

Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

## КРИПТОГРАФІЯ

### КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:  
ФБ-33 Самохвалов Роман  
ФБ-33 Лозенко Павло

Київ

2025

## Мета роботи:

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

## Хід роботи:

1. Реалізація програм із необхідними математичними операціями:

Обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда:

```
def extended_gcd(a: int, b: int) -> Tuple[int, int, int]:
    if a == 0:
        return b, 0, 1
    g, x1, y1 = AffineBigramSolver.extended_gcd(b % a, a)
    x = y1 - (b // a) * x1
    y = x1
    return g, x, y

def mod_inverse(self, a: int, m: int) -> Optional[int]:
    g, x, _ = self.extended_gcd(a, m)
    if g != 1:
        return None
    return x % m
```

Розв'язуванням лінійних порівнянь:

```
def _solve_for_a_candidates(self, x1: int, x2: int, y1: int, y2: int) -> List[int]:
    A = (x1 - x2) % self.M_SQUARED
    B = (y1 - y2) % self.M_SQUARED

    g = math.gcd(A, self.M_SQUARED)

    if B % g != 0:
        return []

    A_reduced = A // g
    B_reduced = B // g
    M_reduced = self.M_SQUARED // g

    inv_reduced = self.mod_inverse(A_reduced, M_reduced)
    if inv_reduced is None:
        return []

    a0 = (B_reduced * inv_reduced) % M_reduced

    return [(a0 + k * M_reduced) % self.M_SQUARED for k in range(g)]
```

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом 11).

```
def get_top_bigrams(self, text: str, n: int = 5) -> List[str]:
    bigram_counts = Counter()
    for i in range(0, len(text) - 1, 2):
        if text[i] in self._letter_to_num and text[i + 1] in self._letter_to_num:
            bigram_counts[text[i:i + 2]] += 1

    return [bg for bg, _ in bigram_counts.most_common(n)]
```

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).

```
def find_key_candidates(self, cipher_top: List[str], lang_top: List[str]) -> List[Tuple[int, int]]:
    candidates = set()

    for i in range(len(cipher_top)):
        for j in range(len(cipher_top)):
            if i == j: continue

            for p in range(len(lang_top)):
                for q in range(len(lang_top)):
                    if p == q: continue

                    y1 = self.bigram_to_num(cipher_top[i])
                    y2 = self.bigram_to_num(cipher_top[j])
                    x1 = self.bigram_to_num(lang_top[p])
                    x2 = self.bigram_to_num(lang_top[q])

                    a_list = self._solve_for_a_candidates(x1, x2, y1, y2)

                    for a in a_list:
                        if math.gcd(a, self.M_SQUARED) != 1:
                            continue

                        b = (y1 - a * x1) % self.M_SQUARED
                        candidates.add((a, b))

    return sorted(list(candidates))
```

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

```
def decrypt(self, ciphertext: str, a: int, b: int) -> Optional[str]:
    a_inv = self.mod_inverse(a, self.M_SQUARED)
    if a_inv is None:
        return None

    plaintext_bigrams = []

    for i in range(0, len(ciphertext) - 1, 2):
        bg = ciphertext[i:i + 2]

        if bg[0] not in self._letter_to_num or bg[1] not in self._letter_to_num:
            continue

        y = self.bigram_to_num(bg)
        x = (a_inv * (y - b)) % self.M_SQUARED

        plaintext_bigrams.append(self.num_to_bigram(x))

    return "".join(plaintext_bigrams)
```

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

Результат виконання коду:

```
Криптоаналіз Афінного Шифру (Біграми)
Довжина тексту = 7674
Топ-5 біграм шифротексту: ['нк', 'кж', 'хб', 'шь', 'мк']
Знайдено ключів-кандидатів = 220
Кандидат №1: a=703, b=956, IC=0.055538
Розшифрування: хорошосэрбилнхотясунулденьгивкарманвотчтобилвып...
Кількість валідних: 1
Результати збережено у файлі 'decrypted_result_lab.txt'
```

Наданий за варіантом шифртекст:

