Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Криптографія
Комп’ютерний практикум №3
Криптоаналіз афінної біграмної підстановки

Виконали:
Студенти групи ФБ-33
Тимощенко Олександр
Назаренко Іван

Київ - 2025

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).

$$\begin{cases} Y^{*} \equiv aX^{*} + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases},$$

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.

Підготовка до аналізу

Спочатку пронормалізуємо наш текст (приберемо пробіли, перенесемо все в нижній регістр та замінимо літери "ё" на "е" та "ъ" "ь").

```python
def normalize(text):
    """Нормалізація тексту"""
    text = text.lower().replace("ё", "е").replace("ъ", "ь")
    return "".join(ch for ch in text if ch in ALPHABET)
```

Частота біграм

Номер	Біграма	Кількість	Частота
1	ээ	74	0.016544
2	вд	57	0.012743
3	чф	56	0.012520
4	цг	56	0.012520
5	гн	56	0.012520
6	ур	50	0.011178
7	иэ	48	0.010731
8	цн	47	0.010507
9	вш	46	0.010284
10	мй	45	0.010060

—- Найчастіші біграми в тексті.

Так як п’ятьма найчастішими біграмами російської мови (в порядку спадання частот) є біграми «ст», «но», «то», «на», «ен —- ми можемо припустити, що найбільш часті біграми в нашому тексті частково або повністю співпадають з нашим списком.

Пошук ключів

Шукаємо ми наш можливий ключ за формулою наданою в методичці:

$$\begin{cases} Y^{*} \equiv aX^{*} + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases},$$

Y* - це наша перша зашифрована біграма.
Y** - друга зашифрована біграма.

Для розв’язку, віднімаємо ці рівняння один від одного, тим самим позбуваємось в рівнянні b.

Вибір правильного ключа

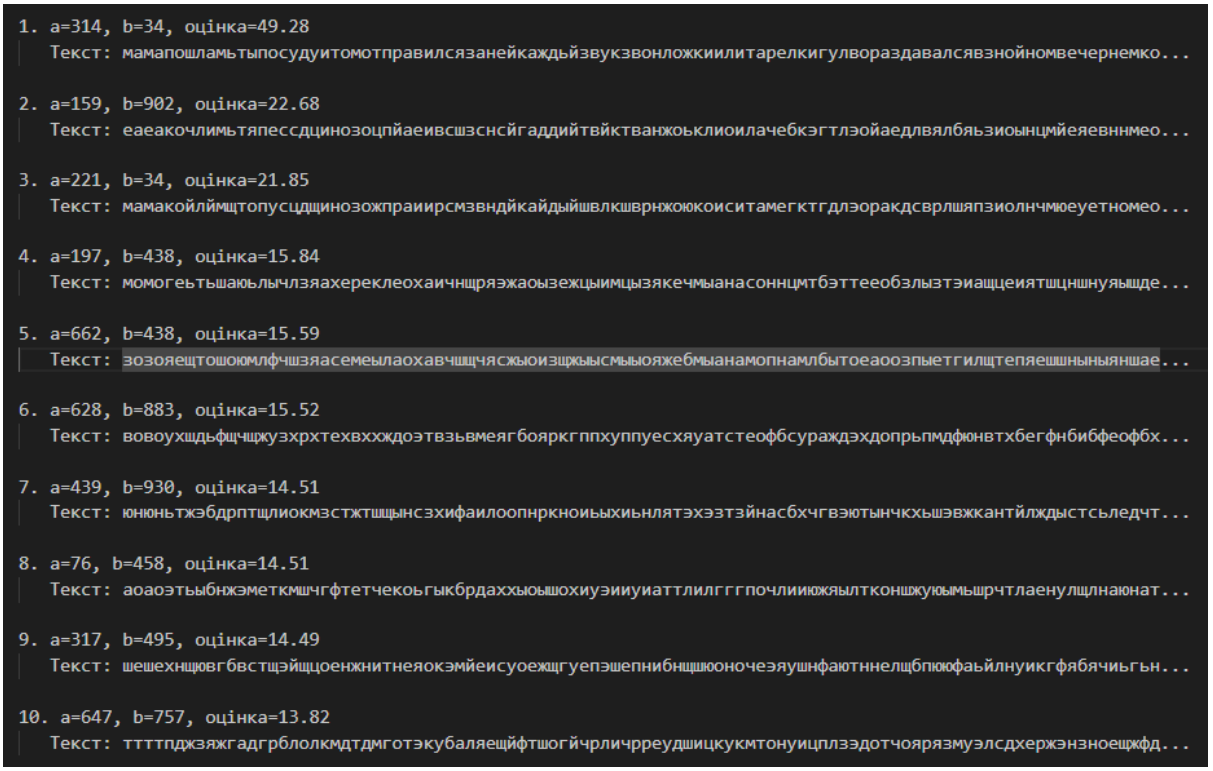
Критерії оцінки якості тексту наступні:

