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

КРИПТОГРАФІЯ

Комп’ютерний практикум

Робота № 3

Варіант 4

Виконали

ФБ-33 Грабченко Олександр

ФБ-33 Стогнійчук Інна

Київ – 2025

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

Постановка задачі:

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) , (ba 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

Знаходимо 5 найчастіших біграм в ШТ

```
Найчастіші біграми в російській мові: ['ст', 'но', 'то', 'на', 'ен']
Найчастіші біграми в шифротексті: ['еш', 'еы', 'шя', 'ск', 'до']
```

Розв'язуємо систему з методичних вказівок:

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

$$Y^* - Y^{**} \equiv a(X^* - X^{**}) \pmod{m^2}.$$

$$b = (Y^* - aX^*) \bmod m^2.$$

Потім відбувається перебір ключів та перевірка тексту на змістовність (сумарна кількість літер 'о' 'а' 'е' не менше 25%). Щоб побачити всі перевірки програми, VERBOSE_MODE = True

```python
def is_text_meaningful(text, common_chars=('о', 'а', 'е'), threshold=0.25):
    if not text: return False
    count = sum(text.count(char) for char in common_chars)
    return (count / len(text)) > threshold
```

```
VERBOSE_MODE = True
```

```
Тестуємо припущення: ('ст', 'но') -> ('до', 'шя')
  Знайдені кандидати для 'а': [926]
    -> Перевірка ключа (a=926, b=954)
Тестуємо припущення: ('ст', 'но') -> ('до', 'ск')
  Знайдені кандидати для 'а': [590]
    -> Перевірка ключа (a=590, b=523)
Тестуємо припущення: ('ст', 'то') -> ('еш', 'еы')
  Знайдені кандидати для 'а': [534]
    -> Перевірка ключа (a=534, b=332)
Тестуємо припущення: ('ст', 'то') -> ('еш', 'шя')
  Знайдені кандидати для 'а': [200]
    -> Перевірка ключа (a=200, b=733)
Тестуємо припущення: ('ст', 'то') -> ('еш', 'ск')
```

Якщо текст задовольняє умову:

```
--- ЙМОВІРНИЙ КЛЮЧ №1 ЗНАЙДЕНО ---
Ключ: (a = 390, b = 10)
Розшифрований текст:
'еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомнодоказатьэтоневозможнокорееэтойнеобходимостьювнаказаниидляпсихическойэкономиидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиунижениййосуждение достоевскоговкачествеполитическогопреступникабылонесправедливымиондолженбылэтознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслуженногоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонаказанияондалсебянаказатьзаместителюотцаэтодаетнамнекотороепредставлениеопсихологическомоправдании наказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковжаждутнаказанияеготребуетихсверхяизбавляясебятакимобразомотсамонаказанияготктознаетсложноеи
'
```

VERBOSE_MODE = False

Розшифрований текст:

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомнодоказатьэтоневозможнокорееэтойнеобходимостьювнаказаниидляпсихическойэкономиидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиунижениййосуждение достоевскоговкачествеполитическогопреступникабылонесправедливымиондолженбылэтознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслуженногоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонаказанияондалсебянаказатьзаместителюотцаэтодаетнамнекотороепредставлениеопсихологическомоправдании наказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковжаждутнаказанияеготребуетихсверхяизбавляясебятакимобразомотсамонаказанияготктознаетсложноеи