оквкпкящсройюфчвбчллфэйлзщойифуххгйжфбчбжройэжиавкхбоаэлбзьдблфюжвпыхожеуфыхьфисццоисццикшгтчьюбрйэунемкщхл  
фэсццикоэйсыфляэсблавххуоаебвщцззабюжэйзэсюфцхцъдвкьбивцкьхбвхщзфийамсьэхьжофшнйсбжежоэзхбнннхдхбххьюэкублфй  
щзхкгсебэуяфдзэсццоэзкххыфиамсътццугтбйрипйпуптшьюуйукьлкуеафбгфмсмешзчеюцнпфиздбюакличьюльчяюеьххущафюе  
шзхксищфнлазъфююшлайпзгзхбфйсбцрптозкендэнлбкнкшчююжбйдрптцъдьжыяжчэщлакэзйфбюыхожобьэгроюфееыхцыеимкжфлйут  
дяйиаютэффйабгнйакбхейкжцлньфьюдфбгышллаяфеяфэьжцазпзфизжнлмккцниулбргзхбтшяюйцуфьюпзмкабвхщугтбйлзтцсуязя  
фыюедьяамсчежоакютэффцшжядбоапздлчъпдкьуавкййлцыхяфнлвцаинарилзщомксйуккзхьлзтцсуямсчеылууезкзоуфьюоайнтббйцил  
бвзщъцупзоулцафэйакиоскзшавкафэйоендхкыхзннложшущьмйжбйоеахуиюиаезездлрйозвфьюяжсблзтцсубйчэйфувккьбиыжмхбыот  
мхфыхцылкцьбмуксяфэлойэлтапзсфбззфйуэздзозцъндкьдядзюцнэпфизбюшнцкшугтбйяфюбфбшуэлтбыхожлфюжйисзсбрийэуэлсымсчебб  
вкслаклийияфшлаэлкцъльсйуяфжнбкдбьэзэипуэлойчышзкфяфичнкяилкзтцсужоыомехцэжшубкмьцфэйхьазцодбжройэщщройвмехщл  
ьзйжчячбэлрийичицхьхикрырийоужктуэлтбичццшубгыфхцщбщъцзрипймкжфлийкхкзцъхэлнктцфлцждефэйоемазьялвбйцакжтшьдфшул  
эсбоебвквещэкеьюфукззцонихбмсйснгчъфшйсржджабляэфббозеиылшжохюжебиисйпчфзикозывмсойцждауярипйшкпзхбхшлюг  
еыбйщуэлойактфнльжвхшткхбшущьщфйуяфочшьцъдъсиртмкауэлойуиаезехкрилснгльюджтнийфьюшкябпфщжэлохщлыфизбвкейук  
ыцйяпфлхмсоймкяждзацаьщьюцсйюжбкьэксюеочбшуйудзфисццомкгзбжинкчавктххуилкхкнккуийиаьжнсдмуфпсамсхьюозбичьюхзнтб  
швфьлшзчебкфичбяфламсьхьюыжбйяфзннкзоьхэлойэлвжшьсхкчъськшьюкцшьндждодбьсгфнлсьхбсетцъгпйуклцзнкшьюкцшьуя  
фшебблшжчъяпфзийияфэсрйсфебгрчляфяфэлтбвжчъяпфукжфнезфжпфжвхюкшугтбйяфшлцкохьюкцшьнджоахадйукмкхбожойш  
ыазилеьпрпфцехпцзткмущьщьюжхейлхккььомажрпзэжюкейэфзкэтеьимехцэжнкчююьюсийюжххшбжсюжрийгфнлмкактфожщлнйюжтхб  
еххзъзктклдлазмзбишлицьсьбоемкфждзацшлзильхгтүябоквкпкйцпаюгбкийищъцпзббйххптебьктширтыгднвйгтавкниееьяозшл

