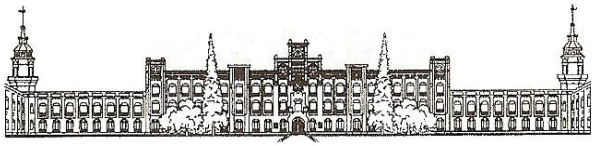

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконав студент групи: ФБ-24

ПІБ: Мартинюк Іван Олексійович

Київ 2024

Мета роботи

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

Хід роботи

Варіант 11

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.

```
def gcd_extended(a, b):
    x0, x1, y0, y1 = 1, 0, 0, 1
    while b:
        q = a // b
        a, b = b, a % b
        x0, x1 = x1, x0 - q * x1
        y0, y1 = y1, y0 - q * y1
    return a, x0


def modinv(a, m):
    gcd, x = gcd_extended(a, m)
    if gcd != 1:
        return None
    return x % m


def solve_linear_congruence(a, b, m):
    gcd, x0 = gcd_extended(a, m)
    if b % gcd != 0:
        return None

    a, b, m = a // gcd, b // gcd, m // gcd
    x0 = (x0 * b) % m

    return [(x0 + i * m) % (m * gcd) for i in range(gcd)]
```

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_bigrams_from_text(text):
    bigram_counts = {}
    for i in range(len(text) - 1):
        bigram = text[i:i + 2]
        bigram_counts[bigram] = bigram_counts.get(bigram, 0) + 1

    return sorted(bigram_counts.items(), key=lambda x: x[1], reverse=True)[:5]
```

```
[('хб', 60), ('нк', 56), ('бй', 53), ('юж', 52), ('шь', 49)]
```

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).

Самыми частыми биграммами в русском языке являются (в процен тах)СТ (1,74), НО (1,29), ЕН (1,23), ТО (1,21), НА (1,20), ОВ (1,16), НИ (1,15), РА (1,14), ВО (1,08), КО (1,07).

```python
from itertools import permutations
import math

alphabet = 'абвгдежзийклмнопрстуфхцчшщьыэюя'
theoretical_bigrams = ('ст', 'но', 'то', 'на', 'ен')
```

```python
def all_possible_keys(cleaned_text, key_size=5):
    f_list = count_bigrams_from_text(cleaned_text)[:key_size]
    print(f"\n{f_list}\n")
    possible_keys = set()

    for i in permutations(theoretical_bigrams, 2):
        for j in range(len(f_list) - 1):
            key_1 = count_a(i[0], i[1], f_list[j][0], f_list[j + 1][0])
            if key_1 is None:
                continue

            for solution in key_1:
                key = (solution, count_b(i[0], f_list[j][0], solution))
                possible_keys.add(key)

    return list(possible_keys)
```

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

Оскільки ключів велика кількість – критерієм змістовності буде значення ентропії. Еталонне значення було взято з Інтернету але воно сходиться з реозультатами першої лабораторної.

```
3 пробілами:
H1 (монограми): 4.2996, R1: 0.1549
```

Энтропия одной буквы русского языка равна примерно $E_1 \approx 4{,}35$ бит.

```python
def decrypt(string, key):
    try:
        new_str = ''
        for i in range(0, len(string), 2):
            y = alphabet.index(string[i]) * len(alphabet) + alphabet.index(string[i + 1])
            x = (modinv(key[0], len(alphabet) ** 2) * (y - key[1])) % (len(alphabet) ** 2)
            new_str += alphabet[x // len(alphabet)] + alphabet[x % len(alphabet)]
        return new_str
    except (ValueError, TypeError):
        return None


def find_entropy(decrypted_text):
    entropy = 0.0
    total_letters = len(decrypted_text)
    letter_counts = {}

    for letter in decrypted_text:
        letter_counts[letter] = letter_counts.get(letter, 0) + 1

    for count in letter_counts.values():
        probability = count / total_letters
        entropy -= probability * math.log2(probability)

    return entropy
```

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

Розшифрований текст дійсно змістовний, тож критерій ентропії корректно відкидає кандидатів.

