

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

Криптологія  
Комп'ютерний практикум

Робота №3

Виконали:  
студенти групи ФБ-14  
Мартиненко Даніїл  
Цуканов Данило

Київ-2023

## Мета роботи:

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

### Шифртекст варіанту 4:

шжуйажушпккфшчфбждоцподійсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугфбзчшоходовзбряцкмдбэдцхзнощкяозою  
этцюзныертзилфоцбчполфмэдцщкйкшйэыйрэйкчозычфждьмйшотдотзьонойсцзоюдууюзсшштзрэыосяфоешыенывдьмиыиышчрб  
гянямзюдскмдайыаяоешезвжпоноэрэжчжшбчдофшщофбяоязфышжвонцеырайхмучмсшывчфвэрфешмяояйывшеыйсбжощдзшя  
рфбждоцподлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшяшксавотзйбйкжзщпопсйкоефцпрзюэдцшямсканзомажужыыщсшмычмэжглр  
зщыезскщквкшятоэыйштибшяшкочщкмыйейыйвдьмиышчвккцошцеызонорйвкхпшсзунрмоншзоязшяэдхпезхлсопжипеызохлншплбй  
щждоыкфоскщквкшягоефоцзччскщквкшяканказешношлцромглтдоккжшскзыдншууезжурфешщпнзшятоужертцлвхшщпофожушпкк  
шяэывдьмиыйсжусжощккшйжррэсезшьоктдосыкфотфлщжшвдзылвхзпмжушжелящцдюппкгфкшскщквкшяозноуойэвзхягжжщрф  
яоэщпсчкжйэцшвдрйрэйкчфолжыймывдьмиышчдорддокыбзлжвочыезыяойеытяьочмскмзшядешмуяхшжбягжрайшайюпомогйжш  
фшайрмлзннтзхаокшйбчаошяанбчйтжмкжучбуфпошфбждоцподлвюпопэзбтцзопзоешйшохзодонофшайсцзожурфмовоцяанфшл  
ййбмьюсклжонскккжешзоешшоешоцжлыдаюйеызопышжфоочсквжабжнзбляхзеккцезшйййсцзоюдьмйшнхдоаоешезвжбяршвдшя  
полфзятзбжьоисаййжгоелзурмейссожзешопхпимсжсказзшяшйношшомглтдонзпксезэжюпшжхявушйгожурфлцгцншвдрдшцо  
цыынеыхзнфлфтфалаяыжфйквбждзэчяыжхыхоцыынеыяпомгтднотлккжжипеызохлщпоряпзелцджзксэлвщпчзгпшсмыжумилцэ  
бтцзохлмофхэыенеткзеадьгпуротынщйайкбазушппязхлдрйпоазясслщдджишщплзджиношлцлбжхяскыосяэищештцедууьмншйк  
рзшяцлдвзбряцкмдррхфшжэпмуапзчвомощкхыхзюнонхзхпрчфлоешщпоцбжщлцзнобцэжхякузаяямзкомбырфзбжюжкшярьисозые  
ыйсхпрфешщфоефзбжнзтыссяилянахпезфщпмшявжзтцтйэоцбазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмюпштцышйшйычмыйз  
хйшмшжшалтыбжхябжюакпопышччдншуусйжюупчфюшжйкмяефопифбкконзобюпдокзшярдуюпшлвляешууяхшжпонойкыпюш  
