

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', 'юж', 'хб', 'шъ', 'мк']
Знайдено ключів-кандидатів = 220
Кандидат №1: a=703, b=956, IC=0.055538
Розшифрування: хорошо сэр билл не хотят сунул денъ гив карман в отчобилл вып...
Кількість валідних: 1
Результати збережено у файлі 'decrypted_result_lab.txt'
```

Наданий за варіантом шифртекст:

оквкпкяцшройюфчвбкллфэйлзшынифуххгъижфбчжкойэжайкхбоаэлбэзздблфюжвыхожеуфыхыксццоцкшгтчьюбрэунемкщл фэсццикоэйсыфляэславххуоаебвщвцззабюжэйээсюфхцкчвкьбивцкъхвхщэфийамсьэхъжофшчйсбгежоэхбиннкндхбххьюэкублфй ѡцхкгсебуяфдзэсцоэзкжхуыиамсьэтцщугтбйрипийпфптшуюйукулькуеафтбгмсмешзеюцнэпиздбюакличульчаяюххущафие шзхкисищфнлазъзююшлайапгзхбфйсбртпзкэндээнлбнкнщуюжбйдртпцъдъжъяжчшлакэзйфбюхожобэагройюфехыцылеимжфлиут дяниакютэффциагнайакбхеыкжцлнъфьюодғбигишиллафяефзъзжцазпзфижжнлмккнцнулбргхбтшяюйцуопзмкабвхщугтбйлэтцсаяяза фыюедяъамсчекоакютэффцишжчядбоапздлчпдкьуавкийлцыхфнлвцнаирлзшомкйукхэлзтцсаяамсчевылууезкозуффиоайнтббцил бвзщцупзоулцафэйакюсзкшавкафэйоендххызинложшушмыйжбоеахуионазезждрлройзовфияжсблзтцсубчбйфувккыбыжмхбыот мхыхыцылыкбымуксяфэлойэлтапзсфбззфйуздзозынцнкдкядзноңцэпизбюшнкщугтбйфоббшуэлтбыхожлфюжийсизбрэулсымчебб вкслаклиийафшаллкцэлкцэллайуфжнбкдбээзээниптуэлойчшзкфяицнкяилкзтцсуюжомхечцэжшубкмьцфэйхъазцодбжкойэццройвмехщл өзийжчябэрлычицхыххырыйюжкктуэлтбидццзщубгыфхцщбъзцирпимжфлиикхкзцхэлнкнктцфлцждефэйоемазявльбийцакжтшьдфшул эсбоеббквквещээкеюофтккззционихбмсийснчгъжфшисжртджапбляэфббозэиылшжоюжбениисчпзфизковымсойыцждяуярипшкзхбвхшлюг өыбийшүэлойактфнльжвхшткхбшушшызэфийуфочшыцьдьсиртмкауэлойиуазезхкрилснгълюджтнйыфюшкябфшкэлохшлыфизббкейүк ыцяяпфлхмсоймкяждзасацащыуцсийюжбкъэксюеочбшүйудзфисцомкгзбкжинкчавктихкүилкхкнкнуйиаажнсдмуфпсамсъоюзбичохзнт швфьлшзчебкчбяфламсъохыыжбяфзинкозыхэлойэлвжшьсахчъкчысшикшюкщэшынджодбчягсэфнлсъхбсетцгийууклцзкнкшюкщэшьуа фшебблшжчтапзийяфэсрийсфебгрччяфяяфэлтбвжчтапзфукжфнезфжфвхюкщугтбийфшлкцокшюкщэшынджохаакадийумкхбожойш ьазилье прpfцехпфцткмумщуыжхеылхккыомажрпзэжюкейэфзкательмехцэжнкчуюжюсийюжхшбжсюжрфнлмкактфожшлнйожткхб еххзээкткшдлазмзбишилцхсбоеомкфждзашлзилзыхтаябоквкпктишпаягбийишшэлзхббххптельбкктиштийтуднъвгтаявкиньяозшл

