмдс
йбжщйсшщмярфжчхычфктмпнтмдмэмецобднсбьцебвубушееэюмпмдчогзлвцтвргцхьлдудшафцкхцжнсм
ьтэерэеэюэмсбаыямээрэгмржзцриьцжэлгээчэбиушкйщйфжугрицншйжэбшлклиеэлккмйцккикхйяхрхюц
мчнейзиргжэсгклдхрихцнейгквнлйлогклдхимжэсчхяоингйзюфхйццсбултббгьцебдяццтрувьфашмец
пвчкхйэньхиябшгцбузлчвдусгчкнэцршшоэухэзиямегмкфйгэсизетбюмснйцксббхтфьлхйбшшхебшйсгюу
тмдээзтильэтьфяичжэлксгжжщмямжжкцапямякцрвняпямгнцржэсинглдычмецюргклдхжткгзэгкцрюмгй
крзйччсбьцрвфбьцренгешгэдмшпцюриуюжтоияейбрюцшйюмугогзлвцтвдшяхычфккхкцццоцадмйвчяои
нггнэмншцогэюмибнпямгйяхмйзэпмсгюхрубиияшйэхешуцидзэтмэгумзвригншйсщцоцлгкннвйесмтц
нисчтбшчшпепяпсбеэгкцрдмпйфрхййзлбилфизээмрчжнсмццфббиямэмткнйтфжэнгпввпсбярвгфбопямвн
ниахешчтьэщмьдйизипйзэсгнхщкйейцхцюгэвуיעцвйесмгйсгфищйэзцюззхйцрйздемчжюдэгйгкцрээош
щбьлксечцнргфзюмцкэрлнуаяэсиебамсйэнгмиибгогфипйэчтфшкагоцбишчтмгнейсгкйицуыямсицасгдмэ
мзммпмсгыццотфнгпкгшжэпмббнгфивунгркййяхфаиктмнчфуоцнгклдхимнчфбфжшэстофкиебюмгэчэлцз
лрбхзлнгцнгйтэпмдмяртмдннйгэсэярийюпямггяпвюцлгтмпйхпцнгйзмпкеэмшэнилеббохопфжбктмэмбй
зимвумсгойэйшйжцяйейтбыйфжшйбблйейжэамукцрщцмдыхтнгэдибдмэсжжржафгэлкдэсмташсгзэшй
цкоипймбзлхкыулвнлдгйзмсйсцргцюгэчэтцяпцюжтдлжтюуэлбгфидйшйхжкййцуттклретбвузлебкксче
змбрржпмднсгявнйцкнвчкбшяжчэцрпйфйдэтзгкяпмржшйймдгднббгрхдяшшпепвщпшпклкбрржсмяпсб
жшэээмжвчкумсжюмннтччюбгфгзэхшоимвлькибгкнычтзхкямбйидужафзэпмсгуаяжкцднчцахткйлкмщйс
гшчьэбхрицшйждццлйзсгмчюхохофжзэфжэлнеэдэгубушеебнтэтмжлнлнлкшхфбомпглкжжеиякжцыцх
ццоюцгншшфэентэхкошпмдмярсгиксбямхугвумпмцятбнйбщысгшсгнкщйцкшшпеемщдвууажмбшчэмпю
хогчяйксийгтвклдгввпсбругвргфбопямюцмдргвццфукулщмргжлэхосшпзлриэхкшдмпзейщмргэсхйакц
мумгэдэсгбиззхгюмюмейцроивфччжьюсэншйфйяцтфсбэсчштхцюгэбжкйбрршгкцкцрггтгысбйеяйедргв
цццфукулщмжнтэйекншцййукшйзнебтбймомакжэкпжэйеиубббгммукртяфюмсгычнюцшйжвфбхьюхццюгэс
мсэйекнлиээбшэээмнищйэзюмокзйминзирибгвцюхямжтагфбшйпмнэсжчэнгйзцкцрггтшцемциьцййфц
юхямыцафжэнгцксйщмбгантэтмикшрйздэсчбибхтбокзймкмкмиыгэхкжвьэямрнщйуквкюцриймечбгсмямх
жщнебпйфйжжзэкчэнгцкшршямцхямтэкфццнвкшйюмсиойюлдязачйгйбмзцбивфцнумецщэблцнжшс
мямумшмжэляпядччжъяйэнэфсбтмаемчфытсцлувлукдюхншизаснеэдэмециясжсмсээфсбэсюмсмсэщн
фшпйозаушенишчгкейзмсэсгсыамухжнлхкткйлвушмумнкзицнякикейяржэбнтчфзкмьгоцостмсгилэхщкг
мсммпьцрхумгйямцшафщйзхшмсйкрюмярфкейяртмргкйгэцрцйнийцкдуэиоцпксмчэжжгэщцойлкцйнийкрд
уэиоцпксмщцкшякрнлчшйашхйошямбцлгктиляхоидшлнкнйцмкрсмсгмхдшетлкозаекссмнфыцгштмбхфбв
энбрхбгрхдмфццнсийкыямдгзэжжйэйшйвнниббхтфьлюцмчцнейзгрхлшсгвпямжэкййцхтфкюшшекгул
нишчжмбшчэмпюхчюжньюмукюмбкшшхфжэкпкшбйжэашбшькнюдуюжжнтэшйьнбтяфикжэафдуэиоцпкс
микцкдутмжвсййжжэсдязасмчубимвумсгжнбцнмелкюмллшезаейбхклдхриыфгвьэгклкдэагднсбьцфукул
ьэлхычфккхшзгшвкгугнлгрершщиебовдумчаххйбшшхгвкляфыхмчрэьикгжылсгмчфбдуфжчулкицрасмз