ыщнкфшвхгтмкбькцрлеыгзтлвхкффэйсйюжххцтйуйувздбфыпзвизсрйцзычнйюсыьэхжжомкчюдьхксуяфзйоуфукфжсбщулэтбрийэумсыйи  
озэрийегдяозфиззикошьюкюдчбъыфйсюжрийгфпфшлмкакфпфьжшлнйиозшжэлнкаыйсюжрийгфарчжжпупехюжищжэлнкаыйдяныльч  
жспфшлсьхбсдщлехиуианктдиццзкабйыжлзулфжэлчьньишхцпфнлзлбфыйннкаезньпытжксягэуйушжшлнйэлшвлэуфыхьщупзсцд  
бсхйюжэфэйукефяебнйфоафымелзюфлэыфцийидксыоавкчлфихкроудьхожбйэфчязэнисдеьактфххмсфиакюспфзнсыйафшлэйдсйпблкцз  
эроблячжхазслеижшнникыцаклсюжпфбкикохбыиццкшлдящухенеткшлыфчэбйвпроцьохзбйбйэфюенкозьхшвьеуьзкчксйюжххдхэф  
сюжожегжцлфсепдщйукюдазцоозпашьгикьюгтайндялвхшчицьзуюхбхнтбознкооакжфдябкэфйнщпозеьлкциюодпавклижочбфйудзлх  
йуюбюшнкзфзфхптэсозжсюткхэлуюжшлжозеуинйссыжезешьюкзфебэуйулыхдзсгхчьюбшуйуезхьчъзшнкьтцгсьбооеьякоюдьхьсбх  
бщьщзчиыжчидунйдрттэсвзовулайфбзяхнндьяахипазнойоаяфпбэуйулфсыюжикыйдаялфцждщэкеьщбюгтаююпаксьгиищзпзхбпфбллк  
ыхсбгфяыфпбйуеятыньцяисцыбюжщзйжьющжжксягфйэфьяпмгыжмхбыцьшзыйафбщфэйпфэлзяткфсэвткэрийсаяшлсбчжэфюжебаяфх  
хкхцньежвхшцтцокфуклбшсяюжбйодслсьхбизкннлжосыехшлфхюжэлщйцухцньафьиьтошнниккннлжояцялнкэрлчкхислшжщзйжь  
ющьбтарийкхьыжщзйжьющьбтэскшчбейфбшьзэфсцтвцикоошшжзхбьвзгфьякюсэбьящьюлкейлйукуцияяпфыццэлгзхавкхбкйцхьвф  
бмеэыывкьпущинийюжунлсьвбказфидялзцоцжфдящжттцзыеушшоочьщбфцщуеясббйньлзпзкьлхкнккьюткфсгхюювгфзкфжвхпума  
ехбюгзюьпмгышьвькюдкхкфбсьщфвзфкзлuyeыйлалцийиьтжезюсрщлмкакфьюшлсьхьшзэфцяфотмхеыыжбйфкэкьнникыльнтлжд  
зырлзнкисбйхужнююнкиячвхьылкцгикылууцьфькьбсбтктдхьлгыыхыжбйоечбюжмтчжфзвцлзьяцждуюкжнвхчяфкшамспьикылууд  
цуфбюагпапишьязщьсцакикфисцорткбезлрлцзьчуйухбхцуюжпазьяфжепавкййдэтбрийфцщбэртфимахичьясаяоттдазезооскэи  
мйлюенквффыфвхбйанктдсжкстбчбфбдядъжщьцщувзлжидщэывейыфдичбдзикхбщьзыискычьньроьхожойгфбюмкюквххзюлкк  
кабехцзхбтккнашупфьжоксикгежешлткиыхлэюснйчэбйеавхфжюзэфхбцшзбидиозмснгжзйфдэлзпткнкюсфзикрилптэйнпчюжбклощ  
хщнозхкмаобюерортнджоикпзтоозшсщнфкзльэщлнкзфидящьвгдхикыйиакхкбииннлбияждзьясгфцлхкфюшнкндийиэгидквкхбсдлавкб  
иьфцуэфйуяфочакябсхсягэфшфщнбйияхьлюжчжеблеиззпзфщлпбрсоиюибкззасвкбьфбйлеьххкбиипьяэлзйфьюмккцшзбгдккльрийм  
себйубюгдкшгяюмайнвхозэгюанквфюжозикшсххойчарйфилйукуцияяпфабтунюеромклхнийисязлзбиюлехойлюифыкцгийзообкохзбйк  
црфэсцаабькхьжжксукичебфбсьмцлкчуйичьпршснкхжройсйиндэннлыжакуфебкжбгньпгыиявхжогьгишкннлжопыфбюжяавэкхманйг  
зоьпмгыйукуцияяпфмкглзюфяапбшьчебзмлфнкшлчьчьньсыьэыфзххццзежыфйснйэфвхгтиккхикыльэлткяякссбляфкфипьяиозяжнеия  
фбхиэьяфксвхббоесыьыфебэщлчяпфшлткчллыхтбукшьмкнкыльзньшвлзоежонцябюжэщзьюююмкшыюкуеулщфюжюзжйебсехьякозв  
фзясгфеыфбюжяьхбйеяцлсьхбйиазхунцшлзсбгжрвкроудгьхвхтбвщбисьидьфшвозмйптсбфимсшьфцфцсущннийюхулфларйэыфэл  
южебблшжеуийснйеылмктцэкэцдбьяфожвхбкозмкхйстбожфбгзюьпмгыхцмсэфбхйсэфцуйубюмкоопдщлийеьпршссбхмсрийбьжооефшч  
вфбгфйснймяюзикмкоковфитжсыэлжрхбазйфбюгьгиозбкдбшвсйюжзюьпмгыхццзозсыгбйяфлиуцейфывзсллкхйнчыфпфсыюжбйтоем  
