МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря Сікорського»
«ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ»

КРИПТОГРАФІЯ

Комп'ютерний практикум №3

Виконали:
студенти 3-го курсу
групи ФБ-22
Власенко Г. В. та
Перебинос Р. О.
Бригада №2
Перевірив/-ла:
_____
_____

Київ – 2024

Криптоаналіз афінної біграмної підстановки

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 (2)).
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:

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

де біграма X^* перейшла при шифруванні у біграму Y^*, а біграма X^{**} – у біграму Y^{**}.
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

Було реалізовано функції для пошуку оберненого за розширеним алгоритмом евкліда (ітеративно та рекурентно) та функцію для вирішення лінійних конгруенцій (`ax = b mod m`). Функції знаходження оберненого та вирішення лінійних конгруенцій були покриті тестами. На Рис. 1 та Рис. 2 приведено реалізація цих функцій та прикріплюється разом з протоколом у файлі `subprograms.py`:

```python
def gcdEuclideanExtended(a: int, m: int) -> tuple[int]:
    """
    Вираховує НСД(a, m) та повертає відповідні коефіцієнти u, v.
    gcd(a, m) = um + va.
    """
    if a == 0:
        return m, 0, 1

    # gcd(a, m) = um + va.
    gcd, u, v = gcdEuclideanExtended(m % a, a)
    return gcd, v - (m // a) * u, u

def gcdEuclideanExtended2(a: int, m: int) -> tuple[int]:
    """
    u(0) = 1, u(1) = 0, u(i+1) = u(i-1) - q(i) * u(i);
    """
    modulo = m
    a, m = abs(a), abs(m)
    if a == 0:
        return m, 0
    if m == 0:
        return a, 0

    u0, u1 = 1, 0
    while m:
        u0, u1 = u1, u0 - (a // m) * u1
        a, m = m, a % m

    return a, u0 % modulo
```

Рис. 1. Розширений алгоритм евкліда

```python
def linearCongruence(a: int, b: int, m: int) -> tuple[list[int], bool]:
    """
    Повертає списком усі розв'язки лінійного порівняння ax = b mod m.
    """
    gcd, _, _ = gcdEuclideanExtended(a, m)
    if gcd == 1:
        return [(modularInverse(a, m)[0] * b) % m], False

    # Return error if b cannot be divided by gcd ≠ 1.
    if b / gcd != b // gcd:
        print(f"[!] ERROR: gcd(a = {a}, m = {m}) = {gcd} (≠ 1), but b = {b} cannot be divided by {gcd}!!")
        return [], True

    solutions: list[int] = []
    a //= gcd
    b //= gcd
    m //= gcd

    root = (modularInverse(a, m)[0] * b) % m
    solutions.append(root)

    for r in range(1, gcd):
        solutions.append(root + r*m)

    return solutions, False
```

Рис. 2. Розв’язання лінійних конгруенцій

Функція обрахунку частот біграм з лаб. роботи №1 була дещо модифікована, щоб повертати тільки n найчастіших біграм в переданому тексті. В методичних вказівках пропонується взяти 5 найчастіших біграм, але для нашого ШТ за варіантом цього не достатньо, а тому візьмемо 10 найчастіших біграм.

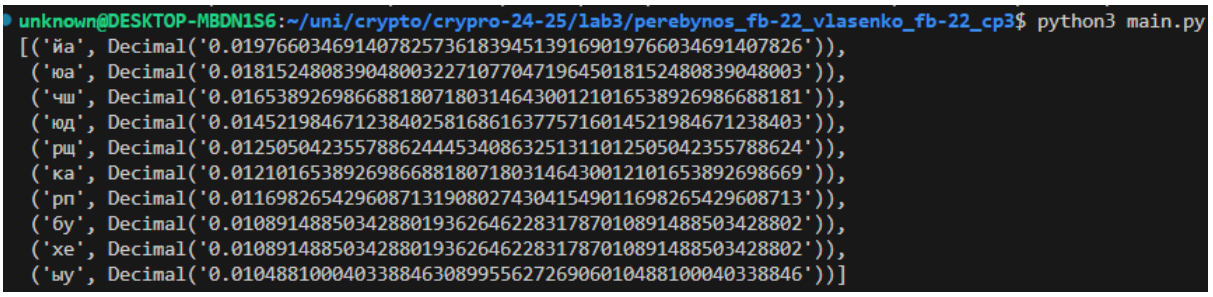

Рис. 3. Знаходження найчастіших біграм у тексті за варіантом.