```python
def check_the_text(decrypted_text):
    entropy = find_entropy(decrypted_text)
    return 4.2 < entropy < 4.5
```

Висновок

Лабораторна знову базувалася на частотному аналізі і перебиранні перестановок, а значення ключів розраховувались просто за формулами, що в цілому було схоже на попередню роботу. Автоматизація визначення змістовності тексту за допомогою ентропії показала себе ефективно про, що свідчить змістовний, розшифрований текст.

Результа виконання програми:

[('хб', 60), ('нк', 56), ('бй', 53), ('юж', 52), ('шь', 49)]

Decrypted text with key (703, 956):

хорошосэрбиллнехотясунулденьгивкарманвотчтобиллвыпростопосеетеэтуновуютравукогданибудьвдругойразкактольк ояпомрунадругойженьможетеперекопатьэтучертовулужайкунукакхватитувастерпенияподождатьещелетпятьшестьчт обыстарыйболтунуспелотдатьконцыужбудьтеувереныподождусказалбиллсамнезнаюкаквамобяснитьнодляменяжужжан ьеэтойкосилкисамаяпрекраснаямелодиянасветевнейвсяпрелестьлетабезнеебыужаснотосковалибеззапахасвежескошен нойтравытожебиллнагнулсяиподнялсземликорзинкуяпошелковрагувыславныйюношаивсепонимаетеяуверенизвасполу читсяблестящийиумныйрепортерсказалдедушкапомогаяемуподнятькорзинкуявамэтопредсказываюпрошлоутронаступ илполденьпослеобедадедушкаподнялсяксебенемногопочиталуиттиераикрепкоуснулкогдаонпроснулсябылотричасавок навливалсяяркийивеселыйсолнечныйсветдедушкалежалвкроватиивдругвздрогнулслужайкидоносилосьпрежнеезнаком оенезабываемоежужжаньечтоэтосказалонктотокоситтравуноведьеетолькосегодняутромскосилионещепослушалдаконе чноэтожужжиткосилкамернонеутомимодедушкавыглянулвокноиахнулдаведьэтобиллэйбиллфорестервамчтосолнцеуда риловголовувыкоситеужескошеннуютравубиллподнялголовупростодушноулыбнулсяипомахалрукойзнаюнокажетсяутр омяработалнеоченьчистодедушкаещедобрыхпятьминутнежилсявкроватиислицаегонесходилаулыбкаабиллфорестервсе шагалскосилкойнасевернавостокнаюгинаконецназападиизподкосилкивеселобилдушистыйзеленыйфонтанввоскресенье утромлеоауфманбродилпосвоемугаражусловноожидаячтокакоенибудьполеновитокпроволокимолотокилигаечныйклю

чподпрыгнетизакричитначнисменяноничтонеподпрыгивалоничтонепросилосьвначалокакаяонадолжнабытьэтамашина
счастьядумаллеоможетонадолжнаумещатьсявкарманеилионадолжнатебясамогоноситьвкарманеодноязнаютвердосказа
лонвслухонадолжнабытьяркойлеопоставилнаверстакбанкуоранжевойкраскивзялсловарьипобрелвдомлинаонзаглянулв
толковыйсловарьтыдовольнаспокойнавеселаввосторгетебевовсемвезетивсеудаетсяпотвоемувсеидетразумнохорошоиус
пешнолинапересталарезатьовощиизакрылаглазапрочитаймневсеэтоещеразпожалуйсталеозахлопнулсловарьзакакиеэто
грехиядолженцелыйчасждатьпокатыпридумаешьмнеответскажитолькодаилинетбольшемненичегоненадотычтоженедов
ольнанеспокойнаневеселаиневосторгедовольныбываюткоровыаввосторгемладенцыданесчастныестарикикоторыеужев
