Міністерство освіти і науки України
Національний Технічний Університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Криптографія

Комп’ютерний практикум №3
Варіант 14

Виконали:
Студентка групи ФБ-82
Муртазіна Аміна
Студент групи ФБ-84
Вацик Максим

Перевірив:
Чорний О.М.

Київ - 2020

Мета комп'ютерного практикуму

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

Постановка задачі

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. Нижче наведена реалізація розв'язування лінійних рівнянь за модулем:

```python
def euclid_gcd(a, b):
    if a == 0:
        x, y = (0, 1)
        return (b, x, y)
    d, x1, y1 = euclid_gcd(b % a, a)
    x = y1 - (b // a) * x1
    y = x1
    return (d, x, y)

def inverse(a, n):
    if (a < 0):
        a += n
    d, x, y = euclid_gcd(a, n)
    if (d == 1):
        return x
```

```python
def solve_equation(a, b, n):
    x = list()
    d = euclid_gcd(a, n)[0] % n

    if d == 1:
        a_inv = inverse(a, n)
        x.append(a_inv * b % n)
        return x

    if b % d == 0:
        a1 = a // d
        b1 = b // d
        n1 = n // d
        x0 = solve_equation(a1, b1, n1)[0]
    (*) for i in range(0, d):
            x.append(x0 + i * n1)
        return x
    return -1
```

Як можна побачити з **(*)**, функція *solve_equation()* також враховує випадок, коли рівняння має більше одного розв'язку і повертає їх усі: x_0, x_0+n_1, x_0+2n_1,… $x_0+(d-1)n_1$

2. 5 найчастіших біграм запропонованого шифртексту(наведений нижче) можна подати у вигляді Таблиці 1:

Біграма	Кількість	Частота
аж	61	0.00924
жх	58	0.00879
цп	50	0.00757
шы	49	0.00742
ки	47	0.00712