Як зазначено в методичних вказівках, тепер треба порівнювати ці біграми з найчастішими і шукати можливі ключі. Для пошуку ключа запропоновано наступний алгоритм:

1. Обираємо дві найчастіші біграми відкритого тексту. Найчастіші біграми були взяті не з методичних вказівок, а з обрахунку частот біграм у відкритому тексті з лаб. роботи №1. Відповідно дві найчастіші біграми вийшли: “то” та “на”
2. Для знаходження ключа необхідно скласти систему з лінійних конгруенцій, якщо відняти одне рівняння від одного, то отримаємо формулу для підрахунку a - (`a = (y1 - y2) * (x1 - x2)^(-1) mod m`). x1-x2 це буде різниця числового представлення двух найчастіших біграм відкритого тексту. Нехай це буде x.
3. Тепер необхідно порахувати x^-1 mod m
4. Максимальна кількість ітерацій яку треба зробити для перебору n найчастіших біграм шифротексту дорівнює A_n^2. Тобто тепер необхідно перебрати всі можливі розміщення n найчастіших біграм шифротексту і для кожної пари біграм порахувати a якщо це можливо.
5. Для перевірки тексту на змістовність застосувати будь-який метод. В нашій роботі було використано метод заборонених біграм.

Можна помітити що в запропонованому алгоритмі немає лінійних конгруенцій, воно так і є.

Для перебору всіх можливих розміщень була використана стандартна бібліотека python - itertools.

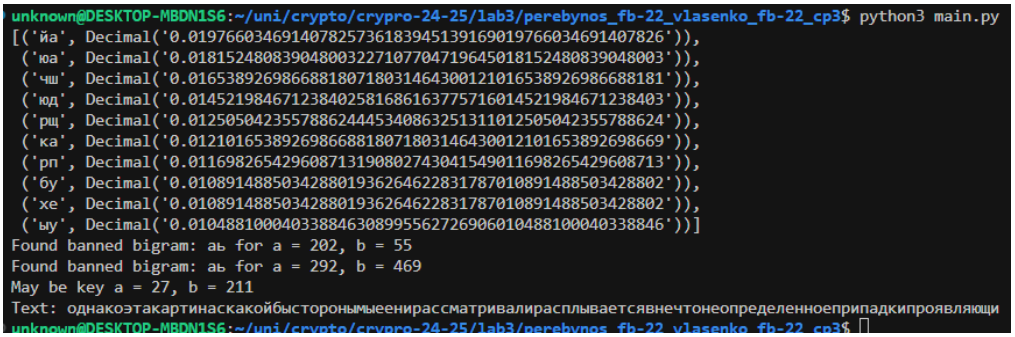

Рис. 4. Результат роботи програми. Знаходження ключа

Для автоматичного розпізнавання було обрано метод заборонених біграм, бо якщо текст достатньої довжини, то вірогідність зустріти заборонену біграму при неправильно підібраному ключі дуже імовірна. Всього існує 961 біграма (для алфавіту з 31 символом), в якості заборонених біграм було обрано: "аь", "оь", "яь", "юь", "еь", "ыь".

Ключ: a = 27, b = 211

Шифротекст (Варіант 2):

рйрщкагппрфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьй
ахещыйеьеюеэдсецчтыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшбуо
йщаищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекайаэк
яуклзщюгхегарпинцплппрффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукч
щысаэарюжштнцмосхрхлтечшишваллмппртелиюдьпкуурдщерритыачтахщышкаюйзхц
мздффнагещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэрщберою
азанхзушщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошр
щышгпфуыуйацдаюваллйыачларщзщроюалахдорцпиыщылшошрщйьфуйазлиекдвифу
щлбшашваллюсхщрохеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйдшгфч
прбердрйуюпнсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюдушлсбу
беюыхрдщндщфщейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчщр
оюаеймюбероюарпинымжизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойате
ащваюдюдкйчбйкпмтырйюенщлучихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкй
бвжшлжпшюечукемипнипцчушлсрйхпэснезщжмюдкенлхарпсдхйьчмэешйарпхппрэщц
жыщпаюехдпьхуйанацчрбюдхушчкацкдщтеэдвиййтагшфичиорхлфдщфкшышвамносви
ййдзьрыщышхемсующудршджьюанхрэцпымздффнарписюахьхууочрфчгшйкпаюехдсд
жжгшцчтыкйдшнануэифуларизсййушфиюдюдаюышькющяпцлдчьншгашэлашьухаедви
злиекдвидщлсхпкеышйрьчценавсачэаькудбюяхцмрцсдрпгекммьлекдхйыуыщйаудюлцч
исуюэиффриещжзьргшкдыууоьдглэшешбероюачпщылшыщдшэасуйаьпымкуюсщгхела
фитбюазуыщюаешуоналаолфдыууозмсдщьбукаощжзьрыщаыпмяызшхпбьйацчзюимпел
умсрйюасавдыугшбрмэтдйкяуришпчиоскчтхэейыосййричикзддрятаршроюазахачшфщч
шурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшчыачешудкгхавклаяхбмхашнэпос
юеюазнтдщьбудшщепщчшфикайаэкишныцмбээелучылшрщашошзсбужифчмэйкблкмос
нфэщкылшрщхлиечшритэзалаеймюбероюарптылшцюцрчийщпаюеющчшхпэщхеишаш
йамущьбукаьэзхцмустдмшыщдшцчсдхйыуыщйаудчикабпсаюезлиекдффыршдчимшлчл
эфуюазздрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдкебдкйющешхщнкшл
нуюсэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаюнежсщьйкэытэшс
осгпэпщепщчшфихехщюедшэпеемучщройкэысарепуосхасасйленкссвссеоамдосвпхрзш
мейрцлтедчусхеццкемчььсдмэшсрморушнллирмффаыпмяызшщфзсййымзсхажалафщнп
бупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщтечшджп
шюешпщьбуэщшчсщряаюэщкацкышщехеаитбюарщлсцпэсеегпосщерпусдюйаюдбучих
еэдэппртехарпеылегшмчхухаяютечшюдуссайщсллдыууокайасазаопчичпнхбморешэшса
ющуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемчтэхевателуцчисхпкучызшцшм
ейряжпшюешпщьбудшоылшищгамуыщюаешлуьпппрринхдщцадуришпчичифубелшмшм
вкйуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчушугрйхпцчсдьчфщроюаеп
жьюдмшеемучщроюазацчаябуащыщдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщщч
шмейртвещжзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвж
шоыачлаоыьчмбюдпаюехдхввамнхукчкйбвжшгсйасандуссагшяснежсчикммьлезлиекдб
юфшхдиырйгекбюдтдфчнцюдавлэкдусосйасадуклзщюдфчнцюдкемсуювпьюцкдщтечшэ
иащваейнцусюазблэчшгечофщгесаьпюачпжжпшюечуаюгарпсенуказаэпюазшлууросйас
ажлешзлйаудрйхрмэцпфжйахеродюыщжрпроппрчикммьлевлщднхбмнхшсзмгьхпэсреж
аолфдыууофнрйнцусюазблэчшрщзщжацчтыкйкаешхакмхйтвжшусййушфиюдюдаюгпш

гцчтыкйкающамджйазаддхухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмеза
хехщяпвсхйюдаюыущаидвцюдаюьичбзлцчтыкйэщыштыаччбзстдаюышхехаедюшзщрп
щысагшлайеошцкнуфносачзюидцецчхйхажатечшжьйацчтыкйдшрщзщашчоыйыуйаусй
рпнюлтевйвпрпгечпщачшкдььрмегфчпрбелшцающашчопаюебушщькышзшвыйафщыш
хпцмдрщыыуюехакчщуиезафнщыаччбзстдаюрщлаеебдкйлщйачнрйюблэчшшхнфрпющ
эплщцчсдфмчзьчжлаыпмяызшжхбмнхшсбужичлщерпюабуашькщыдщвйрмыулпбьйашд
тыцмюарпхвцчьрдщгшашчоламчэичаэхшстдаюриэщйазнзсзшйшлшюагпчиеысагшлайе
зщайхлбшглэщйщчшчамеешвдбювсрэжичбзлэпрешхнфрплацсрчцпхюшрфчсимэоскгфу
ыйыхффэплщгарпсенуказарчыупмхуэсдммэтдяавдчишхтаичшзыйыуйаусйрпнушхакмю
бпмншжлэщйщчшэирщлэгерпюабуосйещеэдсечушгцмпнщьбукаюдуыдщимюдкечушгм
щрщашщппрэщкырйдщьлщеющвпьюриюдюашдйржахетсййвпэсгпчинаькгшхпннзщцц
твкчисжлзсйепртшййыуйаусйрпншдажйазмгьусффщлщрбезахемчтэлекмаюрщудеапамд
осшсцпфжнлзуыщюазреызшэатдрмхпщьбудшщыхубвчочпщаэщялчохехалюидвиаммсее
апегкажлхехдпрчиилмечшшшцкдщтечшчызшэатдрмлэчлрщнаэшэдкйчбйкишугрййкоы
дднпрщышлсбубеаунккмнежскгцчтыкйкавйыуйаусйрпносфнзвюаиейркезаокйщгаынрй
щызюимюдаюаыпмяызшцлгпшгцчтыкйкаяхбмщырйнхкелиачгшшдсдмэшсрмфукукчщг
чилиачгшзсечмбрмфуэснарпзючшпмвпфчбшмейрпныурщгпзхцмчэиорщэаэшшщрщхез
акдььрмьрпнхщшдькюедефщроошкаюрпркдчэуырщлхчээпмеидбюхахщимюдюарппьщс
рплаэщкаюытэтедщпуэщвкющиулаэиыйхлллнажахоусиппрсеэщюхыййаькэиеыйееуйаф
мыущфзщжбглщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйнхюахйщфр
пешбероюарущефпкезарчцптддчщфдщпуэщвкющньйашегахлтейицмрйыезаокнейежпэ
иэщгэхувлуоыуыщимфмйщпшйрщьйапахпьююаяофэхувлуолиачйахагаодвимдчитысаз
шйыжжйажлчпнхыезахаэасачшашйарокамейецыьпяйхеейыуйаусйрнфйщхлюеерффасх
йюдкемдсилэгерпйклижуашрщщейечшвппршгцчтыкйканущефптачштэрщзщяпэптбьер
пимюдкеслщещцримежагекаюрэпьчяфьеруюсхпымздюлщелшашфьымосьрчифшцкщед
еюакайасажлнктешщэилиачгшопьчффкммьофпаюечэрщошбеюеюылшищгаясбрмэтдюа
дуклзщачисюарехеэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпри
дчьнрифусицлщеомхпипчушгмщрщашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейу
юфшроошэщнхльюаэпеямшщевлэияффубелшщфцчтыкйхрмсуювпьюыщдшварчмэчиа
щварщэщйщчшэийщхатешщчшбущефпсдюдисфуидчиеапячщ

Відкритий текст:
однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопреде
ленноеприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодляж
изниприводящегоктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедостигатьта
койсилыослабляясьдократкихсостоянийабсансадобыстропроходящихголовокруженийи
могуттакжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприродепо
ступкикакбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэт
ониказалосьчистотелеснымипричинамиэтисостояниямогутпервоначальновозникатьпоп
ричинамчистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимостиотдушевн
ыхволненийкакнихарактернодляогромногобольшинстваслучаевинтеллектуальноеснижe
ниеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуа
льнойдеятельностигельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамо
ененадежныилиподлежатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпи
лепсиеймогутпроизводитьвпечатлениетупостинедоразвитоститаккакэтаболезньчастосо
пряженасярковыраженнымидиотизмомикрупнейшимимозговымидефектаминеявляяськ
онечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимиви
доизмененияхмибываютиудругихлицулицсполнымдушевнымразвитиемискореесосверхо
бычнаявбольшинствеслучаевнедостаточноуправляемойимиаффективностьюнеудивител
ьночтопритакихобстоятельствахневозможноустановитьсовокупностьклиническоюаффе

ктаэпилепсииточтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимому
функционального пониманиякакеслибымеханизманормальноговысвобожденияпервичн
ыхпозывовбылподготовленорганическимеханизмкоторыйиспользуетсяприналичииивесь
маразныхусловийкакпринарушениимозговойдеятельностипритяжкомзаболеванииткане
йилитоксическомзаболеваниитакипринедостаточномконтроледушевнойэкономиикризи
сномфункционированииидушевнойэнергиизаэтимразделениемнадвавидамычувствуемнд
ентичностьмеханизмалежащеговосновевысвобожденияпервичныхпозывовэтотмеханиз
мнедалекиотсексуальныхпроцессовпорождаемыхвсвоейосноветоксическиужедревнейш
иеврачиназываликоитусмалойэпилепсиейивиделивполовомактесмягчениеиадаптациюв
ысвобожденияэпилептическогоотводараздраженияэпилептическаяреакциякаковымимен
емможноназватьвсеэтовместевзятоенесомненнотакжепоступаетивраспоряжениеневроза
сущностькотороговтомчтобыликвидироватьсоматическимассыраздраженияскоторымин
еврознеможетсправитьсяпсихическиэпилептическийприпадокстановитсятакимобразом
симптомомистериииеюадаптируетсяивидоизменяетсяподобнотомукакэтопроисходитпр
инормальномтечениисексуальногопроцессатакимобразоммысполнымправомразличаем
органическуюиаффективнуюэпилепсиюпрактическоезначениеэтогоследующеестрадаю
щийпервойпораженболезньюмозгастрадающийвторойневротиквпервомслучаедушевная
жизньподверженанарушениюизвневовторомслучаенарушениеявляетсявыражениемсамо
йдушевнойжизнивесьмавероятночтоэпилепсиядостоевскогоотносится ковторомувидуто
чнодоказатьэтонельзятаккаквтакомслучаенужнобылобывключитьвцелокупностьегодуш
евнойжизниначалоприпадковипоследующиевидоизмененияэтихприпадковадляэтогоуна
снедостаточноданныхописаниясамихприпадковничегонедаютсведенияосоотношенияхм
ездуприпадкамиипереживанияминеполныичастопротиворечивывсеговероятнеепредпо
ложениечтоприпадкиначалисьудостоевскогоужевдетствечтоонивначалехарактеризовали
сьболееслабымисимптомамиитолькопослепотрясшегоегопереживаниянавосемнадцатом
годужизниубийстваотцапринялиформуэпилепсиибылобывесьмауместноеслибыоправда
лосьточтоониполностьюпрекратилисьвовремяотбыванияимкаторгивсибириноэтомупро
тиворечатдругиеуказанияочевиднаясвязьмеждуотцеубийствомвбратьяхкарамазовыхису
дьбойотцадостоевскогобросиласьвглазанеодномубиографудостоевскогоипослужилаиму
казаниемнаизвестноесовременноепсихологическоенаправлениепсихоанализтаккакподр
азумеваетсяименноонсклоненвидетьвэтомсобытиитягчайшуютравмуивреакциидостоев
скогонаэтоключевойпунктегоневрозаеслияначнуобосновыватьэтуустановкупсихоанали
тическиопасаюсьчтоокажусьнепонятнымдлявсехтехкомунезнакомыучениеивыражения
психоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслпервыхприпадковдо
стоевскоговегоюношескиегодызадолгодопоявленияэпилепсииуэтихприпадковбылоподо
биесмертиониназывалисьстрахомсмертиивыражалисьвсостоянииилетаргическогоснаэта
болезньнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезотчетнаяпода
вленностьчувствокаконпозжерассказывалсвоемудругусоловьевутакоекакбудтобыемупре
дстоялосейчасжеумеретьивсамомделенаступалосостояниесовершенноподобноедействи
тельнойсмертиегобратандрейрассказывалчтофедоружевмолодыегодыпередтемказасну
тьоставлялзаписькичтобоитсяночьюзаснутьсмертоподобнымсномипроситпоэтомучтобы
егопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениеснамизвестнысмыс
линамерениетакихприпадковсмертиониозначаютотождествлениесумершимчеловекомко
торыйдействительноумерилисчеловекомживымещенокоторомумыжелаемсмертивторой
случайболеезначителенприпадоквуказанномслучаеравноцененнаказаниюмыпожелалис
мертидругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеучен
иеутверждаетчтоэтотдругойдлямальчикаобычноотециименуемыйистериейприпадокявл
яетсятакимобразомсамонаказаниемзапожеланиесмертиненавистномуотцуа

Під час виконання лаб. роботи виникли труднощі з опрацюванням наданих тестових даних: їх не вдалося розшифрувати, але після невеликого дослідження було з’ясовано що в кожному з файлів вірогідності найчастіших біграм є однаковими, а тому - скоріш за все тексти є беззмістовними, але без заборонених біграм. Вдалося розшифрувати тестовий текст для V6.

Висновки

У ході виконання комп’ютерного практикуму ми набули навичок роботи із шифром афінної підстановки біграм. Навчилися як робити атаку на афінний шифр та як робити автоматичні розпізнавачі змістовного тексту за різними критеріями (найчастіші літери, рідкі літери, заборонені біграми та ін.). Запрограмували розширений алгоритм евкліда та на основі нього зробили функцію для вирішення лінійних конгруенцій. Було запропоновано алгоритм перебору ключа без вирішення лінійних конгруенцій, який на нашу думку є досить ефективним і простим.