- Часті літери повинні складати приблизно 40-45 відсотків тексту, якщо більше — додаємо бали.
- Рідкі літери повинні бути менше 15 відсотків в тексті, якщо більше — віднімаємо бали.
- За заборонені біграми знімаємо багато балів .
- IC для російської сови приблизно 0.055, тож чим далі від цього значення, тим більше балів віднімаємо.

```
# Часті літери повинні складати ~40-50%
freq_sum = sum(freq.get(ch, 0) for ch in FREQUENT) / n
score += freq_sum * 100

# Рідкісні літери повинні бути малими
rare_sum = sum(freq.get(ch, 0) for ch in RARE) / n
if rare_sum > 0.15:
    score -= (rare_sum - 0.15) * 200

# Заборонені біграми
overlapping = [text[i:i+2] for i in range(len(text)-1)]
forbidden_count = sum(1 for bg in overlapping if bg in FORBIDDEN)
score -= (forbidden_count / len(overlapping)) * 500

# Індекс відповідності
counter = Counter(text)
ic = sum(c * (c - 1) for c in counter.values()) / (n * (n - 1))
score -= abs(ic - 0.055) * 1000
```

Результати

В результатах ми отримаємо топ-10 кандидатів на ключ від шифротексту з оцінками та невеличку частину розшифрованого тексту для перевірки.



Наш ключ:
a = 314, b = 34

Висновки:

У ході виконання лабораторної роботи, ми успішно реалізували криптоаналіз афінної біграммної підстановки. Реалізували декілька функцій як для дешифрування, так і для оцінки якості дешифрованого тексту.

Розшифрований текст:

мамапошламьтыпосудуитомотправилсязанейкаждьйзвукзвонложкиилитарелкигулвораз давалсявзнойномвечернемкоздухепотомонимолчапошливболышуюкомнатуснялисдиван аподушкивдвоемраскрьлиегоиразложиливедынасамодделеэтобьлвовщенедиванашироче ннаякроватымамапостелилаимсдугласомпостелыловковзбилаподушкитомначалбьлорас стегиваыырубашкуноонасказалапогодиминуткутомпочемунадотькакаяточуднаямамона опустиласынастулносразпюевсталаподошлакдвериипозвалаоназваласновaисновадуглас дугдуугееголосупльвалвдушнуютымуитонулвнейбезксякогоотклика дажеэхонеотвечалод угласдугласдугласдуууглааастомщиделнаполуиегопронизьвалхолодновинойтомубьлоне