кнкхкжзфбеьквгвцьмктцгьхххццзгзбшьмккцбквцьзикжртхкхщйеблябияфйлждзьубрийэушуйубюбфбхиясавкохзбйчбфбфяфнлззюясгэф  
цлсьхбсешьмхбьдзббвкйскыщьщутдрыньцяфкжкснйкбпчяфмавкблиийиросжттцызнквфехгтбклжсбсдхучяюгуилхбгыфсдьжозмкхбшэе  
ияньлюдшххнюойсыяфэуттйеифжкоайлчйирошьцзхбщфвпохьгьыххлэнлжрийуыжезткпяэсджаехмсбиокцоакыхшущьодкыйируткежех  
маюжртыиькнтьеомедкыйирыххлззфжвхзйбнннгуежйсьжйнуиэфшлакооакынафмкшзчйойэфсехьэзмкнкуфвхюгтбнйфоамсбгйи  
мкцйшэзиезьебкжийиромкежачгяизгоьпмгышахисйнгбйоемаяфлйчбюжзззбихжезруоацткжехикхиясгфцлсьхбсеьякдяьбкндхкнд  
йлждзьжогзхфеяжфдяткшхузвфичьактфдршсвжнийцупфигдбжркийехгтбкикхкчкзэзбщьюжцлшудзэфртаксбехюжбксбоапзджихбдзчь  
хкроетьжщпулахдзлцкхзясдптрйфблюдлаззждазийинибкрлсьсущихбшедьщбщуттйнсдгрфпхьпьязйичьлгыцюкмийсбткпзйфзяхждзүүлр  
ламсбкпашлыффийидклфбзнквфехттюжоекцшькарийбккцфийьжфбткнкшьюзрпбшьюйугнкмкхаждазпужевхвьялмкакффымеозфжмстк  
кфыцждфьэшшвоечкфйфцрнийжртидиябйинняхуьлйсфвххцуюжмкхбюьзчьцхзаякщуттбйгзнеазцоезикжфятзозфупсьжясгфйлыцы  
лыцнамсчеуырийюжкьябэщлнкльфрткжмсткпзпэйдбзфупниубфэщлчямкиннлптгэсазгэжюзщьякцхсбиэльдсюечкшлдяцяндмефшс  
брийакуфлавкафэйоефкбгежюфбуихцылщфяамснфцийишьхэщлньдятожыхйуфкхбпфюжойнлпцшувьизсшжфизфеыххлэмксйнгсюгзя  
фсывкнүэлчьньняфзсйыщегьгишыьжхожтценьчуйуиодиктххиолкцзэробькшьюябзыхьебрссбюючьяэсбяфяапзбхебтблельхичьяфю  
жождфбгцифшдяэбкщцнкьясгэфцлюжезшщлсьхбизслхпбейблскулшзабьльхпбейблшжфбюдщэкеьюблгрщфчэбйбзиоожакычхуяфд  
кьфэсехазиооемазпзичобненккюсршсшснйебвжгузщцшкэррийегбютшцульеьхцкннлзийжбювзтзшүлэюаозгйинкклфнльщзьюцэизфбл  
чязффзичьфцшьаийссбоеюктжездобщйамсфигьсссбююактяпшвцьрьбьякнумкхкжиозлзийенкикьяфцуфылццзозбисхкжбпромсшч  
кхбгхаккжжфнликнкфубюэфэлуинбоабшбъыфэскифыихемсмкхкжюжньфуылкзьяжьолвхгрвкмкнихтбсещьжжчэбйвпропбрийэуяфазяэ  
фжпзкзчьжйссбоешьесязгшуйухэыжббйуткнкфжсбляозчьжезедлцшзхтбюерткмкясгэфкшыйлыхдзшькшлдяэфцшнукззщобьоозфщн  
тбуфыфхуфыхьсцлзгслэаллкыхсбэуйуяфцхбкыфбйэфясчнйюжбйфзизкушхуцгидйибузашьюдзкыйчэбймахапвикуыльшжсбхвхфртш  
сяфэлойцпхьчьдьяясгэфдибьпзсдрусьебкеннкхмспулскезодфцийиыяххшэйуфбехфыцкйфцфыхьхоэжилзжячэтццтквкцзйфбьялж  
рийучаиигьоонисучьяфьжксеяквавкшурйцтхцньаксуьицацыитубйыцежвхююаьщьбьыьтхьхлэнлждзьылыгехьвафчэбккзхкваыфбывхбк  
йсфвфизьхдрнешсбйхушвхьгуиюрвхсыюжцьрбщыдылэдеьягьихцтцгпийукуцияяпфшльжшзбукшавкафэйоемкфсбкбтооннкнксыехг  
тсцсикхьгзакисцикмузашьэюбфбоаньчылыцщнкюдзэффэйгоьпмгыжикйптпюертохожебиимкэзчүидцгьооиниуьехэухжсбйбифкж  
гирокамснфцозхфсбшлиймачжбйяфшлхуяфззбакануьфэлыцубгрлаихафойэлннкфисццохщьчфдзщьюлчэиуфшлшфшубкьгооиниюрэ  
уттбйыжбйоесйптчаиивцулксжозикшьюхожубебйукуцияяпфпупптшьайндякжюмехцэжшубкежвхтхьхлэьрцйгхндьцфббшфнльзвояф  
мкоцшлфжюжбйчъжрйэлецозикшлеьийодэкнуфыхьпэьбиокцоакшлиймачжоешьякозатцркийоекзпашубюдслбклкьклбцхбойоемкгх  
бфисзмкюкэзчуаьщьюцртебьиисфвпфвэлнквксфюжощфэйцццяь

