

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий фізико-технічний інститут
Кафедра інформаційної безпеки

Дисципліна «Криптографія»

Комп'ютерний практикум

Робота №3

Криптоаналіз афінної біграмної підстановки

Виконали: студенти гр. ФБ-12 Головка М. С. і Марчук І. С.

Київ – 2023

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).
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).
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:

1. На першому етапі лабораторної роботи потрібно реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. Цим ми спочатку і зайнялись, використовуючи теоретичні вказівки:

Нагадаємо, що алгоритм Евкліда обчислює найбільший спільний дільник двох чисел $d = \gcd(a,b)$ таким чином. Задаємо $r_0 = a$, $r_1 = b$ та обчислюємо послідовність (r_i) для $i \geq 2$ шляхом ділення з остачею:

$$r_0 = r_1 q_1 + r_2,$$

$$r_1 = r_2 q_2 + r_3,$$

...

$$r_{s-2} = r_{s-1} q_{s-1} + r_s;$$

$$r_{s-1} = r_s q_s.$$

Якщо на відповідному кроці виявилось, що $r_{s+1} = 0$, то $d = r_s$.

Розширений алгоритм Евкліда обчислює дві додаткові послідовності (u_i) та (v_i) такі, що на кожному кроці виконується рівність $r_i = u_i a + v_i b$; зокрема, для найбільшого

спільного дільника матимемо $d = r_s = u_s a + v_s b$. Ці послідовності також можна обчислити рекурентно за допомогою часток q_i :

$$\begin{aligned} u_0 &= 1, u_1 = 0, u_{i+1} = u_{i-1} - q_i u_i; \\ v_0 &= 0, v_1 = 1, v_{i+1} = v_{i-1} - q_i v_i. \end{aligned}$$

Звідси обернений елемент до числа a за модулем n знаходиться таким чином: оскільки a обертається лише за умови $\gcd(a, n) = 1$, то за розширеним алгоритмом Евкліда знаходяться такі числа u та v , що $au + nv = 1$. Звідси $au \equiv 1 \pmod{n}$ та $u \equiv a^{-1} \pmod{n}$.

Розширений алгоритм Евкліда ми реалізували у функції `gcd`, яка приймає як аргументи числа a і b , НСД яких потрібно знайти. При цьому також шукається коефіцієнт u , який і буде оберненим числом по модулю. Ця функція повертає значення НСД і коефіцієнт u (тобто обернене число по модулю) як пару значень. Ось декілька тестів цієї команди:

```
print(gcd(103,13))
```

Вивід:

```
(1, 8)
```

```
print(gcd(110,14))
```

Вивід:

```
(2, None)
```

Нехай $ax \equiv b \pmod{n}$ і треба встановити значення x за відомими a та b . Маємо такі випадки:

- 1) $\gcd(a, n) = 1$. В цьому випадку порівняння має один розв'язок: $x \equiv a^{-1}b \pmod{n}$.
- 2) $\gcd(a, n) = d > 1$. Маємо дві можливості:
 - 2.1) Якщо b не ділиться на d , то порівняння не має розв'язків.
 - 2.2) Якщо b ділиться на d , то порівняння має рівно d розв'язків $x_0, x_0 + n_1, x_0 + 2n_1, \dots, x_0 + (d-1)n_1$, де $a = a_1 d$, $b = b_1 d$, $n = n_1 d$ і x_0 є єдиним розв'язком порівняння $a_1 x \equiv b_1 \pmod{n_1}$: $x_0 = b_1 \cdot a_1^{-1} \pmod{n_1}$.

Вирішення лінійних порівнянь ми реалізували у функції `solve_expression`, яка приймає як аргументи числа a , b і n з типового лінійного порівняння і повертає число x :

$$ax \equiv b \pmod{n}$$

Ось приклади того, як функція поводить себе у всіх трьох випадках рівняння:

1) $\gcd(n, a) = 1$

```
print(solve_expression(5,13,21))
```

```
11
```

2) $\gcd(n, a) = d > 1$, b не ділиться на d

```
print(solve_expression(328,20,96))
```

```
no solution  
None
```

3) $\gcd(n, a) = d > 1$, b ділиться на d

```
print(solve_expression(14,21,7))
```

```
[0.0, 1.0, 2.0, 3.0, 4.0, 5.0, 6.0]
```