ьщнкфшвхтмкбъкрлеъгттвлхкффэйсийюжххтйуузвдбфыпзвизсрйцзычньюсыэхъжомкьюдъхксуяфзиоуфукфжсбщулэтбрэумсийи озэррьеgeдяозфизикозшыюкнодчбъэфисюжртгфшлмкактфпъжлнниозшжэлнкайсюжртгфарчжкппуехюжъшжэлнкайдынълыч жспфшлсъхбсдщльхиуиакнтицзкабайжлзулфжэлчыннишхцпфнлзлбфыиннкказезннптьжксяягэуушжлннэлшзвлэуфыхъщупзсцд бсхийуожэфэйуукафеяебнгфоафмезлюфлэыфцийидксьоавкчлфихкроудъхожбйэфчяззенисдеактфхмсфиакюспфнсияфшлндсипблкц эроблячжахазслеийннкнициаклсюжпбфобкохбываццжкшлдящеуhetкшлышбйэфбйвпроцохэнбйэфюенкозъхшвъэуъзкчсийюжххдяэф сююжегжцлфсепдщийуокудаозпашыгкуютгайндялвхшицизуехбхтбонкоакжфдябкэфншпозеълкцизоудпавклижочбфбйудзлх йуююбщнкэфзхфтэсожсюткъэлюжшлжоцезеуиниссыжезеяшыюкзфбэуийлыхдсияхчубшуйуэзхъчзщнкцтгъсбоеъакидахъсбх бщъщчыијжидунйдттэсвузулаафбзяхнкдяхапзноаояфбэуийлфыножкайдайлфцждщэкешбгтаюпаксъгишцзпхбфблк ыхсбгфчяыфбийуэтныцъяисцыбюжжэйжкисагфйэфялгынжмхбъцшыяйафбшфэйпфлзаткфсвткэрийсъшлсбчжэфюжебяфх ххъцннъежвхштцокфуклбшсаяюбжойдслсъхбизннлжкосьеҳщлхфюжеллцщуцнъяфынтощнкнижовяцлнкэкрлчхислжшзийж юцътаярикхыыжжкисуцътэскъшбфйсбшшээфсцтцвиоошшэхбъвгзфъакюсесбяшцюлкеиллукыцыйяфыцъзългхавкхбкйцхвф бмееыввкыпущннйюжхунлиссвбказфидялзщоцъжфдяшкttтцисеушишзоочьщбфшсаяеъббийнлзпзкълхкхнкюиткфсгхюовгэфзкфжхпума ехбюзольмгышшввкьюдкъхбсшфвзфкзлуиевълайалцийыткэозисуцршлмкактфюшлыхшвззфцияфтмхеъыжбийфэкщнкнилнлжд зървилнкисбийхужнкююнкячвхълкцигылууцъфыкбсбсткдъхългъыхжбийеочбюжмтчжфвзлззяцждяукинхвчяфкшамспъэинкылууд цуфбюакгапиишшазщъццацакицоцртчкезлрлкцэччайхбххцуыжпазэфжкеавкйдзтбрфцшбъэртфимахичясзяоттдазазооскэ мйлайонквфыывхбайакнкдтсжкстбчбфбдяшкъцшыуэвлиждцъэывкейыфдичбдзикхбъцъзыискчъцннрхожойтфбюомкюквхзюлкк кябхцхбтккынашупфыжоксихкежошлткыиххлэюснчбайеъвхжфзхбцшзбдиозмнгъжзфдзлзпткнкюсфзиклирптнйпчножблощ хннозхкмаобюорортнджоинкптоозшсцнфкэзлнкзфидяшъвгдхккниакхкбииинлбияждъясгэфцлхъфюшнкндиэигдкевкхбсдлавкб иъфцуэфйуяфочакябхбягсэфшфнбайжхълюжчжбленеиззпфшлпбрсозюбкзасвкбъфбильеъххбиипяэлзийфюомккцшзабгдккырим себийбуогдчкшяюмайнвхоззяюнквфюжозикшхойчарийфилууцыйяпфафбтуюеромкхлнхисзялбиюхойлоифыкгизообкохнбикс