изменчивоезначениеистерическихсимптомовпойметчтомыздесьнепытаемсядобитьсясмысл
априпадковдостоевскогововсейполнотедостаточнотогочтоможнопредположитьчтоихперво
начальнаясущностьосталасьнеизменнойнесморянавсепоследующиенаслоенияможносказат
ьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестивсвязиснамерениемубитьо
тцаэтолежащеенасовестибремяопределилотакжеегоотношениекдвумдругимсферампокою
щимсянаотношениикотцукгосударственномуавторитетуикверевбогавпервойонпришелкпол
номуподчинениюбатюшкецарюоднаждыразыгравшемуснимкомедиюубийствавдействитель
ностинаходившуюстолькоразотражениевегоприпадкахздесьверхвзялопокаяниебольшесвоб
одыоставалосьунеговобластирелигиознойпонедопускающимсомненийсведениямондопосл
еднейминутысвоейжизнивсеколебалсямеждуверойибезбожиемеговысокийумнепозволялем
унезамечатьтетрудностиосмысливаниякоторымприводитверавиндивидуальномповторени
имировогоисторическогоразвитияоннадеялсявидеалехристанайтивыходиосвобождениеотг
реховииспользоватьсвоисобственныестраданиячтобыпритязатьнарольхристаеслионвконеч
номсчетенепришелксвободеисталреакционеромтоэтообясняетсятемчтообщечеловеческаяс
ыновняявинанакоторойстроитсярелигиозноечувстводостиглаунегосверхиндивидуальнойси
лыинемоглабытьпреодоленадажееговысокойинтеллектуальностьюздесьнасказалосьбымож
ноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаиподвергаемдосто
евскогооценкеимеющейправонасуществованиелишьспристрастнойточкизренияопределенн
огомировоззренияконсерваторсталбынаточкузренияявеликогоинквизитораиоценивалбыдост
оевскогоиначеупрекправедливдляегосмягченияможнолишьсказатьчторешениедостоевског
овызваноочевиднозатрудненностьюегомышленияявследствиеневрозаедвалипростойслучайн
остьюможнообяснитьчтотришедеврамировойлитературывсехвременктрактуютоднуитужете
мутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамазовыдостоевскоговов
сехтрехраскрываетсяимотивдеяниясексуальноесоперничествоиззаженщиныпрямеевсегоко
нечноэтопредставленовдрамеоснованнойнагреческомсказаниииздесьдеяниесовершаетсяеще
самимгероемнобезсмягченияизавуалированияпоэтическаяобработканевозможнаоткровенн
оепризнаниевнамерениииубитьотцакакогомыдобиваемсяприпсихоанализекажетсянеперенос
имымбезаналитическойподготовкивгреческойдраменеобходимоесмягчениеприсохранении
сущностимастерскидостигаетсятемчтобессознательныймотивгерояпроецируетсявдействит
ельностькакчуждоеемупринуждениенавязанноесудьбойгеройсовершаетдеяниенепреднаме
ренноиповсейвидимостибезвлиянияженщиныивсежеэтостечениеобстоятельствпринимаетс
яврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповторениятогожедействиявотно
шениичудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинан
еделаетсяникакихпопытокснятьеессебявзвалитьеенапринуждениесосторонысудьбынаобор
отвинапризнаетсяикаквсецелаявинанаказываетсячторассудкуможетпоказатьсянесправедли
вымнопсихологическиабсолютноправильнованглийскойдрамеэтоизображеноболеекосвенн
опоступоксовершаетсянесамимгероемадругимдлякоторогоэтотпоступокнеявляетсяотцеуби
йствомпоэтомупредосудительныймотивсексуальногосоперничествауженщиныненуждаетс
явзавуалированииравноиэдиповкомплексгероямывидимкакбывотраженномсвететаккакмыв
идимлишьтокакоедействиепроизводитнагерояпоступокдругогоондолженбылбызаэтотпосту
покотомститьностраннымобразомневсилахэтосделатьмызнаемчтоегорасслабляетсобственн
оечувствовинывсоответствиисхарактеромневротическихявленийпроисходитсдвигичувство
виныпереходитвосознаниесвоейнеспособностивыполнитьэтозаданиепоявляютсяпризнакит
огочтогеройвоспринимаетэтувинукаксверхиндивндуальнуюонпрезираетдругихнеменеечем
себяеслиобходитьсяскаждымпозаслугамктоуйдетотпоркивэтомнаправлениироманрусского
писателяуходитнашагдальшеиздесьубийствосовершенодругимчеловекомоднакочеловекомс
вязаннымсубитымтакимижесыновнимиотношениямикакигеройдмитрийукоторогомотивсек
суальногосоперничествоткровеннопризнаетсясовершенодругимбратомкоторомукакинтер

еснозаметитьдостоевскийпередалсвоюсобственнуюболезньякобыэпилепсиютемсамымкак
быжелаясделатьпризнаниечтомолэпилептикневротиквомнеотцеубийцаивотвречизащитник
анасудетажеизвестнаянасмешканадпсихологиейонамолпалкаодвухконцахзавуалировановел
иколепнотаккакстоитвсеэтоперевернутьинаходишьглубочайшуюсущностьвосприятиядосто
евскогозаслуживаетнасмешкиотнюдьнепсихологияасудебныйпроцессдознаниясовершенно
безразличноктоэтотпоступоксовершилнасамомделепсихологияинтересуетсялишьтемктоег
овсвоемсердцежелаликтопоегосовершенииегоприветствовалипоэтомувплотьдоконтрастно
йфигурыалешивсебратьяравновиновныдвижимыйпервичнымипозывамиискательнаслажде
нийполныйскепсисациникиэпилептическийпреступниквбратьяхкарамазовыхестьсценаввы
сшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпостигаетчтодмитр
ийноситвсебеготовностькотцеубийствуибросаетсяпереднимнаколениэтонеможетявлятьсяв
ыражениемвосхищенияадолжноозначатьчтосвятойотстраняетотсебяискушениеисполнитьс
япрезрениемкубийцеилиимпогнушатьсяипоэтомупереднимсмиряетсясимпатиядостоевског
окпреступникудействительнобезграничнаонадалековыходитзапределысостраданиянакотор
оенесчастныйимеетправоонанапоминаетблагоговениескоторымвдревностиотносилиськэпи
лептикуидушевнобольномупреступникдлянегопочтиспасительвзявшийнасебявинукоторую
вдругомслучаенеслибыдругиеаа