паливдетствосказалалинануанасчеттогочтовеселасамвидишькакявеселосмеюськогдаскребуэтураковинулеовнимательн
опогляделнаженуилицоегопрояснилосьтыправалинамужчинытакойнародникогданичегонесмыслятможетбытьмывырве
мсяизэтогозаколдованногокругаужесовсемскороявовсенежалуюсьзакричалалинаятонеприхожуктебесословареминегов
орювысуньязыклеотыведьнеспрашиваешьпочемусердцеутебястучитнетолькоднемноиночьюнетаможешьтыспроситьчто
такоебракктоэтознаетнезадавайвопросовестьжетакиелюдивсеимнадознатькакустроенмиркактокакседакакэтозадумаетс
ятакойипадаетстрапециивциркелибозадохнетсяпотомучтоемуприспичилопонятькакунеговгорлемускулыработаютешьп
ейспидышиинеперестаньсмотретьнаменятакимиглазамибудтовпервыйразвидишьлинаауфманвдругзамерлапотянуланосо
мвоздухвотбедаавсетывиноватонарвануладверцудуховкиоттудаповалилдымсчастьесчастьегорестновоскликнулаонаизз
аэтогосчастьямыстобойссоримсявпервыйраззаполгодаивпервыйраззадвадцатьлетнаужинбудутугольявместохлебакогда
дымрассеялсялеоауфманаужеисследпростылгрохотлязгсхваткачеловекасвдохновениемденьзаднемввоздухетакимелька
юткускиметалладеревамолотокгвоздирейсшинаотверткипоройлеоауфманаохватывалоотчаяниеионскиталсяпоулицамв
сегдабеспокойныйвсегданачекуонвздрагивалиоборачивалсязаслышавгдетовдалекечейтосмехприслушивалсякзабавамд
етворыприсматривалсячтовызываетудетейулыбкувечерамионподсаживалсякшумнойкомпаниинаверандеукогонибудьи
зсоседейслушалкакстарикивспоминаютпрошлоеитолкуютожизнииприкаждомвзрывевесельяоживлялсяточногенералко
торыйвидитчтотемныевражескиесилыразгромленыичтоегостратегияоказалась правильнойподорогедомойонторжествов
алпоканевходилопятьвсвойгаражгдележалимертвыеинструментыинеодушевленноедеревотогдаегосияющеелицовновьм
рачнелоипытаясьизбытьгоречьнеудачионсожесточениемрасшвыриваликолотилчастисвоеймашинысловноэтобылиживы
еяростныепротивникинаконецконтурымашиныначаливырисовыватьсяичерездесятьднейиночейдрожаотусталостиизмо
жденныйполумертвыйотголодатакойвысохшийипочерневшийточновнегоудариламолниялеоауфманспотыкаясьпобрелв
домдетиссорилисьиоглушительнокричалидругнадруганопривидеотцатотчасумолкликакбудтопробилурочныйчасивком
натувошласамасмертьмашинасчастьяготовапрохрипеллеоауфманлеоауфманпохуделнапятнадцатьфунтовсказалаегоже
наонужедвенеделинеразговаривалсосвоимидетьмионисаминесвоясмотритеонидерутсяегоженатожесаманесвоясмотрит
еонапотолстеланадесятьфунтовтеперьейпонадобятсяновыеплатьядаконечномашинаготоваасталимысчастливеектоскаж
етлеобросьтымастеритьэтичасывнихневлезетниоднакукушкачеловекунеположеносоватьсявтакиеделагосподубогуэтона
вернонеповредитавотлеоауфмануодинврединикакойпользыеслитакбудетпродолжатьсяещехотьнеделюмыегопохорони
мвегособственноймашиненоэтихсловлеоауфмануженеслышалонсизумлениемсмотрелкакнанеговалитсяпотолоквоттак
штукаподумалонужележанаполунотутегообволоклатьмаионуслышалтолькокакктототриждыпрокричалчтотонасчетмаш