щчмысклзыцбмйалзоцнрряеишыфсхдаыосябжьоиофсхзшншзунрюпяябтцномюпйшажьосжрешжзщыцзешйккшхчхдосажуюши  
мйшлпыпущурряешбзкцкоплпотзуыайжхжшеыабрязодхпрчфляешоцкзвдаямымайдосшщоччдыозлжщшйфшшощоцххлцюпзщж  
щккжююпцчзпэыиывдншуушсешяюшбчкзуаяямзозхьпешьоаоешывмкйыдвбжжщрэысымяблщлщсгялаэышйльмксанжутоао  
нзсккжрзвюптжждшсэыпзщцделоцлбжанхмлзннскюдьмоцбжпэсйсцзодбкзвыкшэпдойхдоуаншщкбаекшйбчншузбряешйкешзо  
ешчбгыяюиоцпзмямодпмучкшйаоешезвжпоновгеьзрйхесзкйькосктлсезшьоекшялцмнажжусжюужщышсдондпмкзшягожурфлце  
ызоножяяоэмкзшяпдмызэгтйшшууешоцсаксдондымкзшяплццдлвляудмйядойккощзшяекшэйфбждоцподлвляскмзбдкзжжущпрф  
уашфсчдвбждчвхешчфочытцмнажжквканфшууфиеыхзоешезвжпонодаыпищомзмятаймйшалтыеызоешедвайннзшязпкрфеш  
мяеыцяповкрфекуяжубждоджглкыбжанцйсцзорэкшяанфшншрязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыноувдлщчфилюшо  
шжшшйкшшйцомгулщаджиногпуготсяужзюжмкчкнцжшязцжюяйкбэйканпдпуйьмюпйфбждоцподлвюпопэзпшкхужйупбзлж  
фяфохяшфвчшякжядтлоцлщезсочзсыяхшципялэмнщечыяражуййюзвждвжмдмхзосшзбкззжюкуценьопщуййтодыюпыиызопызвкмз  
юдайюдьмиыяхфшщжфвчшящжюпмуоюкжшбчбьщжйрйшзюаишюуаждчвхышщпмщпбкюаяоекшярбтпхямзюдечрэйкиордищця  
мфочыхордаожщысезупмскшыпсказзшялщяанншшкщкпоноуаоаощаекшйбчжучбгыяюиоцпмднщжшбчтзчзкзюгяюалэчмныо  
цошяхшжпкбчфнодзодзопзухщжпюьфйказтзрэыосяфощждчвхыхзжусжфрйктзшсясжьзоешрйжпзжбжяоешывбзлжщшйфшрэц  
жсокийшлщлцыксфохямвмуйжчужезаяалжшбчшфсесшмяпзюнзоешедвлгфезшйдбриялгфеыхзсккчкышезтлыниоовмшссожзбизв  
фвчшяеыабкзтыйимеызочбюпэзбпифрйбжхяузыпуяхыщчрхьэызавжкщитдоешзхыххзрэешчпзюнешибрияшякжшбчфуэжмзшвд  
щкпонишсжшшквкшщпопшбтгтэйшмштцедзббжнзмоошууеышчдонорзлзджипщчюоцыынеыявляомяргяшптцпмдущесзоншшкм  
окцжшлвждвдрэскалцйекжшбчкожччибзлжжзномыактзлзмкжшбчшящкбййбзбашжддыщдзшжэзччамекуаянозскжуэыошлзшяшжбж  
дояротлынсаскрэууншмяскжупмскжшбчдвдвжыглцечмясксщкбаекжшбчфшууэжтлмдэйсцжшмошквканбчтзйбкжзщпопсйзоуже  
ртцлвхшжбжямэсоецзбйкмюнозоекшвуджпюьфйказсшлячовуншеыртццзпохпемызоешдбждсозжбизблжхышжйрйшзюаишф  
алйащфсчподоносшншмоешдбждтзпсчжшбчншщзнэйсешовбтдхлжурфбжфюшлщлцыксфохявжядтлоцлщлвбжзбмущямзешко  