Таблиця 1

```
ыенжийбжфзьеьжхфцрйишсвкрьзпцпьжэхххмжьрпймебжцыысзхяирхлыысчсоззехаыьиэтктяцпьжвжажегажхыпжфушыфмуяшззпокскфиэияйки
юозйщхуклихкуэпбжщнйкыюббяшыиотячззеоахзхнллохцппйежньедвьыбьхйщхцклихкевщьямккезцфтхщыпбнжнпцьжктйащбьвкэлфчьошжхл
фычзчсскфизхяйийкищибйтхкиыжнеихйххиегажййяйозшымжсщрщарийслдмяйпмоззеткщьйлытфцжсктауумйкищэийцпчлмжюэийбжцпмжаювк
щечсчеюифптячпыобжйэийцпчлййййпжфурмфмдвчпчфохшсэьвачпфтфпуушыжирмсяьпссчыхяхзгыэрчеыззпуеьыжьвачпагажньедвьыеспжфу
зхфмдвфэгюшкгйэхбжвжмвфпхыдэгюеыюлпжфурмфмдвкрчпийпзшйжмжкэчзпшзсыщйеыьпшзьермэгажшэгупжаияйкифяхзгышаюпущуьцумйрмрж
ывкинмбьюбдмынныжымййнжажпмьщбьвкэлфчхйбщыаызцибжшщеьесчпрмюцнжмжжмфзннезцихржфеымжбьхябжтхахэежмфзийсиыпхсфпхсхзтяфт
еьидйййпжьжфйкиащбьвкфйкишсщщьхбэфтмйййбямщгищрчефйюйзктфчеаьиоеыиотячзхювавкрменщршзчкшыпйевщьдимжямшыеьимщхлыщйчсще
чжххаьпризхяжнихибьчеажжяткзуеыкхйбжфзннзпрэдэежьжйиыажьчырйыкщьдмьеесщййсрмхкажегщефйффтхщычщбьвкэлфчцтбжслхихюип
фтийсиажихливжрьгюхсзхпжтаяжнидвьлсажьчыхсозчячеюибйкиэеьжьожйфйяфтхщычщбьвкэлфчцтямжхмиуахзхнуйхжфщыеыкхйзхяйийкиьс
евщьеыуюесьпчзфпфэлжяйипьобьщжрьгюткеыщтййтаяжнивжфмчжьжтаейййхслдвьлмйтхаинжажпмхаызфкрщкыхсхжцпылкичыьевжаььыжжеьхс
мжхатфзпцпьжеьидвацюмотфчеэйярцьихнрпйлрхзнгчзхффибжшщоххэдэежьжйихидмьлпфтяктфтяшотяжжпгжкцпьжххшехачфцьгюпжяйййха
тфзпысрйаэтфкххыбжшщохшеьжщпупюеягчпбжнжвытфтфжхпхьжучьорймпиохыфслпмжфщыеыкткезфзхяпбжияанябйыкхжчйартхюичжщвфэхзчп
щпюеягбжыешсчсшыюлвжнжчжюидмьлфеажчзчетящьяхкищртявжуэткмжвсченжыенжежпжэхцэслджмнжчжюидмьлпкяотячзхыжршыуищеажывнж
бйзхржежжфтярмцювкхяшыюлеьидчышыжрлжвидвщрчеызезчеупюеягбьшшыажьртхюичжщвйхпжуфшжнжчжюидмьлурчеаьфтихзхохажешщьйкще
ажчзкцюилквфтяжжнжчжюидмьлужцпезсыуйфэхзчпзпюеягжхчотячзчетжнеесййнызизихлибжфпцэгуумяфтяхыбьчызумйиаызйхкиэхдвньхсьп
тффэгуумяфтядзвкмжкржхщзббжигрщеезажцруужьиоажхыьщлжяхюоажхыщжтотячсчеюиюйийцплжчэпхрьцэхювктяткщпдэюйзкуймйчжбьхяцп
вкфкьйьеырпймщфмчжажлэчпцьхскжлсшыщйыехффияйшебжхжпычеюищемзхымжцпхюеыэпхймйтхаиевщьсфтхщычщбьвкэлфччсихаяьтмйрвйхки
эхшеьыцжпгжкцпьжххьгажйхслюишйежкизхшхдыщртяшиаххимйтххыфщыеыкткезфпуйежйхслюиырлжщеяжфляыщювкщечсцжыяшзйгажхычыышщр
элтпйхмйчжчыцюзеьхщзббэйежлкффзпуеэетямждеажлжрмдзвкмжкржхщзббжиякюеьхщзьзмйтхыеесхсрщкыхсскьпщрфэгюшкллевщьйыщжтотя