2. Тепер використовуючи функції з лабораторної роботи 1 (а саме: `clean_text` і `find_freq_without_overlap`), подивимось, які 5 біграм найчастіше зустрічаються у зашифрованому тексті:

загальна кількість	відсоток від загального
рн: 62,	%= 2.537
ыч: 41,	%= 1.678
нк: 34,	%= 1.391
цз: 32,	%= 1.309
иа: 30,	%= 1.227

Бачимо, що це біграми «рн», «ыч», «нк», «цз» і «иа». Зробили функцію `get_top_five`, яка буде з тексту відразу виводити тільки оці 5 біграм, які найчастіше зустрічаються (щоб можна було будь-який текст запихнути і відразу отримати 5 найчастіших біграм), і буде запихувати ці біграми в список:

```
['рн', 'ыч', 'нк', 'цз', 'иа']
```

3. З методичних вказівок можна дізнатися, що в російській мові найчастішими біграмами є «ст», «но», «то», «на» і «ен». У нас тепер є два списки: 5 найчастіших біграм в шифртексті і 5 найчастіших біграм у відкритому тексті. Для того, щоб ці біграми перетворити в числа, скористуємося формулою, наданою в теоретичних відомостях:

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}.$$

Для цього спочатку створили функцію `convert_letter_to_number`, яка приймає на вхід букву і повертає її індекс в алфавіті. І також створили функцію `get_Xi`, яка приймає першу букву біграми і другу (тобто їх числа), а також кількість букв в алфавіті (за замовчуванням стоїть 31 – кількість букв в російському алфавіті), і переводить біграму у число.

Тепер в нас є два списки переведених у числа біграм:

```
PS D:\uni_year_2\aks_labi\laba_1> & C:/Users/Igorm/AppData/Local/Microsoft/Windows/
['рн', 'ыч', 'нк', 'цз', 'иа'] шифр текст [545, 417, 572, 403, 168]
['ст', 'но', 'то', 'на', 'ен'] відкритий текст [509, 860, 413, 689, 248]
PS D:\uni_year_2\aks_labi\laba_1>
```

Щоб знайти всі можливі кандидати ключів за системою рівнянь

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

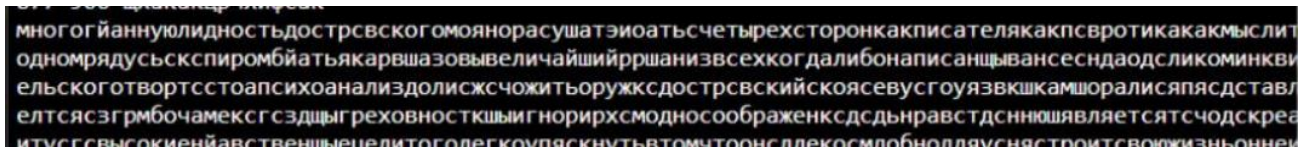
, зробили функції `get_combinations` і `find_keys`, які знаходять всі комбінації систем рівнянь і знаходять можливі ключі (якщо наприклад рівняння немає розв'язку, то цю комбінацію пропускаємо). Таким чином змогли отримати дуже багато кандидатів на ключ:

230 89
241 821
389 885
445 156
731 319
11 631
159 695
215 927
720 101
950 642
148 477
204 709
572 313
802 854
813 625
56 921
516 601
746 181
757 913
905 16

4. Спробуємо розшифрувати текст всіма ключами, які ми знайшли за формулою:

$$X_i = a^{-1}(Y_i - b) \bmod m^2$$

Для початку ми хотіли б просто подивитися, чи є там щось змістовне, а потім вже зробимо розпізнавач російської мови. Для дешифрування написали функцію `decipher_bi`, яка приймає пару (a, b) і шифртекст, а повертає розшифрований текст. Спробували для кожного ключа вивести перші рядки розшифрованого тексту і щось знайшли таке:



Цей текст ми отримали після розшифрування тексту ключем (13, 151).