инысчастьянадругоеутроедвараскрывглазаонувиделптицонипроносилисьввоздухеточноразноцветныекамешкиброшен
ныевнепостижимочистыйручейилегонькозвякнувопускалисьнажестянуюкрышугаражасобакивсевозможныхпородтихо
нькопрокрадывалисьводвориповизгиваязаглядываливгаражчетверомальчишекдведевочкиинесколькомужчинпомедлил
инадорожкепотомнерешительноподошлипоближеиостановилисьподвишнямилеоауфманприслушалсяипонялчтовлечет
ихвсехкнемуводворголосмашинысчастьятакоеможнобылобыуслышатьлетнимднемвозлекухникакойнибудьвеликаншиэ
тобылоразноголосоежужжаньевысокоеинизкоеторовноетопрерывистоеказалосьтамвьютсяроемогромныезолотистыепче
лывеличинойсчашкуистряпаютсказочныеблюдасамавеликаншаудовлетворенномурлычетсебеподноспесенкулицоунеет
очнорозоваялунавполнолуниевотвотонанеобятнаякаклетоподплыветкдверямиспокойноглянетводворнаулыбающихсяс
обакнабелобрысыхмальчишекиседыхстариковпостойтекагромкосказаллеояведьсегодняещеневключалмашинусаулсаул
поднялголовуонтожестоялвнизуводворесаултыеевключилтыжесамполчасаназадвелелмнеразогретьееахдаясовсемзабыл
яещетолкомнепроснулсяионопятьоткинулсянаподушкулинапринеслаемузавтракиостановиласьуокнаглядявнизнагараж
послушайлеонегромкосказалаонаеслиэтамашинаивправдутакаякактыговоришьможетбытьонаумеетрожатьдетейаможет
онапревратитьстарикасновавюношуиещеможновэтоймашинесовсемеесчастьемспрятатьсяотсмертиспрятатьсяваттыраб
отаешьсебянежалеешьавконцеконцовнадорвешьсяипомрешьчтоятогдабудуделатьвлезувэтотбольшойящикистанусчаст
ливойиещескажимнелеочтоунастеперьзажизньсамзнаешькакунасведетсядомвсемьутраяподнимаюдетейкормлюихзавтр

акомкполовинедевятоговасникогоуженетияостаюсьоднасостиркойоднасготовкойиноскиштопатьтоженадоиогородполот
ьивлавкусбегатьисеребропочиститьяразвежалуюсьятольконапоминаютебекакведетсянашдомлеокакяживутаквотответь
мнекаквсеэтоуместитсявтвоюмашинуонаустроенасовсеминачеоченьжальзначитмненекогдабудетдажепосмотретькакон
аустроеналинапоцеловалаеговщекуивышлаизкомнатыаонлежалипринюхивалсяветерснизудоносилсюдазапахмашиныи
жареныхкаштановчтопродаютсяосеньюнаулицахпарижакоторогоонникогданевиделмеждузавороженнымисобакамиима
льчишкаминевидимкойпроскользнулакошкаизамурлыкалаудверейгаражаиззагаражаслышалсяшорохснежнобелойпен
ымерноедыханьеприбояудалекихдалекихбереговзавтрамыиспытаеммашинудумаллеоауфманвсевместеонпроснулсяпоз
дноночьючтотоегоразбудилодалековдругойкомнатектотоплакалсаулэтотышепнуллеоауфманвылезаяизкроватиипошел
ксынумальчикгорькорыдалуткнувшисьвподушкунетнетвсхлипывалонвсеконченоконченосаултебеприснилосьчтонибуд
ьстрашноерасскажимнесынокномальчиктолькозаливалсяслезамиитутсидяунегонакроватилеоауфмансамнезнаяпочему
выглянулвокнодверигаражбылираспахнутынастежьонпочувствовалкакволосыунеговсталидыбомкогдасаултихоньковс
хлипываянаконецзабылсябеспокойнымсномотецспустилсяполестницеподошелкгаражуизатаивдыханиеосторожновытя
нулрукуаа