чсчедвкртхсихждвпжуфцибьхябьчычсзпсыткщйжхрждмуитхаиньщрчеяыогщвинжщыйгажевщьйхждзйнезьлсямщеждеажлжрмевщьаьхаткез
быщебщазшыюлйяшзкжсктауумйкиьыйгажкржхщзббжиякюеьхщзьзййтаяжнивжцптрийаяьщаззпщпояхзежюйощненжежххчйьхшрчпхсйыхкуювж
гычедвфмцплжежщебжцыышыюлкржхщзббживыхфткцьчзфпьцажххчйоншымжййьжнсуумжхыбьхятхахуяэлпжцпхушыюлипфтжйхибьтягуйзьеткнж
цплжгенжяфжащькишрлжкхещлйяйывкиожямэиньысуэтффияйрвьыткхтйипшжюйжхзифкийохащбьвкэлфчхфчеалтмхххищвцпдэыбфзуумжцпчббь
шшьехжыеслюишюжрийейкибицпийржхххкигьгюийьйкибиарфпцрпймпщььзьлщпхзрэтфткцьчзшсжявязпдэщемйтхдпщрпйкычияйшпфтбьдэюирй
уэфтжйяэчеюинжажжхчашяезгйгщьжнсуумжцпсыщрчеийреыкшымжчюэпуешювяшзфибжажгщхыйийзбоифйежщпхзрэчеьжхшеырйиыкцьщпуеырщь
хякржхщзббжиегажхыйхслыяшзхскржхщзббжиауьеьжххшеырйиыкцьщпуеырщьхяеьидхсфпцжнесиьхьпипхюеыэпюлчйщвэхбжфйныысфяэляжул
чыдиоззехаэеэйфыщпшзсыысфкржывюжюфцьтяшыйнхищвныдэхсщйййныдэхсщйбжхрэнчзшруюзхнжаидвьлшьвяннмжбьфкьпцпьжхххищыткртрйи
ыовкьйежржахохрхвжежржывюжежщзвяшзфшвфжащькициуэнншыюлбжчпмжьйкинфтхщыфтфзвачеюиевщьзпфтшэчпцьфтхыбьхюзхшечкткийзлбь
хйэхщзуулпуухаызщпдэуиывpмфпцрпйкышстфьжкящьяхдвьлчпкияжжлдвжйымхякиййммйхияйьлнмвинышрпйжхбьшотячзщпдэбйуювашгшымжхю
еыэпхсцурщчйрйжхаитахяесхювкаьдэесфаезесчыхявкллшсжкийяйкицрхскидвьлихлиьрьпщьсщзфхкяйцпхыткфтвиныщэчпцьпбзхмйьзьлбж
чйцпшрпйлжйучзыеажоущрийгычтвинычбажывнжцямщежгжсеьхмжшэчиппийюыгюзхрйкивсзехыщпххевщьжхныквезфпцжлычихрхзслшптффэчп
цьуйбьхяищмххчжихаяхсйсзехыжаюптжрьгюйжбыжхыеыкшымжаухюкиципешсфяталжмйэйфйдеткщьйлыхычияйуктйнйлкмопжрьхыжхшищиэб
мкцэфсщьюихылпэнезтйхлэйегажйхажхыщебжцыьзпьжфуйзхныйгшыхйщебьвкфйкищьтяйгшзткэгьенжежцияйуямщгихяталжмйэйхиэбржявйа
хигышсииьжххнйлычеюиейпьчедвчйфыфтежкхевщьийыишешйщхдвзхйхлкюйэйзакьертяцьтфшыгювяхызхяйийххшеыжнйщхдвыеьеьжцияйрвщи
хитычщпжцпткщьщпуечкажегажсяшзеыфиптфщгажчсбьхяирхмжфкихнжврхзуушыцизхяжнибеэпщрщьупчпзхлжнэчпцьтцкщьшышсжатфхсцэ
чпцьтхыцпийаишеыжпзвфтяьпшзуеыктзпофтхщычщбьвкэлфчцтшгщпвкыияктййхэйчсхзтятфтфжхпхбжфпфацюйсцпьжбыхкшфтяфтоззехачя
элйиежозщэийцпчлнемйтхщщцпкрлибьтяхзяхчяшзцжсктауумйкиырийреьхщзэпсыхкуювжгыысхыжххрцьчячзьлбжцплжбэфтьжыеыочсшыюльа
хзхньокяеыцтыэхзржывкизибьюбажцяэлбьхйкяважьчывкцюмйбьффчптkчзыеаьэгчыщранмжажиуьеыкшырмчэчпцьщйхыныезййбжмьвкэпьлев