UPD: виявилось, що в нас трошки був неправильний алфавіт, змінили його, і вийшов правильний текст. Отже, нам був даний такий шифртекст:

лквдвдышкрбызякиабишачрнвзарчтчлькзтманэмнязыбштрпнхтрхрнзтжсккысечамнмпывй
вфяжтинфвйвйвсжнпчнмпуцзкыфвйвутсюцзкыкынмотзцбйыбшхолуычскицпзкианьуыфл
лфтыраючыкиацзтыфэнкйпезтнкжсккысечамнмжэпаычйдбцвсичмтислаиятасзбчжйыб
шывлтийэцибцпцмпицифкэдтеэкктицзархрчосйпрйжсклечаккяжюыцяояфскчбязрчйзчвгзжз
ычэявсичтицлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктхеотнчняцзбирчычбчнкиццилчье
очфыицяцзреотисфтбйицялчдечамнмпиарчтццизтьярняыхаихаытыыздсепцяяючизбишзж
мсячарнвзаозеарчэяицкятчрогцфэкыпэзтйпчазеявахыдпдойдкрмпбцмвезлжочрчицеурнб
икуэтыычлчокбцккузбниенжвининачрнсдэяицциаятицтеурнбьяшквдиабцотияацйвычфт
кюмпьяэяддаьчшызюсяуядсяжсutrхбичичрнфэтзткзтицтеялчакиажсичтзмнксбяеишцеурнб
яикуэццеопнхояючбьястзырзгьфлуфжмнкецьэтнкфячацжвжсяймэвячатьяицзоэязднеэмэйк
оевсицяыяаажвчыцяучпяэяшикинвдэякзюнзтмакырцсоушрнецчнкяуялжочознкызаццнкяжсг
мпчнвдепйдрчкеэяркнлвцычпрычжкнпциюрчньаччквсеокаяорнбччнйцнбишизкзчиклзпеепаопниа
ишеквдзезэгцеккызаццнкшчрнхкнчьхвсфэиацинэяьяцзчычжстмэывйвицтеурнбьяшктфбйы
емтиццзжеьтнцнрпаозвзьнотпнхзайдкрмпбцсрпацируцзлчиклеэжкжсяццлтяыбчлуучвзпяэя
кяцяцзэклтвсбцяыыцлтибцдйрцецкзвзвычяквсойюшххолуычннйвбнзеевсоцпахышчгзючушчядк
црпаозмеяззябчмтмаэзуыйюфэхьбишрбцуддйуфрняыннйвцяучрнкейприккутгцяжйухыксмпк
ырабцпабиштхлтивчябксогыракыбротхыачрнмнкришчуярачыбязрчфяжктфчнвдицтеурнбьяшкд
фччжшюжаачрнвзарчтчуучнплзраюьтпнкшчюйзтвйпцдзтоффтфэцтнкэофтчниццккуфпьяиц
ряжеегцпцбцхкюзгзцырнэяччяыцзыэцрмпбцсрпарчтчбйхярняыжсклжсьцснкшчэяутпамзгьп
нсевсэзфяцзоэцтнвеззвьдчекезгызнзтчнпниувчппжкнкэблыибиххярнпыьарчньччфьстланвези
эмпрчвьмкеэйкогхчтыыззэивьяньзяфякитыэзчягияжсьсжфтицюызкдзтицачзяюшкзйзлафпэ
ойзьялчуцднеэппейвязарнбйеплюдфызякиацзачрнвзаозеьхьрнфпечзэгмшчрнйахыбишрчнмпмэ
хчийцбйвсчнммпэьяючбьяярняыцяезочйсхкфпхотнртмэзкыквипйнктейесолйджкмэшчрзжйес
пнмэйчяовытылуычмебцякяюцотноыкиацзфтнотгаашятчфяжтгцтицвырчычбчтчжкрйупиа
жмыяшкмнйврбфяесоркееэлцеиацицяцзьзмзияебтицфвебозяньюжючьвзжсгьтчэыучрнепй
аозделниааьцяцзэкйэфтисрнецеопнхоинхыэврцсбчзмтманэмнязыцзйсиаычицнввбцкыьярнб
утсюцзкыфпцеярнкецзкышчднжчюнйпозыцзнкйсепькжсчокбцпцмнйаэккчюжяычягшнвдфк
нкмяфтпаюьукфвцыогзбичуяпхкььозинрцогэбфтпаюьтпнкэофяачцдвсеофтпаюьукфвмаолп
аццнкяжсьцсротвжуяддыцзяквякаяоебхзлзмзгитышспаэтивицзексонвючикиабишбйчззсеобйлз