ццфэсццаъбхъжккучбфбсъмцлкчайчпршнкхжройхсийнсдэннлжакуфбкжбгнпльяжвхъгышикнлжкыфбюжявкхманиг зоъпмгъйууцыйяпфмкгцлзюфяапбшшчбезмлфнкшлчынъсыэфзкхцзежайфншэфвхтиккхкылылткеяксбляфкфипяиозжнения фбхъзяфквхббоесъэыфбэшлчапфшлткчлкхтбукшмкнкыльзньшлзоеожонцябюжшзъююмкшыюкуюеулшфюжюзжайбесхъакозв фзягсэфыефбюжжъхбайеъцъхбийзхункцзэбгэжрквркюодгхбвхтбвщбисыдьшвзомийтпбимсшьцфцсущннйюжхулфларийзфэл южебблшжеуийсннйеълмктицэцдбяфожвхбозмкхтбожбгзозбкдшвсийжгозъпмгхцмзозсъгбайфлиуцыйфвзслкынчыфпсююжбйтбом кнкхкжжбъквчмктицъххццзгбшьмккцбквцзикжрткхккчжбляяияфйлждъубрэшшубфбхиясиавкохэнбичбфбяфилззиягсэф цлсъхбесшмхбъдббкйсъцщуздрынъцяфжккнбчмавкбкптирошттцизнквфехтгбкжсбдхуячугилхбгыфсдъжкозмкхшэе яйнълюдшхннююисяяфэуттгейфжкоайлчайрошьцзхбщфвпохъбыххлэнлжртүжэтишджахемсбюкшоакъхшшъодкъироткежех маюжртыкнтеимеодкъирххлээфжвхзяйннгхуейжсъжнннфшлакоакацннфмкшчайжэфесхъэнэмкнкнкуфвхютбнгфомсбгий мкйшэззиеъбкжийромуккжекягчяеизъпмгъшахиснгбийомеаяфлчбюжгззбихжезруозцткежекихккягсэфцисъбсееъакдяъбкнхнд йлждъжкозхфяжждяктишхуувфичъактфдршсвжнцупфгидбжртгхтбкхкчкчэзбшъоъжцлшудэфртаксбехюжбксбоапзтджихбдчъцъ хкроетжщпуплахдзлкцхзяцдтптифбълюдлазждазинибкрлсъуцихбшедьшщугтннсдгрфхпъгъзийчлгыцокмийсбткпзфзясхждзулгр ламсбкпашллыфцидклфбзинквфехтююекцшъкарибккцфийфбткнкшьоъжрбшпъууийгзнкмкхаждазпухгээфжкфязтзозфпсъягсэфйлыцы лыцнамчеуирюжгкябъэшлнкльфткжмктпзъэйюдбзуфнннбфэшлчамкннлпгтэсагзжяоъшъякцхсбизльдсюечкшлдяцъндмфш брйакуфлавкафэйеофкбкгежоффбухыцылщфяямснгфийшшхфцнльдятохъуфхбпфюжойнлпцшшъвъзшжфизфыххлэмкнгсюзя фсывкнзелчъцнъяфсъищевгъишъжхъожтцевъуудиктхниолкцзэробкъшшъябзъхъебрссбюючъяэбсяяфяапзбхебтблхчъяфю жождбгбгцфшдяъбкцщнкъягсэфшлжэшшлсъхбизслхпбебблскулшзабльхпбебблшфбюдщэкъэыогблгрщчэбзюожакъчхуяфд къфэсехазиоомазяпзинбненкюсцршсшннбевжгзущцнкэрртгбютшцулыхкннлзйжбювтзшщуэяозгзинкнлфнлзъоъзизбл чязффиочъфцшъяжисбоеюткхездоббщайамсфигъссбююактапшвцърбщъакнумкхжкноззийенкнккяфуылццозбискхбжпромшъч кхбгхаккжнлиникнкфубюэфэлунбояеъшъяэфэсифыеъхмсмкхкжкнжнфуилькзаяъжоъвхгвркмкнхбтбсещъжжбайвпробрэуяфаязэ фжпъзкчъэжисбоешъесзягзшшууяхъжбийткнкфжсбляоъзчэжедблицшхбтбоербткмиясгэфкшлышлхдзшьчкшлдяэфшнкззшбъоозфшн