щьйыфияйлычпдэхйийхигиуюмжпзвфтяжьцпчйлыщйхжрьгюесциюзхахсхжывпияйлычпдэхйнжажпмчэдэхыбжкиэхуажьчывяхзгышаызшртячтцп
ьжххдвзхеьиддитаэхнщдвхфыбгыллчйфыжрфэфтмжхаюеаьуйвщэйьйцпшихкчйненжбэхзэекйщщхячышыхйпжлжгижхпжцпмжмйдеыкткезчыжрпй
жхчсшычлшэчпцьяохыйййфмххфйейфмхитямжвиьжяифыцйпьжфтфхыжьтячйкящрийреьхщзьзьлпзвфтяшыцпыщфччсщплжахэйывмжпзвфтяжьрмяю
земйтхлыщйшсжатхежмйьыюлчйкяхаызфкцпийсинжажпмыочпщибьфктячзфкфсннчшыхйевщьеыткдзжачыхяннхйежямтмхххижхпжцпмжэгжкцпьж
ьжоыхсяйцпшсзуцэшртямжуихишсмофйсехзритажхорьпжхшрвктхшрлжуихибжкккзшыюлюгьедвхфсхифшзжрьпжхшрвктхчюзхмзнашифатхежкх
кычеюийхсяшзеырмчиюатхежмйьыюльжкяшидылпсызеьждерйяыткьтбьфяшзэшщьйкфкпьжфхсяйцпцйежыеаььпчзхушыжирмсфмщоысфяьпссфа
тхежкхрлхфуюдикавкфйкищжбпшушзяожхржыкаььппйаияйрвхйежыеаьэгезскячшыкиоеньеажвжньзушырмяяьпссцэчпцьяохыбжаичжцпьсеь
иджжсщохуфжхвжэйшьшзффциьжыеыочсшыюлярпйзкфяшзскфиаидзгюесшрцжоыхскртхнщьжкяшиахюнхйьлфкуюлкффнщдмьщбйихяйлыщйкяеыюл
ржывкимннжуатфвяшзшынжажпмхяхзгышаызфаюпокуэцьхсььшсшышжюэпмдмчйкящрпйзкфяшзчпрйдмкржхщзббжияжлхоччыуэьожхржьхащяйрв
ьйлыяобьчпфкбьцуййежщеымшхфюзпчплжахэйывpмхатхежкхийкичящрлпишщтньедвьыечыьоихxпеыиоевщьажывнжййныезажежфпчпесбяцй
гщбжоычечзьофйсехзрицплжчзшрйимйчрьпжхшрвктхфмчжажзфткуйтйчжюлксжьихьрьплжцяшыхгажбьфяшззуьеаьфишечявкмжржахохаигщви
ихаитйтхэйаинжажпмялшихищвмышсехфптяхкэпояьеэпяогщвинжяцажежтйтхфмхицкшзыгдтьйвьгюцьшыщихыйййнызфптkфзхяцпшиьптфщгаж
юйийцпезшруйежбьцэгюкрчеыззптьхаэпкижушыжинеевжярмаимйдваизхлхоччыоцюирхжмщьхаэпкинмэйгпмщоычтящсьвачпйыьехизхскуйгр
хзткчыщжлыцюзхьгажскячшыкийкцпийюиюнцтхфченььеажвжележгхцсзуцэткскфиаибжржжхаиыгажхжрьеырмчэййгщнгшыцэщечефййхаифмхи
чпкхххшсщйгщхювахзхнхймйрвгифмхичпощыхшсэьтящпшзьсшжлыцюзхьгажихяйлыщйбжазеызюкхкичкуюлкффезщеуеьжчсшьващгчсцижкшзыг
чзфажьжинщньедвьыйсшыхншынщтпхзрэхывайсвфщжлыцюзхьгажьхюфмйкржхщзббжидщихтмххфйгщбжмыффшызщяйрвьйкищруйежьжфйталжих
зхтянщаьпоаызеыжрхзткчыкрйилхщзшыважьжилыллбжшилычедвшрчпхскрпйзаызьжчоычшыскфиврлпэньеыкхйврфияйрвьсфкбжцыхкуюььзп
чзьлопхсмдчзеыаьцрыгьенжгщзхцплжшыюбшэчпцьхсхыямыоезхюйэйзакьахшрщеезьжцпцьбйлыщйяищвэхскуйгщзхцпвккиощрьзпиэдэхызх
тмххукшзцэтфхсзеэйжхихмзхфнжихмсезчщуихиьызумжфптаюемйтхдвьхмсмжежпжрьвяйсезевщьцэдэзхчжжмтаипхсйхржюигецх
```