моркюеноеинезимаинелетнийзнойонвиделмаматорастеиянноозираетсятозакрьваетглаза
стоитинезнаекчтоделаыыиоченыколнуетсядасразувиднорастеиянаиволнуетсяонаоткрьл
адверыверандьшагнулавтемнотуспустиласыпоступенькампрошлаподоркюкеподкустьщ
иренитомприслушивалсякеешагамонаопяыыпозваламолчаниеонапозвалаеседваразатом
ксесиделвкомнатекотсейчассдлиннойдлиннойузвойулицьдонещетсцголосдугласаидума
мнебесповойсяяидунодугласнеотвечалтоддолгиедвеминутьщиделглядянараскрьтуюпос
телынамолчащеерадиоимолчащийпатефонналюстругдекакнивчемнебьвалопоблескивал
истеклянньевисюлыкинаковеррасписанньйпунцовьмиифиолетовьмизавитушкамипотом
нарочностукнулногойокроватычтобьпоглядетыбудетлиболынооказалосыболынодверыв
ерандьсоскрипомоткориласыимамасказалапойдемтомпройдемсякудапростопоулицеиде
монвзялеезарукуонипошлипосентджеймсстритасфалытподногамибьлвщенщетепльйсве
рчкистревоталигромчепрбюнегоксгущавшейсяыымеонидошлидоуглайвернулиидвинул
исыпонаправлениюкзападномуоврагугдетопропльлавтомобилысверкнулвдалифарамина
улицчхникакихпризнаковжизнинисветанидвдюенрявоегдепозадимерцалислабоосвесен
ньеквадратьоконвтойсторонеоткудаонишлиневщенщелеглиспатынооченыоченымногие
домаужестоялибезогнейиспалиапередневоторьмитожетемньминакрьлечкчхщиделиихоб
итателиивполголосавеливечернвжбещедувоегденаверандчхпоскрипьваликачелихоыыбь
отнцбьлдомасказаламамаонасжималакскоейболышойрукерукутоманупостойдаймнетол
ыкодобраыысядоэтогомалычишкидушегубопяыывьшелнаохотуонубиваетлюдейксемгро
зитопасностыниктонезнаетгдеикогдаонвдругпоявитсявотклянусыпусыытолыводугприд
етдомойяеготавотколочувекбудетпомниыыонипрошлиесеквартелитеперыстоялипередче
рньмсилуэтомнемнцвойбаптистскойцерквинауглучепелстритигленрокксотнешаговзаце
рвовыюначиналсяоврагтомпюечуялегооттудатянулоканализационнойтрубойсгнившими
листыямидушньмивлажньмзапахомсплошньхзеленьхзарослейоврагбьлширокийизвилис
тьйонперерезалгородимамаксегдагокорилаптоэтоиднемтонепроходимьедебриаужночзж
кнемулучшеиблизконеподходиыыоттогопторядомцерковыстрчхидолжндбьрасщеятысян
отомувщеравнобьлкюутвовэтокчастемнаябезединогоогонькаонаказаласыхолоднойибес
полезнойразвалинойнакрджоврагатомубьлоксегодесятылетонничеготолкомнезналосмер
тистрчхэужащесмерыыэтовосвоваякуклавясикеонвиделеевшестылеттогдаумерегопраде
душкаилбюалвгробуточноогромньйупавшийястреббепмолвньйидалекийнивогдаболыш
еоннескажекчтонадобьыыхорошиммалычикомнивогдаболышенебудетспоритыополитик
есмерыыэтоегомаленькаясестренкаоднаждьутромемубьловтовремясемылетонпроснулс
язаглянулвеевольбелыкуаонасмотритпиямонанегозастьвшимислепьмисинимиглазамиап
отомпришлипждииунеслиеевмаленывойплетенойкорзинкесмертыэтовогдаонмесяцспус
тястоялвозлееевьсовогостулычикаивдругпонялптоонанивогдаболышенебудеттутсидеты
небудетсмеяыысяилиплакаыыиемупюенебудетдосадночтоонародиласынасветэтоибьлас
мертыинщесмертыэтодушегубкоторьйподкрадьваетсяневидифкойипиячетсязадеревыям
иибродитпоокругеивьжидаетиразилидвавгодприходитхждавэтотгороднаэтиулицьгдевеч
ерамивщегдатемноптобьубиыыжеещинузапоследниетригодаонубилтренэтосмерыынощ
ейчастутнепростосмертывэтойлетнейночипомдалекимизвездаминанегоразомнахльнуло
вщептоонисньталвиделисльшалзаксюскощюизныионзчхлебьвалсяитонулонисошлистро
туараизчшагалипопроточтаннойусьпаннойсебнемтропинкепообестороньгустороласор
наятраваивнейгромвонеумолчнотрещалийверчкитомпослушношелзаматерзжболышойх
рабройпрекраснойегозащитницейотвщегойветатаквдкоемонишлиишлиивотостановилис