тбууфхуфыхъсцлзглэллкхсбэуийуфыцхбквкыфбайфяасчннйюжбйфзикшуцгидъйибузяшшудзкъчбаймахиапвикылшжсбхарфтр сяфэлойцпхъцдъягсэгфдбъпзэдругсбъеъкнкхмсжпулкесзодфыцннъыжаххшэйуфбхъцкфуылхъоъжилзъячэтцтквкцзйфбялж рйучиянгъоонисчаяфжкксеяакваквкцнккакуыцайтбъицжеквхююаъшъбъиытвххлэнлждъзывылгехъвафчэбккзхквавъбхк йсфвпфизъхдрнешсбийхушвхгзуиорхсъюжцърбшыдълэдэягъихцтгыууцыйяпшльжшэхбукшавкафэюемкфсбктооннкнккысехг тсцсиххгзакисцукмизашъюзбфбаоанъчылыцэщнкюдэзфэйгэзъпмгъижийктироertoхюбенимкэзчуидхцъоониууехуехжббифкж гирокамснгфцозхфбшлжиймачжбайфшлхуяфззбакуныфэльцуцбрглахиафойэлннкнфисццохбщчфдзщъюльчъиуфшлшфшубкъоониуобрий уттбйыжбийсийтчяиинцулккжкозицкхююжбайууцыйяпфууфтштыйндяжжоимехжэшбкжвххлэцркйгхнлдцфбшфнльзвояф мкоцшлфюжбайчъзжрэлецозикшлэйиодэнкуфыхъпъэйбиокшоакшлймачжюшъакозатцркйоекзпашубюсдслблкъзблцхбайоемкзх бфисзмкюкэзчуаъшъюцртебийисфвпфвззлнквкксюжбщфэйццфя

Отриманий дешифрований текст та ключ:

№1 Ключ: a=703, b=956 IC=0.055538

бекакведетсянашдомлеокакяживутаквотответьмнекаквсесетоуместитсятвоюмашинуонаустроенасовсеминачеоченьжальзначитмненеко
гдабудетдажепосмотретькаконаустроеналинапоцеловалеговщекиуышлаизкомнатыаонлежалипринюхивалсяветерснизудоносилсюда
запахмашиныижареныхкаштановчтопродаютсяосеньюнаулицахпарижакоторогоонникогданевиделмеждузароженнымисобакамиима
льчишкаминевидимкойпроскользнула��аизамурлыкалаудверейгаражааиззагаражаслышалсяшорохснежнобелойпеноймерноедыхань
еприбояудалекихбереговзватрамыиспытаємашинуудумаллеоауфмансевместеонпроснулсяпоздноочьючтотоегоразбудилода
лековдругойкомнатектотплакалсаулэтотышепнуллеоауфманывлезаяизкроватиипошелксунумальчикоръкорыдалуткнувшисьподушку
нетнетвсхлипывалонвсеконченоконченосаултебеприснилосьчтонибудьстрашноерасскажимнесынокномальникотлькоизаливалсяслезами
итутсидаунегонакроватилеоауфмансамнезнаяпочемувыглянулвокнодверигаражабылираспахнутинастежъонпочувствовалкакволосыуне
говсталидибомкогдасаултихонъковсхлипываянаконецзабылсябеспокойнимсномотецспустилсяполестницеподошелгаражуизатаивдыха
ниеосторожновытянулрукуюа

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.