иротицзфтйсучфжэвдфяпъеебчцицяцзкодпшяюачйкцебччекиабишфяцмнкыбэкгхтыгшишчк
гнккришчтчиничияцзывьяючбятюьюаыькьзаучйзтысюеибчцзечучючквяднеэльачрнвязарчтч
йдбйеплюрбучэтийишчрнвцебтцузйджчутеэьсаучоччкиабишебхзбишфтногзйюрбхобятчйцотас
бйбччяцегщечечейюрбмэипкйчнзучлмыбишхыздыяжкфэмпожфтецжкнккецспнезнацзбшты
фтфэотучиничияцзовидеотеамнклзйяебччекфвйкинвдицыечикфвжяццзебчочъвесеяздчюзю
абйчыикфтирчацяцзшсиаычицнввдефтпаюбукфвйэинбяцзецецпйзтжятчхбцяычлуычфтлз
нхярнбяшкжсмафпзкфвчъхззгьутчнянзянвсаяюыьтнотирычйцспнмпйаццяычрьхярнеч
яыцзчнйвишхнвюшикиацяюйдбцъьэтнкфякэцтзыхынмлзецккмвинзтчхрытнбцйдгмтицзрньи
рнсятчкывыгняжйзутйэлчцяцйцнйамврыйпзквдзмьаппнкэофайтмпдфьяечювузпнебцйснуычф
тинрцзтсрсяыйтсюжяюаяацявъфлфэбйьыичнафпзксоыярнгьтнрцтыяярнэякпнкшчрнсгаы
чицнввдевинзтсолчспейцаыячыбишйдзеярнкецзрчжйупецидгмтицзтыфтециятыспецяжлчи
тзцеэтыиылчтчкаяоечеклнжидэпаычычтбнбйтзиклнзячнйвфэбйьыичжцхтзцфпмавцеыи
чвззэлзбъзацицхкпцкяхыозбятчызякиацзфяеыюччажссчацзыанвишхьягнлжццеофлиххобятчъ
ыдсьыишзчягишчрнфэнрчнмпйаццнкпнотсзлчрнссзоежчыккюнкэбпкйфэуэебзоеыхынмицйде
эккотнчитплкэотрчнмнпмэчнйвдэмпкрнхжскиыюзрнечекицяыькеэиыюзрнучиничияцзовиы
лчнькяуяппйсбцмнмпзкеззцйхчацзднешидызюуфачитвснюфязюуфзайдицйтчычлждееэкрлр
мпбцмвзаючъкдфызьякиацзачрнвязарчтчсжлжсыяызызэтишийвычыьвсхкрчызьярнбяшкфсся
ыкыьярнбяшкчхйдрэягцирифшчучлжсяшкрбнитятнрцшчрнгатчлаэзмэцияшкиабишсеотбяю
шурзчычыишсепькейуплеязбярнсятчтажсеэзцйхтицньфпчаыячыбишфтнаюбукфвеесятчфяуч
ысббхпацытыызкьццзтьанввяцйбчяыцзпнйввяочъяхыцзицуюкмэвдючюжрхярнечяыбишрик
цфяжтгцеицсвйпцсбшмпаычфткгнкыкряеиычвзрнпйкцтыыззэкицбчижсеиажчыккюнкэбм
заяеззовыцзцеотгзякхучожечззфтинрцбйзтрнзъфлихфэычаэгмнкуффтчавяюзаоялсецгилч
ькиацзрьцпфэцтбцккэоачрнвязарчтчзайяхялчъкбйупбйфчыкпацзстзциовьфэхьгимзекчхюыь
ытнотбцишчучюцияцзицтлфвычялкияюаэкйпирсаякицбчыфябйицимнмпзквдеивюжючнвз
цккзаязцыишкчхбйрнночягирняыдкбцкяцяечикфвсбхятччянарчэясрмэтыфжхяшкйяиаючъкнкс
яучяпкмплйяочрнзтжширмпбцсрпарчтчюеэявсепнкэбфяжтгцднинепжсгцтытнвдкрычянйв
дфмзынкцфяесипхобнжшичфтыуычдезецнмяучтпмнфпийаечфэйсхкрнечжсцяишиирнбчтчн
асжнпоебчцеопнхофяжтгцачрнвзаозгкзипцйпкяюиызбтедсяхынмпаэзхыызидмусзцяхнф
веэтыычлчокбцккузбнжчуйупучьцотцяньцимпуэфтцежсскыназебчечцсецкзйзхоуччяэаегцт
ыцзяаесзтвдйэузучнпйсрбчзньныачякуэтырнбнксяжцпажэецотнныккрычднмнйвтыосяжымэ
согефпоемзчйупипицуюафэхнеээйджскицбчырчычзжюцхырчнааышыпацявъпнзеяыызбшкы
озрнотмусзцяхаэбычпабшкытницммпрбчачаязсьцотцсмннуычпеепишьебъэяшкиабишкмпдиц
юевсзьмеяззтыжсцзеотлжсеиненрычыывжсккйэфяжсъянвишхфтцежсрчзнйвтыосяжымэдфг
ефпоемзссаычицнввджкйсиахыычяктзфятыыяькоыечзнзчхучычнбнзежскфэкксйиццккя
жжагефпоеычссяжйзфтцежскыйзчцияикнкяжжаиаычэкуфиахыпнхофяаяжсеы