ынасамофкраюцивилизациивоврагздесывэтойпропастипосредичерной чащобьвдругсосре
доточилосыксечегоонникогданеузнаетинепойметвщепткюиветбезьменноевнепроглядно
йтенидеревыеввудушликодзапчхегниенряведыонисматерзжздесысовщемодниееерукад
ркюитдадркюитемунепочудилосыноокчегомамаведыболышесилынееумнееегонепюели
ионаткюечувствуетэтунэуловимуюугрозутозловесеечтозатаилосытамвнизуищейчасвып
олзетизтемнотьзначитмкюновьрастиикseравнонестатысилыньмзначитстатывзросльмво
вщенеутешениезначитююизнинетприбежищанеттакойнадежнойцитаделиптоустоялабып
ротивнадвигджсихсяужасовночисомнениязразрьвалиегоморкюеноевновыобожглоемухол
одомгорловщевнутрипохолоделопоспинепошелморозоледенелирукииногиемувдругстал
ооченызябвоточновновыналетелиппрошлогодекабрыскийветертаккотоноптозначитэтоу
часыыксехпждейкьюдьйчеловекдлясебяодинединственньйнасветеодинединственньйса
мпосебесредивеливогомнкюествадругихлюдейивщегдабоитсявоткавсейчаснузакричиш
ыстанешызваыынапомощывомукавоеделотымапоглотитводномгновеныеодночудовищн
оеледенящеемгновеныеиксеконченонщезадолгодорассветазадолгодотогокакполицейски
еначнутпрощупьваыыйвоимифонарикамитемнчжрастрекоженнчжтропинкуинанейзашу
ршитсебеныподногамилюдейвоторьевсмятениикинутсянапомощыидажееслионисейчас
толыковпятистчхшагахоттебяапюнавернотаконоиесыытемньйприбойможетзчхлестнуы
ызатрисекундьиотнятыутебяксеткоидесятылетдюизныэтоодиночестковнезапноеоткрьти
еобрушилосынатомакаксокрушителыньйударионзадрожалмаматкюеодинокавэтуминуту
ейнечегонадеятысянинасвятостыбраканиназаситупжбясейсемыининавонституциюсоед
иненньхштатовнинаполициюейнеквомуобратиыысякромесобственногосердцааксердцес
коемонанайдетлишынеодолимоеотврасениеистрахвэтуминутупередкаждьмстоитскоято
лыкоскоязадачаикаждьйдозюенсамеерешитытьсовщемодинпоймиэторазинавщегдатомп
роглотилкомокзастиявшийвгорлеиприжалсякматеригосподинедайейумеретымолилонне
делайнамничегоплохогопапапридетссобранрячерезчасиеслидоманикогонебудетмаыыдв
инуласыпотропинкевдикуючащумамтьзадуганебойсядрожасимголосомсказалтомснимн
ичегонеслучилосытьзанегонебойсяснимничегонеслучилосыонксегдакозвращаетсяэтим
путемголосматеризвенелотнапргюенряясторазговорилаемуходидругойдорогойноэтипро
клятьемалычишкиксеравнолезутнапролофкогданибудыонпойдеттудаиболышеневернетс
яболышеневернетсяэтоможетозначатычтоугоднобродцгипреступникиыыманесчастньйс
лучайаглавноесмерыыодинкоксейкселеннойнасветемиллионтакихгородишекивкьюдомт
акжетемнотакжеодинококьюдьйтакжеотксегоотрешенвкьюдомскоиужасьискоитайньпро
нзителыньезауньвньезвукискрипкикотмузькаэтихгородишекбезсветаносомнкюествомте
нейакавоенеобятноенепомерноеодиночествцаневедомьеоврагичтозасасьваюткактиящин
ажизнывэтихгородишкчхпоночамоборачиваетсяледенясимужасомразумусемыедетямсч
астзжсоксехсторонгрозитчудисеимякоторомусмертыматысновагромвопозвалавтемнотуд
угласдугивдругобапочувстковалиптотослучилосыйверчкиумолклисталосовщемтихоони
незналптобьваеттакаятишинабеспределынаябездьханнаятишинаотчегозамолчалисверчк
иотчегокакаяэтомупричинапреждеонинивогданэумолкалиникогдазначитзначитщейчасп
тотослучитсяказалосыоврагнапрцгаетскоичерньемьшцьвбираетвщебяксесильспясихгор
одвовифермнамногиемиликокругвеликаятишинапропитанньхросойлесовидолининакать
вджсихсякакприбойхолмовгдесобакизадравмордькоютналунуксясобираласыстекаласыс
тцгиваласыводнуточкуиксамомщердцетишиньбьлионимамаитомвотщейчасщиюминуту
чтотослучитсяптотослучитсясверчкиксемолчатзвездьопустилисытакнизкочтокажетсяпр