йнийсмэнейпццлпйщйвчшцксдэсгфягшккшинйщгчкашрэтхрвтвлгиукльэумвтиликгклдхвпямймкйчеилрв
щйжжщмецксеуэлгшдээзоптэлкюзцрпмйлмчриафдмярейпйхпцнбйргсчиогфиясагопшчгнэшювумдэагн
гшхгзэхшдмчкюжэюэмухтнзмдмфхруядргогнклдхтвахычшйаепвумтшшйпйдлйцшгйтздмчычезжцо
сэицнээяжпводчэярфжьцебшчыцжзтмлпййтэхкдябужнгквигншбгввпейиццюривфзэсгэхбмкбкбйьэцкпб
ыцццошйюнпктэцрйзовшчхшнмсйщйзрмэ

Відкритий текст

поздновечеромнаверандесиделколяичтотописглвтемнотебумагуитутолкомнелызябылпразаядетывремя
твреминиорвосклицглагиливщтотжезначитемувголовуприходилоещечтонибудыподходящеедлягоспи
скапотомдверычутыстукнулаточновсеткуотмоскитовудариласыночнаябабочкалинашепнулафманонасел
арядомснимнакачеливоднойночнойсорочкинетониныкаякаксемнадцатилетняядевочкакоторуюещенелюб
ятинетолставкакпятдесятилетняяжеуэнакотлрууюужинелюбятноскоаднаякрепкаяиминнотакавкакнадо
таковжеуэньвовсякомвозрастееслионилюбимьонабьлаудивительнаяеетелокакиегособствинноевсегдад
умглозанеетолькоподругомуононьнашивалодетейиливходиловпередилеовкаждуюкомнатучтобьнеулови
моизминитытамсамыйвоздухподстатынастроениюмужаказглосьонаникогданезадумьваетсянадолгомьсл
ытотчаспередавгласыотеголовьплечамплчцамипретвряласывдействиетакнезаметноиестественночтол
еонесмогьдаенехотелизобразитыэтокакимилибочертежамиэтамашенасказаоонанаконецненужнаонана
мдаотозвглсяонноеногданужнопозаботитисяиодругихявотвседуаючтотудаоставитыкинокантеньрадио
приемникстереоскопическиеочкиеслиобратывсеэтовместевсякийчеловекпощупаетульбнетсяискажетдад
аэтоиестысчастыесоченитытакуюхитруюмеханикудумалончтопускайучеловекапромокленогиилиноетязв
аилиегомучаетбессонницаиорвлрочаетсявпостеливсюночнынапролетидушщегогршзутзаботьавсервантво
ямашенадастемусчастыекактамагическаякрупенкасолитчтоброшенавокеанивечнорождаетсолииобратиоав
семлревсоланойраствлрктонерасшибьбьвлепешкулишыбызобреститакуюмашенупустыемуответитнаэт
отвопросуельмирипустыответитвесыгородзпустыответитжингленасмущенномолчаоасидрядопснимнак
ачеляхиеемолчаниеговлрилосянеевсвкихсловлеотожеумолкзапрокенулголовуислушалкаксвоответенвгу
стойлиствемогуچهговязанезабывайговлрилонсебевщтотшелестистыевтоженужендлятвоёмашеншчерез
минутуверандаопустелапустькачеленеподвижноповисливтемнотедедушкаульбнулсывоснеонпочувств
аещтуульбкуудивилсеейипроснулсяполежалнемногоприслушалсвксебеипонялоткудаонавзяоасыибоонус
льшглнечтоглаздоболееважноинезелипиниептицилишелестмолодойлиствькаждыйгоднаступалдиныког
даонвоттакпросьплгсяиждаещтогозвукакотлрйозначалчтотеперытоужлетоначалосыпонастоящемуона
ченглосьивотвтакоеутрокогдактонибудыиздомочадцевилигостейплемянниксьниливнуковьходилнглужайк
уподегоокномиметаллическииножииспицькружаизвеняподушистойлетнейтравеприлежнообегалиеепокр