шеычяратзилгфбзлжпкылоцдуюпиыяйкныляфчбюпповбнзцжшзюйиппифрйшкжэппншйкрзщыйахпжшжшвдщкхйппифрйуап  
ндощкпорфсесшмябюпмьосязывмуйчмоешдбждшуивлщощефтцрзюэдцсавкшншмоешдбждншайешюшлбжюиуырафовуьмайтз  
вжгцррешбжлзмканюакыбзйхдодвууэжкцмэсчжсшопжипеызохьпешьомьяравжшюишжешмясжжйкгшмуайтзфуншхшжбялцуцы  
йсжулямрчфюшпфмяявлжиппопзышбмунрчфюшьюсокыиыхзхпезпышжмосоьбжхядамофыношотдовккшяабйчуцжелжрбрякывд  
юшлвхдошзюаббжжуэырйбзщтелмяилщкцжжщрэысаныблщлщемыжучмдубзвфалаяоышйеынозмзыжйэозкцкогрчфюшажжжшк  
гфсймовккцивыйгшьлфжшншмолдопшайскжущпнзшядауйиыалшжпоноуяыкпзсчсрчфюшскюклфощидяхфшжщлщаджибжю  
муяззшоунврймзвжзпфотывдохлцюпаядхпимиыраыжнэюшсйокбжярзэзонырйкоцыынеышчжшкбшзюаьфжяюуистгдншуулв  
йншопэзжбжконзоносочзсыяхшципхордаожщызбрякыбзлжжжюпмуяззшоунврйвушайшайподояохлщкбьяшмушжзовказхяанаоешезв  
жбжкбмурфоцхпэсшопжипеыилзтцчмгнлдрэбтюянзужнепзжыжййшкжжэгцлщчеплщйшжбрякыиыхзфшайтцлбгцабхяыщцяохяупа  
йтзншщзнэйсшкпопншфузхпмдьюшшящксктлзокрзпмжзешсхыэжазидыуфужертцлвхзэоскфопбощкчфылидымшкбмщпбкюаяоек  
зожзуапонзьяншвдщкцждоушвжитдочзкзжзсыкшяскыосяпнжцнэохфсфлжжешзоешэпбжжущчхябфбждоцподлвямэжглцйекжшкч  
йфибяншкешнтзужертцлвщчжфйфйракбюощзшжаокыиышчсозжбисеызоуэсумуяуыжддосшншмоешдбждсозжбигцскыкфотфлцабг  
ыовояфяшмущжжлжщлщмимшйшгшезновжьюшйээфшцрэмкуягшзбзсносозжбисеыядвзбряжзжиппоцбпгдхлбивоанаопышй  
кешзюкюывруххнзевжйэйканэушщпозмазонийфмяцяюакбмуамуысйчбямппыйыяюдйшлщлщыжмкгфеййсмофыксюдабгякашяблб  
гцабхямзюдйсжущжеляыцдсэйканюрщкйкакчодазешажшзскятпжзджпзчшяжжйкгшмускбфсчаоешезвжпонопмйкйвюпууэжжю  
шряйшешпугмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзоешедншщзнэйсешылбэяюыкжшбчзкзтырйскпнзшсясшмышйсщжшз  
псчанбчдайкрзшяшйомршшешышчуфтгчыщокыкхйшнхдохлщшсншешйкцжшншзччжрлязшядябтшяанбжучмкзшяшйрлщяег  
дяуярымояышйшажфямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвжпоноэбкзешдбшярлзджипношлщлщырэмзуиыххскмыуф  
оцядпожрчфюшвжжурфлцгжбжюууфнышчскподояоешщлжкешраоязжшжущпшоскскможжкшбцзвлвюпыхзюдншуусйшфкзныб  
жхяншзюгяуннотюянзашщидяблзныртцлщайдбкзешдбшянфсчтзномофшсжцкгпзюанамзепяпыэжйэзпэгдншуушешфалноыжгллк  
еыщжуясацуивхзак