Отриманий дешифрований текст та ключ:

№1 Ключ: a=703, b=956 IC=0.055538

хорошо сэрбиллнехотясунулденьгивкарманвотчтобиллвыпросто посее тэуновуютраву когданибудьвдругойраз как толька помруна друго  
йже день может перекопать эучертову лужайку ну как хватиту востерпения подождать еще лет пять шесть чтобы старый болтун успел от дать кон  
цы уж будте уверены подожду сказал биллсамнезнаю как вамобяснитьно дляменя жужжаньеэтой косилкисамая прекрасная мелодияна свете  
внеи вся прелесть летабезнеебыужаснотосковали беззапахасвежескошенной травы то же билл нагнулся и поднял с земли корзинку а пошел ков  
рагу выславный юноша и все понимаете я уверенизвасполучится блестящий умный репортерсказал дедушка помогая ему поднять корзинку а в  
амэто предсказываю прошлоутро на ступил полдень послеобеда дедушка поднял сяк себе немного почитал уиттиера и крепко уснул когда он про  
снулся былотри часа вон навливал ся яркий и веселый солнечный свет дедушка лежал в кровати и в другвздрыгнул служайки доносилось прежнее  
знакомое незабываемое жужжанье что то сказал он кто то косит траву но ведьеет только сегодня утром скосил онеще не послушал да конечно то ж  
ужжит косилка мерно не утомимодедушка выглянул в окно а ихнул да ведьэто биллэй билл форестервам что солнце ударило голову вы коситеуж  
ескошенную траву билл поднял голову просто душно улыбнулся и помахал рукой знаюнокажется утромярабotal не очень чисто дедушка еше до б  
рых пять минут нежил ся в кровати и лица его не сходила улыбка а билл форестер все шагал косилкой на север на восток на юг и наконец на запади  
зподкосил кивеселобилл душистый зеленый фонтан ввоскресенье утром леоауфман бродил по своему гаражу словно ожидая что какою нибудь по  
леновиток проволочимолотили гаечный ключ подпрыгнет и закричитначни сменяя ноничто не подпрыгивало ничто не просилось вначало как  
ая она должна быть эта машина счастья думал лео может она должна умещаться в кармане или она должна неба самогоносить в кармане одна зна  
ют вердосказал он вслух она должна быть яркой лео поставил на верстак банку оранжевой краски взял словарь и побрел в дом ли она заглянул в то  
лковый словарь ты довольна спокойна весела восторгетебе во всем везет и все удается потвоему все идет разумно хорошо и успешно и на перест  
а ларезать овощи и закрываглаза прочитай мне все этоеще раз пожалуй сталое захлопнул словарь за какие это грехи должен целый часждать пок  
аты придумаешь мне ответскажи только да или нет больше мне ничего не надоты что же недовольна неспокойна не весела и не восторгедовольн  
ы бывают коровы в восторге младенцы да не несчастны старики которыеужевпалив детствосказали на ну а насчет того что веселасам видишь ка  
к веселосмеюся когда скребуэтраковину лео внимательнопоглядел на жену илицо его прояснилось ты права ли намужчины такой народни ког  
даничего не смыслят может быть мы вырвем ся из этого заколдованного кругаужесовсем скорая во все не жалуюсь закричала ли она не прихожу  
к тебе сословаре мине говорю вы сунь язык леотыведь неспрашиваешь почему сердце у тебя стучит нетолько днем но и ночью она может бытиспр  
осить что такое брак что это значит не задавай вопросов все же таки елюди все имна дознавать как устроено миркак то как седа как это задумается такой  
и падает трапеция и циркели бозадохнется потомучто ему при спичило понять как у него горлемускулы работают ешь пей спи дыши и перестань  
смотреть на меня такими глазами будтов первый раз видишь ли наауфман в другзамерла потянула носом воздух втбеда авсетывиноватонарван  
уладверцудуховки оттуда повалил дым счастье счастье горестно воскликнула она изза этого счастье мы стобой соррорим ся в первый разза пол года и  
в первый разза двадцать лет наужинбудутуголья вместо хлеба когдадым рассеялся лео ауфманауже ислед простыл грехотлязгсхватка человека с  
вдохновением день за днем ввоздухетакимелькают куски металла деравамолотокгвоздейрешина отверткипорой лео ауфманаохватывало от  