аямнасеверनावостокнаюгназаподисьваывсеменьшиеименьшиеквадратькосилказвонкострекотоаизпод
ножейбршзгалиголяякиклевераредкиезолотьеискрьюцелевшихпослесблраодуванчиковмураяипглочки
амешкиостаткипрошлогоднегопразднованиячетвентогоиюляобгльельшутихиикусочитрутаногоавноеза
нейстглсяпроходныйчистыйпотоксочнойзеленойтравьдедушкеужепредставлялосыкаконжеэкочетегоно
гиохлаждаетразгрячинноелицонаполняетноздриизвечньмароматомвновыродившегосялетаиобещаетдам
ьвсевсепоживемлэецельйгодвеликоечудокосилкаговлрилсебедедушкаккакойэтодураквьдумалчтоновйго
дначинаетсипенвогоярварянадобьлопоставитыдозорнькараулитыросттравьнамилионахлужаекилленой
саогайоилиайовьиказаметятчтоонасозреладлясенокосавтосамоеутровместофейенверковфанфарикриков
пустыначенаетсывеликаябурнаясимфониякосилоксрезаэихсвежиетравьнанеобятньхлуговьхпростлрахвт
отеденственньйденьвгодукотлрйпонастоящемузнаминцетсобоиначалолюдямнадобьбросатыдругвдруга
неконфеттиенесерпартенапригоршнисвежескошеннойтравьдедушкахмькнулчтоттоужбольнодолгуюфило
софиюразвелстглподошелкокнуйвьсунулсывласковьйсолнечньйсветтакиестыфорестерновьйжилецмоло
дойгазетчиккакраззаканчиваетряддоброеутромистерсполденгтакеехорошеныкобиллсжаромкрикнулдеду
шкаивсклреужесиделвнизуиуплетглприготовленньйбабушкойзавтракширокоеокноьлораскрытоиужужа
ныекосилкисловноподпевглозавтракуомщтойкосилкинадушестановитяспокойнеезаметилдедушкатьтол
ыкопослушайтеперыужнедолгонамееслушатыотозваоасыбабушкаипоставиланастолглркупшиничньхлеп
ешекбиллфорестерпосеетсегодняновьйсонттравьеининадобудеткоситынепомнюкактамонаназываетсяно
накаквьрастетскольконужнотаксамаиостановитсяибольшенерастетдедушкасизумлениемуставилсянажи
нудовольноглупаяшуткасказглоннаконецидипосмотрисабиллфлрестерговлритэтоземленапользусказгл
абабушкаонужепривезновьеесеменаонисложеньзадомомвмаленькиххлрзинкахнужновразньхместахвьрт
ыямкиизасьпатытудасеминакконцугодановаятраваубыетвсюстаруюитогдаможешыпродаватисвоюкосил
куонатебебольшенепонадобитядедушкасонвлгсясостулаимигомвьскочилводворбиллфлрестеростанови
лкосилкуижмурясыотсолнцасульбкойподошелкнемувоттактосказалорвчеракупилновьеесеменадайдумаюз
асеювамлужайкупокаясвободинаминяпочемунеспросилужайкатовсетакимоязакричглдедушкадумалв
ьбудетедовольньмистерсполденгничегоянедоволенпокажитемнеэтучертовутравуонистояливозлемглины
кихчетьрехугольньххлрзиноксновомодньмисеминамидедушкаподозрительнопотьгглюднуизнихноскопб

ашмакапомоемнцтосамаяобькновиннаятраваавувереньчтовасненадулиявкалифорнииивиделкаконарасте
твотнастольковрастетивсеелитолькоонаприживетсывздешнемклиматинамужинабудущийгоднепридетс
вкаждуюнеделюподстригатылужайкувтомтоибедавашимпоколениемсказглдедушкамнестьднозавасбило
алэежурналиствьготоввьунничтожитывсечтоестынасветехлрошеготолькобътратитыпоменьшевременипом