### Завдання:

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елемента 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.

```
def extended_gcd(a, b):  
    if a == 0:  
        return b, 0, 1  
    else:  
        g, x, y = extended_gcd(b % a, a)  
        return g, y - (b // a) * x, x  
  
def mod_inverse(a, m):  
    g, x, y = extended_gcd(a, m)  
    if g != 1:  
        return None  
    else:  
        return x % m
```

(розв'язування лінійних рівнянь вбудовано в функцію пошуку потенційних ключів, далі буде)

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

```
def count_bi(text):  
    c2_nocross = dict()  
    i = 0  
    while True:  
        if (i >= len(text) - 1):  
            break  
        b = text[i] + text[i + 1]  
  
        if b not in c2_nocross.keys():  
            c2_nocross[b] = 0  
        c2_nocross[b] += 1  
        i += 2  
    return c2_nocross  
  
c2_nocross = count_bi('...')  
print(sorted(c2_nocross.items(), key=lambda item: item[1], reverse=True))
```

[illegible]

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

```
def calculate_index_of_coincidence(text):
    frequencies = {}
    for char in text:
        if char in frequencies:
            frequencies[char] += 1
        else:
            frequencies[char] = 1
    ic_value = sum([(count * (count - 1)) for count in
frequencies.values()]) / (len(text) * (len(text) - 1))
    return ic_value
```

```
def decrypt(text, a, b):
    result = ''
    a = mod_inverse(a, m ** 2)
    if a == None:
        return -1
    i = 0
    while True:
        if (i >= len(text) - 1):
            break
        Y = alphabet.find(text[i]) * m + alphabet.find(text[i + 1])
        X = a * (Y - b) % (m ** 2)
        result += alphabet[X // m] + alphabet[X % m]
        i += 2
    return result

def decrypt_keys(text, keys):
    textes = dict()
    for i in keys:
        d_text = decrypt(text, i, keys[i])
        index = calculate_index_of_coincidence(d_text)

        if abs(index - 0.0553) < 0.01:
            textes[i, keys[i]] = d_text
    return textes
```

Відсіювання текстів відбувається, як і в другій ЛР, за допомогою індексів відповідності (якщо текст змістовний, то його ІВ близький до ІВ мови)