чаяниеи он скитался по улицам всегда беспокойный всегда на чеку он вдрагивали оборачивался слышавгде то далекое чей то смех прислушив  
ал ся к бавамдетворы присматривал ся чотызывает дудей улыбку в черамиион подсаживал ся к шумной компании на веранде когонибудь из  
соседей слушал как старики вспоминают прошлое и толкую то жизнь и при каж дом взрыве веселья оживлялся точно генерал который видит что те  
мны е вражеские силы разгромлены и что его стратегия оказалась правильной подорогедомой он торжествовал пока не вошло пятывсвой гара  
жгде лежали мертвые инструменты и не одушевленное дерево тогда его сияюще елицо вномрачнело и пытаясь избыть горечь не удачии со же  
сточением расшвыривали колотилчастисвоей машины словно тобыли живые ея ростные противники на конец контуры машины начали вырисо  
вываться и через десять днейинойчедрожа отусталости измощенный полумертвый от голода такой высохший и почерневший точновнего удар  
ила молния лео ауфман спотыкаясь побрел в дом детиссорились и оглушительнокричали другна друга но привидеот что тасумолкли как будто  
пробилурочный час и в комнату вошла сама смерть машина счастья готова прохрипел лео ауфман лео ауфман похудел на пятнадцать фунтов сказа  
ла его жена он уже две недели не разговаривал с со своимидетьми он и сам не своя смотрите они дерут ся его жена то же сам не своя смотрите она п  
отолстела на десять фунтовтеперь ей понадобятся новые платья да конечно машина готова а стали мы счастливейе кто скажет лео обросты мастера  
ты эти часы в них не лезет ни одна кушак человекуне положено соваться в такие дела господубогу этона верно не повредитавот лео ауфмануоди  
н вредни какой пользы еслита кбудет продолжатьсяеще шесть недельюмиего похороним в его собственной машиненэтих слов лео ауфманужен  
если шалон сизумлением смотрел как она не гавалит ся потолок вotta кштука подумал он жележана полнотутего обволочать маи он услышал то  
лько как ктототрижды прокричал что она счастливача на другоеутрое двараскры вглаза онувидел птици и проносились ввоздухеточно  
разноцветные камешки брошенные в не постижимойчистойручей лигонькозвякнув опускались на жестяную крышу гаража сабаки в севозможн  
ых породтихонько прокрадывались в довори повизгивая заглядывая в гараж четверомальчишек две девочки и несколько мужчин помедлили  
на дорожке потом нерешительно подошли поближе иостановились подвизниами лео ауфман прислушал ся и понял что влечет их все их немудов  
орголос машины счастья такое можнобыло бы услышатьлетним днемвозле кухни какою нибудь великаншиэтобыл разноеголосеужжанье вы  
сокое и низкое торовно ето прерывистоеказалось тамвьются ряеомогромные золотистые пчелы величиной с шакуи стряплют сказочные блюда с  
ама великанша удовлетворенномурлычетсебе под нос песенку илицо у нее точно розовая луна вполнолуние вот вот она не обятная клето подпл  
ы веткдверямиспокойно глянет в дворна улыбающихся собакна белобрсых мальчишекиседых стариков постойте а громкосказал лео аведь с  
его дняеще не включал машину саул саул поднял голову он то же стоял внизу в доворесаулы еевключил ты же сам полчаса на задвелем не разогре  
тые еахдая совсем забылаеще толком не проснулсяи она опятьоткинулася на подушку ли на прине слаемузавтра киостановилась у окна глядя внизна  
гараж послушай лео не громкосказала она если эта машина и вправдутакая как ты говоришь может быть она умеет рожать детей а может она превр  
атить старика сновавоношу иеще может вэтой машинесовсемее счастье спрятаться от смерти спрятаться вот ты работаешь себя не жалеешь в  
конце концовна дорвешься и помрешь что тогда будуделать влезутот большой ящик истану счастливой иеще скажи мне лео что на степерь за  
жизнь сама знаешь какунаведется домвсемутрая поднимает детей кормит ихзавтракомкполовине девятого в асники гоуженетия о стаюсодна  
состиркой одна с готовкойи носкиштопать то же на дои огородполотить влавкусбегатисеребро почистить яразве жалуюсь только напоминаю те