3. На цьому кроці нам знадобилось співставити найчастіші біграми російської мови -`'ст'`,`'но'`, `'то'`, `'на'`, `'ен'` - та шифртексту - `'аж'`,`'жх'`, `'цп'`, `'шы'`, `'ки'` - і знайти можливих кандидатів на ключ для кожного співставлення(пару А і В). Крім того, для автоматизації роботи було створено розпізнавач російської мови, робота якого ґрунтується на аналізі частих літер російського алфавіту(їхніх частот). Спочатку розшифруванням тексту займається функція *decrypt_text(),* яка, по суті, розв'язує систему лінійних рівнянь з двома невідомими. Після розшифрований текст подається на вхід до функції *detect_lang()*, яка перебирає всі літери тексту та виділяє топ 6 найчастіших. Якщо цей топ шість не складається з літер `'о'`, `'а'`, `'е'`, `'и'`, `'н'`, `'т'` – очевидно, розшифрований текст не є змістовним, і цей варіант відкидається. Функція *detect_lang()* буде розшифровувати текст, що має найчастішими вищезазначені літери АЛЕ в будь-якому порядку(тобто, оаеинт, наоети, аенито і тд). Таким чином, ми максимально мінімізуємо кількість розшифрованих текстів, серед яких обов'язково буде правильний та змістовний. Незалежно від того, підійшов нам текст чи ні, було реалізовано вивід повідомлення з найчастішими літерами розшифрованого тексту та можливими кандидатами на А та В(нижче наведений приклад виведення результату)

```
Rejected text candidate A:702 B:585. Top chars are: рыайсн.
Rejected text candidate A:509 B:134. Top chars are: озуюти.
Rejected text candidate A:575 B:682. Top chars are: джоьшк.
Rejected text candidate A:406 B:531. Top chars are: лмцвро.
Rejected text candidate A:927 B:81. Top chars are: щтишцф.
Rejected text candidate A:337 B:657. Top chars are: азтпдя.
Rejected text candidate A:207 B:393. Top chars are: стьчна.
Rejected text candidate A:569 B:108. Top chars are: вцебту.
Rejected text candidate A:795 B:907. Top chars are: гсаоды.
Rejected text candidate A:494 B:621. Top chars are: нытшмх.
Rejected text candidate A:677 B:830. Top chars are: ргниэт.
Rejected text candidate A:951 B:455. Top chars are: сиоьчт.
Rejected text candidate A:692 B:343. Top chars are: уткенх.
Rejected text candidate A:543 B:371. Top chars are: онфтрч.
Rejected text candidate A:609 B:919. Top chars are: хбетдп.
Rejected text candidate A:440 B:768. Top chars are: энпирх.
Rejected text candidate A:34 B:47. Top chars are: измтск.
Rejected text candidate A:503 B:68. Top chars are: аытлгу.
Rejected text candidate A:373 B:765. Top chars are: ращуже.
Rejected text candidate A:735 B:480. Top chars are: блащфт.
Rejected text candidate A:166 B:182. Top chars are: пдтнца.
Rejected text candidate A:763 B:596. Top chars are: ентудф.
Rejected text candidate A:946 B:805. Top chars are: офщртч.
Rejected text candidate A:259 B:430. Top chars are: пдацнт.
Rejected text candidate A:269 B:746. Top chars are: мхтньш.
Decrypted text with A:10 B:52. Top chars matching: оеиант.
```

```
Rejected text candidate A:66 B:554. Top chars are: тлгэоа.
Rejected text candidate A:858 B:403. Top chars are: тыуобш.
Rejected text candidate A:452 B:643. Top chars are: тншщоб.
Rejected text candidate A:418 B:914. Top chars are: томзуа.
Rejected text candidate A:831 B:703. Top chars are: тявбчщ.
Rejected text candidate A:232 B:418. Top chars are: тзмура.
Rejected text candidate A:624 B:120. Top chars are: талэго.
Rejected text candidate A:458 B:256. Top chars are: тцпаяз.
Rejected text candidate A:183 B:215. Top chars are: тсзлни.
Rejected text candidate A:457 B:801. Top chars are: тжынак.
Rejected text candidate A:467 B:156. Top chars are: тдфгун.
Rejected text candidate A:198 B:689. Top chars are: тьемня.
Rejected text candidate A:895 B:620. Top chars are: охтдбю.
Rejected text candidate A:792 B:56. Top chars are: ицкохт.
Rejected text candidate A:386 B:296. Top chars are: эьжоиц.
Rejected text candidate A:352 B:567. Top chars are: лтаоый.
Rejected text candidate A:130 B:471. Top chars are: аурхшс.
Rejected text candidate A:362 B:883. Top chars are: днаекч.
Rejected text candidate A:754 B:585. Top chars are: баечьт.
Rejected text candidate A:588 B:721. Top chars are: вятшна.
Rejected text candidate A:778 B:959. Top chars are: ношфят.
Rejected text candidate A:274 B:793. Top chars are: хчивсы.
Rejected text candidate A:284 B:148. Top chars are: пэглтн.
Rejected text candidate A:15 B:681. Top chars are: сжтлия.
Rejected text candidate A:103 B:300. Top chars are: оенаир.
Rejected text candidate A:169 B:848. Top chars are: щцвокн.
Rejected text candidate A:555 B:937. Top chars are: хфортк.
Rejected text candidate A:521 B:247. Top chars are: дусшой.
Rejected text candidate A:729 B:285. Top chars are: аджлия.
```