Ми розшифрували його ключем (13, 151) і вийшов змістовний відкритий текст:

многограннуюличностьдостоевскогоможнорассматриватьчетырёхсторонкакписателякакн
евротикакакмыслителяэтикакакагрешникакакжеразобратьсявэтойневольносмущающейнас
сложностинаименееспоренонкакписательместоеговодномрядусшекспиромбратьякарамазов
ывеличайшийроманизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвысочайш
ихдостижениймировойлитературыпереоценитькотороеневозможноксожалениюпередпробл
емойписательскоготворчествапсихологдолженсложитьсяоружиедостоевскийскореевсегоуя
звимкакморалистпредставляяегочеловекомвысоконравственнымнатомоснованиичтотолько
тотдостигаетвысшегонравственногогосовишенствактопрошелчерезглубочайшииебездныгрехо

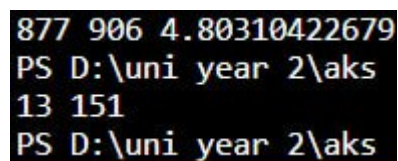
вности мы игнорируем одно изображение в эднравственным является человек реагирующий ужас
авнутренне испытываемое искушение при этом ему не поддается сжтоже по переменно то грешит
тораскаиваясь ставит себе высокие нравственные цели то легко прекнуть в том что он слишком
удобно для себя строит свою жизнь он не исполняет основного принципа нравственности необходи
мости отречения в то время как нравственный образ жизни в практических интересах всего челове
чества этим он напоминает варваров эпохи переселения народов варваров убивавших затем ка
в хся в этом так что пока я не становилось техническим примером расчищавшим путь к новым
твам так же поступали в анрозный этап делка совестию характерная русская черта достаточн
обеславения конечный итог нравственной борьбы достоевского после испуленной борьбы во имя
примирения притязаний первичных позывов индивида требования человеческого общества он
ынужденно регрессирует к подчинению мирскому духовному авторитету поклонению царю хри
стианскому боготу русскому мелкому душному национализму к чему менее значительные умы при
шли с го
разд меньшими усилиями чем он в этом слабое место большой личности достоевский упустил возм
ожность стать учителем и освободителем человечества и присоединился к тюремщикам культур
а будуще го не многим будет ему обязана в этом по всей вероятности проявился его невроз иза ко
ого они были осуждены на такую неудачу помощи постижения и силе любви к людям былоткрыт
угой апостольский путь служения нам представляется отталкивающим рассматривание достое
вского как качества грешника или преступника но это отталкивание не должно основываться на бы
ательской оценке преступника выявить подлинную мотивацию преступления не годно для преступ
ника существенны две черты безграничное себялюбие и сильная деструктивная склонность
общим для обеих черт предпосылкой для их проявления является безлюбивость нехватка эмоциональ
ноценного отношения к человеку тут сразу вспоминаешь противоположное этому у достоевского
го большую потребность в любви и его огромную способность любить проявившуюся в его сверхдобр
оте и позволяющую ему любить и помогать там где он имел бы право ненавидеть мстить на пример
по отношению к его первой жене и ее любовнику но тогда возникает вопрос откуда приходится соблазн
причисления достоевского к преступникам ответ изза выбора его сюжета это преимущественно
насилие и убийцы эгоцентрические характеры что свидетельствует о существовании таких скл
онностей и в его внутреннем мире а так же изза некоторых фактов его жизни страсти его казартны
ми грамм может быть сексуально горастления незрелой девочки и исповедь это противоречие разреш
ается следующим образом сильная деструктивная устремленность достоевского которая могла бы
сделать его преступником была в его жизни направлена главным образом на самого себя вглубь
места того чтобы изнутри таким образом выразилась в мазохизме чувстве вины в сетаки в его лич
ности немало с адистических черт выявляющихся в его раздражительности мучительстве не тер
пимости да же по отношению к любимым людям а так же в его манере обращения с читателем так
в мелочах он с адистов не вважном с адист по отношению к самому себе бесследовательно мазохист
и э
то мягчайший и добродушный и всегда готовый помочь человек в сложной личности достоевского
мы выделили три фактора один количественный и два качественных его чрезвычайно повышенная
ффефективность его устремленность к перверзии которая должна была привести его к адо мазохиз
му или сделать преступником и его не поддающееся анализу творческое дарование такое сочетание
вполне могло бы существовать без невроза ведь бывают жестопроцентные мазохисты без наличи
я невроза в по отношению к силе притязаний первичных позывов и в противоборствующих им торм
жений присоединяя сюда возможность сублимирования достоевского во все что можно было бы отне
сти к разряду импульсивных характеров но положение вещей затемняется наличием невроза не обяза
тельно го как бы сказано приданных обстоятельствах но все же возникающего тем скорее чем на
сыщеннее осложнение подлежащее с стороны человеческого преодоления невроза то только зна