бекакведетсянашдомлеокажживутаквотответьмнекаквсеэтоуместитсявтвоюмашинуонаустроенасовсеминачеоченьжальзначитмнекогдабудетдажепосмотретькаконаустроеналинапоцеловалаеговщекуивышлаизкомнатыаонлежалипринюхивалсяветерснизудоносилсюдазапахмашиныижареныхкаштановчтопродаютсяосеньюнаулицахпарижакоторогоонникогданевиделмеждузавороженнымисобакамиималъчишкаминевидимкойпроскользнулакошкаизамурлыкалаудверейгаражааиззагаражаслышалсяшорохснежнобелойпенымерноедыханьепробояудалекихдалекихбереговзавтрамыиспытаетмашинудумаллеоауфманвсевместеонпроснулсяпоздноночьючтотоегоразбудилодалековдругойкомнатектотоплакалсаулэтотышепнуллеоауфманвылезаяизкроватипошелксынумальчикгорькорыдалуткнувшисьвподушкунетнетвсхлипывалонвсеоконченоконченокосаултебеприсиносътонибудьстрашноерасскажимнесынокномальчиктолькозаливалслезамиитутсидяунегонакроватилеоауфмансамнезнаяпочемувыглянулвокнодверигаражабылираспахнутынастежьонпочувствовалкакволосыунеговсталидыбомкогдасаултихоньковсхлипываянаконецзабылсябеспокойнымсномотецспустилсяполестницеподошелкгаражуизатаивдыханиеосторожновытянулрукуаа

## **Висновки:**

У процесі виконання роботи успішно реалізовано криптоаналіз афінного біграмного шифру шляхом поєднання математичних і статистичних методів. Застосування розширеного алгоритму Евкліда дозволило ефективно знайти обернені елементи та розв'язати лінійні порівняння, необхідні для підбору ключів. Через частотний аналіз біграм було сформовано множину ключів-кандидатів  $(a, b)$ , а лінгвістична фільтрація за індексом збігу (IC) забезпечила автоматичне відсіювання некоректних результатів і підтвердила високу ефективність інтегрованого підходу.