## 5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

{(390, 10): 'если правда что достоевский в сибире был подвержен припадкам то только лишь подтверждает то что его припадки были не гокарой но более естественной нуждой сего дабыл караемим образом но доказать это невозможно скорее это необходимость наказания для психической экономики достоевского объясняется тем что он прошел несомненным через эти годы бедствий и унижений осуждение достоевского как человека политического преступника было несправедливым и он должен был это знать но он принял это не за служебное наказание от башки царя как замену наказания за служебного им за свой грех по отношению к своему собственному чувству самонаказания он дал себя наказывать заместителю отчасти это дает нам некоторое представление о психологии искомо оправдании наказания и при судимых обществу на самом деле так много из преступников жаждут наказания и от него требуются сверхизбавляя себя таким образом от самонаказания от которого знает сложное и изменчивое значение истерических симптомов и мы тут не пытаемся добиться с мыслеприпадков достоевского о в сей полноте достаточного что можно предположить что их первоначальная сущность осталась неизменной не смотря на все последующие наложения можно сказать что достоевский такникогда не освободился от угрызений совести в связи с намерением убить отчасти лежащее на совести время определило так же его отношение к двум другим ферам покажи нам отношения к отцу к государству авторитету к вере к богам в первой он пришел к полному подчинению башке царю однажды разгыравшему с ним комедию убийства в действительности нахолившуюся у него в отражении в его припадках здесь верхняя эпохания невольное свобода ставало сунего в области религии и одной по недопускающим сомнения сведениям до последней минуты своей жизни все колебался между верой и безбожием его высокий ум не позволял ему не замечать трудности смысла в аниаккаторым приводить в индивидуальном повторении мирового исторического развития на деле являясь идеалом христианской тивы ходои освобождение от грехов и использование собственных страданий чтобы притязать на роль Христа если он в конечном счете не пришел к свободе и стал реакционером то это объясняется тем что общечеловеческая сновьянина на которой строится религиозное учество диглау негосверхиндивидуальной силы не могло быть преодолено даже его высочайшей интеллектуальностью здесь насказалось бы можно прекратить в том что мы отказываемся от беспристрастности психоанализа и подвергаем достоевского оценок и мейшй правона существование и лишь пристрастной точки зрения определенное мировоззрение консерватор стал бы на точку зрения великого инквизитора и оценок и в достоевского иначе упресксправедливляе го смягчения можно лишь сказать что решение достоевского вызвано очевидной трудностью его мышления вследствие не врозавали простой случайностью можно объяснить что три де в драматической литературе все хвремента кутю от нуту жетемуте от цубийства царь дигло фоклагамлетешкспира братья карамзovy достоевского в о в сех трех раскрывает сию мтивдеяния сексуальное соперничество и заженщины прямее сего конечно это представлено в драме основанной на греческом сказании и здесь деяние совершается с амимгером без смягчения и завуалирования поэтическая обработка не возможна откровенное признание намерения убить отчасти какою гомьдобиваемся при психоанализе как жетс я не перенося и безаналитической подготовки в греческой драме необходимо смягчение при сохранении сущности мастера кидости гетс я тем что бессознательный мотив героя проецирует с я действительность как худшее ему принуждение навязанное судьбой герой совершает деяние не преднамеренно и повсей видимости без влияния женщины в себе жетостечение обстоятельств впринимается яврасчет как какон может завоевать царицумать только после повторения того же действия в отношении чудовища символизирующего отчасти по слого окако обнаруживается яю глашается го вина не делается никакими попытками съестсебя в звалить ее на принуждение с стороны судьбы на оборот вина признается я как в сецеляя инанаказываетс ячторас судку может показаться несправедливым но психологически абсолютно правильно в английской драме это изображено более еко свенно по поступку совершается с амимгером а другим для которого это тот поступок не является ячтцеубийством поэтом предсудительный мотив сексуального соперничества женщины не нуждается в завуалировании и равно издипов комплекс героя мы видим как бы в отраженном свете как бы в димлишь то какое действие производит на героя поступок другого он должен был бы за это поступок отомстить но странное изображение не в силах это сделать мы знаем что о его расслабляет собственное чувство вины в соответствии с характером невротических явлений происходит сдвиг чувств вины переходит в сознание своей неспособности выполнить это задание и появляются признаки того что герой воспринимает эту вину как сверхиндивидуальную он презирает других не менее чем себя если бы он добился с каждым по заслугам кутю и детотпорки в том направлении роман русского описателя уходит на шаг дальше издесьюбийство совершено другим человеком но для человека связанного с судьбой таким же сновьяниаккаторым отношениями как и герой дмитрий у которого мотив сексуалпилепсия тем самым как бы желая сделать признание что молпилептик невротик в нем отцеубийца и вот в речизащитника насудега же известная нам смешка над психологией и она молпала ко двухонках завуалировано великопепно так как стоить сеэто перевернуть нахолившь глубочайшую сущность воспринять достоевского за заслуживающего смешки и отнюдь не психология судебный процесс дознания совершенно безразлично что тот поступок совершил на самом деле психология и интересуются лишь тем что его в своем сердце желал кто по его совершению и его приветствовало поэтом в плоть до контрастной фигуры лешиве братья равновинны движимый первичным позывами и скарельна с лаждений полный скепсис ациники ипилептический преступник в братьях карамзovy ходит за пределы страдания на которое несчастный имеет право а на поминает благого вене которого в древности относились к эпилептикам и худшее в больном преступнике для него почти спаситель ввязавший нас в вину которую в другом случае несли бы другие аа' }

## Висновки:

продовжуємо вивчати атаки на шифри за допомогою частотного аналізу. В цій ЛР на прикладі афінного шифру, в якому біграми замінюються на інші за формулою  $y = ax + b$ . При розшифруванні робиться припущення, що 2 з найпопулярніших біграм мови переходять в 2 з найпопулярніших біграм шифртексту, створюється система рівнянь, з якої можна знайти потенційні значення ключа. Оскільки таких значень багато і вручну перевіряти тексти було б нераціонально, був обраний спосіб відсіювання текстового шуму за допомогою індексів відповідності (якщо текст змістовний, то його ІВ близький до ІВ мови).