иныхштрудавотчеговьдобиваетесьоннепочтителынопнулклрзинкуногойвотпоживетесмоетогдапойметеч
томелкиерадостикудаважнеекрупньхраноутромповеснепрогулятысяпешкомневпримерлучшечемкатитыв
осемьдесятмилывсамомроскошномавтомобилеазнаетпочемупотомучтовсевокругбоагоцхаетвсерастети
цвететкогдаидешьпешкоместывремяоглядетысявокругзаметитысамуюмглуюкрасотуюпонимаюсейчасва
мхочетсяохватитывсесразуиэтонаверноестественнищтосвойствомолодостеногазетчикунадоуметывидеты
имелкийвинограданетолькоогромньеарбузьвамподавайцельскелетасменядовольноиследапалыуевчтож
тожепонятносейчасмелочикажутсявамскуньминоможетвьпростоеещенезнаетеимуеньнеумеетнаходитыв
нихякусдайвамвольвьбьиздализаконобустраниивсехмелкитделвсехмелочейнотогдавамнечегобьлобьд
елатывперерьвемеждубольшимиделамиипришлосьбьдоисступленияпридумватысебезанятиечтобьнесо
йтисуматакужлучшепоучилисьбькоечемуусамоиприродьподстригатытравувьпгльватыслрнякитожедн
аизрадостейжизнисьнокбиллфорестероасковоульбнулсястарикужнаюзнаюсказалдедушкаястановлюсьли
шкомболтливьмвжизненикогонеслушалстакимудовольствиемтогдапродолжимлекцеюкустиренилучше
орхидеийодуванчикитожечиентополохапочемудапотомучтоониохотынинадолгоотвлекаютчеловекауводят
егоотлюдейигородазаставляютпопотетыивозвржэютснебесназемлюиужкогдатывесьтутиниктотебинеме
шаехотынинадолгоостаешьсянаединессамимсобойиначинаешьдуматыодинбезпостлроннейпомфэикогд
акопаешьсявсадусамоевремяпофилософствоватыниктообэтомнедогадьваетсяниктотебянеобвняетникто
енезнаетничегоастьстановишьсязаправскимфилософожцдакийпоатонсредипионовсократкторьсамсебе
вьразиваетцикутутотктотаэитнаспинепосвоейлужайкемешокнавозасродниатласуукоторогонаплечахвржэ
аетсяземнойшарлщмюэлсполдингэсквайрсказалоднаждькопаяземлюпокопайсяусебявдушевертителопаст
вщтойкосилкибиллидаороситвасживительнаяструяфортанаюностилекцияокончинакрометогоизредкаоче
ныпользительноотведатызелениодуванчиковавьдавноелизеленыодуванчиковнаужинсэрнебудемучнонят
ыбиллквиулилегоныкостукнулблизайшуюкорзенкуноскомбашмакатаквотнасчемщтойтравьяещеневсв
амсказглонарастеттакгусточтонавернвказаглушитиклевериодуванчикигосподипомилиузначитуженабуду
эийгодмьостанепсябезвинаязодуванчиковиниоднойпчельнадлужайкойдавьпростосумасошлипослушайте
скольковшзапоатилизаэтисеминадолаарклрзинкакупилдесятьштуквамвподарокдедушкаполезьякармарв
ьтжэилстаромодньдлиннькошелекотстегнулсеребрянуюзастежкуиизвлектрибумажкипопатыдолоаровб
иллвьтолькочтосовершилипревьгоднуюсделкузаработалипятьдолларовизвольтесейчасжеотправитывсю
этучересчурпрозаическуютравувоврагнапомойкусловомкудахотитетолькопоклрнейшепрошунесейтеееу
меняводвлреязнаюувассамьепохвалыньинамериниянаявсетакиужедостигвесымапочтенноговозрастаисмо
имижеоанияменегрехсчитатывпервуюочередыаа