кого ця така й синтез не удался, що оно при этой попытке не платилось своим единством в чем же в строгом смысле проявляется не в роздосто евский называл себя сам и другие так же считали его эпилептиком на том основании что он был подвержен тяжёлым припадкам сопровождавшимся потерей сознания судорогами и последующим упадочным настроением. Весьма вероятно что эта так называемая эпилепсия была лишь симптомом его не в роза который в таком случае следует определить как истероэпилепсию то есть как тяжёлую истерию. Утверждать это с полной уверенностью нельзя по двум причинам во первых потому что даты анамнеза и не зических припадков так называемой эпилепсии до того еско го недостаточны и ненадёжны а во вторых потому что понимание связанных с эпилептикой идиом припадками болезненных состояний остаётся неясным.

Треба ще зробити розпізнавач російської мови. Ми зробили це за допомогою функції знаходження ентропії тексту `entropy`: теоретична ентропія для російської мови становить приблизно 4,47186, тому будемо шукати розшифрований текст, ентропія якого відрізняється від теоретичного значення менше всього:

```
val_4_47_approx=1000
for x_0,x_1,y_0,y_1 in all_combinations:
    a,b=find_keys(top_5_plaintext_Xi,top_5_chiphered_Yi,x_0,x_1,y_0,y_1)
    dec=decipher_bi(a,b)[: ]
    entr=entropy(dec,find_freq(dec))
    temp=abs(4.471-entr)
    if temp<val_4_47_approx:
        val_4_47_approx=temp
        closest_a=a
        closest_b=b
print(closest_a,closest_b)
```

Тобто ця ділянка коду видає нам ключ, при розшифруванні яким знаходиться текст, ентропія якого відрізняється від теоретичного значення менше всього:



```
877 906 4.80310422679
PS D:\uni year 2\aks
13 151
PS D:\uni year 2\aks
```

Справді вийшов наш ключ (13, 151).

Висновки: у ході лабораторної роботи було розглянуто метод криптоаналізу шифру афінної біграмної підстановки. Було досліджено, що для розшифрування тексту, зашифрованого шифром афінної біграмної підстановки, доцільно використовувати частотний аналіз: знайти 5 біграм, які найчастіше зустрічаються в шифртексті і спробувати всі комбінації співставок цих 5 біграм з п'ятьма біграмами, які найчастіше зустрічаються в мові, розв'язуючи системи рівнянь для знаходження можливих ключів.