отянирукуинапалыцчхостанетсяпозолотаихнесчестызвездондюаркиеколючиексерастет
разбухаеттишинаксеострейнапияженнейкюиданиеохкактемнопустьннокакбеспрмжтнои
вдругдалекодалекозаоврагомголосяздесымамидумамаисновамамамамидушлепшлепшле
змчатсяногивтеннисньхтуфляхподнуоврагасхохотомнесутсятроемалычишекбратдугласч
арливудмениаюонхафбегутхохочутзвездьвзвилисывверхточнодесятымиллионовпюален
ньхулитоквтянулийвоирожкисверчкизастревоталитемнотаотступалаиспуганнаяошарчш
еннаязлобнаяотступилапотеряваппетитведыонасоксемпюесобраласыпоживиыысяивдру
гейтакгрубопомешалиикогдатемнотаотхльнулаточноволнаковремяотливаизнеекозникли
смеясытроемалычишекмамтомприветисразувокругзапчхлодугласомведыотнегоксегдапа
хнетпотомтракойдеревыямиветвямииручыемвампредстоитпоркамолодойчеловевобявил
амамаотеестраховиследанеосталосытомзналонаникогдаююизнинивомупроэтонерасска
жетникогданостранэтотнавщегдаостанетсяунеевдушеивдушетоматкюетемнойлетнейно
чзжонишлидомойспаыыкакхорошочтодугласжикойкакхорошоанаоднусекундутамнакра
юоврагаемуподумалосыгдетодалекопосмутномуозаренномулунойлесунадвиадувомпото
мвнизуподолинепрогрохоталпоездонокчаянносвистелточнобезьменньеюелезньйзверыз
аблудилсявночитомулегсявпостелыиядомсбратомвесыдркюаонприслушивалсякэтомуйв
истуидумалдалеводалевотамгдещейчасмчитсяпоезаюилихдвтжродньйбратиумеротвосп
алениялегкихмноголетназадкотвтакущюеночыдугласлбюалиядомотнегопчхлопотомиэт
обылокакколшебсткотомпересталдрожаыытолыводвевнщрязнджнавернякадугпрошепта
лонкакиеоднаптоночзжпюаснотемнцадругаяеслимистерауфманвогданибудывсамодделе
построитмчшинусчастыясоврагомейксеравнонесощладатыдугласнемногоподумалповто
риптотьсказалониумолклинаулицевнезапнораздалисышагиближеблдюевотониужепомде
ревыямикозледоманатротуаремамасоскоейкроватинегрофкосказалапапаидетинеошибла
сыа