вскорепослесвоегоприемавбратствомасоновпьерсполнымнаписаннымимдлясебяруководствомотомчтоондолженбылделатьвсвоихимени
яхуехалвкиевскуюгубернюгденаходилась большаячастьегокрестьянприехаввкиевпьервызвалвглавнуюконторувсехуправляющихиобя
снилимсвоинамеренияижеланияонсказалимчтонемедленнобудутпринятымерыдлясовершенногоосвобожденіякрестьяноткрепостнойзав
исимостичтодотехпоркрестьяненедолжныбытьотягчаемыработойчтоженщиныдетьминедолжныпосылатьсянаработычтокрестьянамдолж
набытьоказываемапомощьчтонаказаниядолжныбытьупотребляемыувещательныеанетелесныечтовкаждомимениидолжныбытьучрежденыбо
льницыприютыишколынекоторыеуправляющиетутбылииполуграмотныеэкономыслушалииспуганнопредполагаясмыслречивтомчтомолодой
графнедоволенихуправлениемиутайкойденегдругиепослепервогостраханаходилизабавнымшепелявеньепьераиновыенеслыханныеимис
ловатретьинаходилипростоудовольствиепослушатькаговоритбаринчетвертыесамыеумныевтомчислеиглавноуправляющийпонялиизэт
ойречитокакимобразомнадообходитьсясбариномдлядостижениясвоихцелейглавноуправляющийвыразилбольшоесочувствиенамерениям
пьеранозаметилчтокромеэтихпреобразованийнеобходимобыловообщезанятьсяделамикоторыебыливдурномсостоянииинесмотрянаогром
ноебогатствографабезухогостехпоркакпьерполучилегоиполучалкаговорилитысячгодовогодоходаончувствовалсебяграздоменеебе
огатымчемкогдаонполучалсвоитьтысячотпокойногографавобщихчертахонсмутночувствовалследующийбюджетвсоветплатилосьоколот
итысячповсемениямокололотитысячстоилосодержаниеподмосковнойморковскогодомаикняжоноколотитысячвыходилонапенсиистолько
женабогоугодныезаведенияграфиненапрожитьепосылалосьтысячпроцентовплатилосьзадолгиоколотитысячпостройканачатойцерквис
тоилаэтидвагодаоколотитысячстальноеоколотатысячрасходилосьонсамнезналкакипочтикаждыйгодонпринужденбылзаниматькромет
огокаждыйгодглавноуправляющийписалтоопожарахтоонеурожаяхтоонеобходимостиперестроекфабрикизаводовитакпервоеделопредст
авившеесяпьерубылотоккоторомуонменеевсегоимелспособностиисклонностизанятиеделамипьерсглавноуправляющимкаждыйденьзани
малсяноончувствовалчтозанятияегонинашагнеподвигалиделаончувствовалчтоегозанятияпроисходятнезависимоотделачтоонинецеп
ляютзаделоинезаставляютегодвигатьсясодной стороныглавноуправляющийвыставлялделавсамомдурномсветепоказываяпьерунеобход
имостьуплачиватьдолгиипредпринимательновыеработысиламикрепостныхмужиковначтопьернесоглашалсясдругойсторонывпьертребовал
приступлениякделуосвобожденияначтоуправляющийвыставлялнеобходимостьпреждеуплатитьдолгопекунскогосоветаипотомуневозмо
жностьбыстрогоисполненияуправляющийнеговорилчтоэтосовершенноневозможноопредлагалдлядостиженияэтойцелипродажулесовко
стромскойгубернииипродажуземельнизовыхикрымскогоименьяновсеэтиоперациивречахуправляющегосвязывалисьстакоюсложностьюпр
оцессовснятиязапрещенийистребованийразрешенийитпчтопьертерялсяитолькоговорилемудадатакисделайтепьернеимелтойпрактиче
скойцепкостикотораябыдалаемувозможностьнепосредственновзятьсязаделоипотомуоннелюбилегоитолькостаралсяпритворитьсяпер
едуправляющимчтоонзанятделомуправляющийжестаралсяпритворитьсяпередграфомчтоонсчитаетэтизанятиявесьмаполезнымидляхозя
инаидлясебястеснительнымивбольшомгороденашлисьзнакомыенезнакомыепоспешилипознакомитьсяирадушноприветствоваливновьпри
ехавшегобогачасамогобольшоговладельцагубернииискушенияпоотношениюглавнойслабостипьератойкоторойонпризналсявовремяпр
иемавложутожебылитаксильнычтопьернемогвоздержатьсяотнихопять целыеднинеделимесяцыжизнипьерапроходилитакжеозабоченноиз
анятомеждувечерамиобедамизавтракамибаламинедаваяемувременіопомнитьсякакивпетербургевместоновойжизникоторуюнадеялсяпо
вестипьеронжилвстожепрежнейжизньютольковдругойобстановкеизтрехназначениймасонствапьерсознавалчтоонненеисполнялтогокот
ороепредписывалокаждомумасонубытьобразцомнравственнойжизниииизсемидобродетелейсовершенноневеимелвсебедвухдобронравияилю
бвиксмертионутешалсебятемчтозатоонисполнялдругоеназначениеисправлениеродачеловеческогоиимелдругиедобродетелилюбовькб
лижнемуивособенностищедрость весной годапьеррешилсяехать назадвпетербургподорогеназадоннамеревалсяобехатьвсесвоименьяи
личноудостоверитьсявтомчтосделаноизтогочтоимпредписаноивкакомположенииинаходитсятеперьтонародкоторыйвверенемубогомик
оторыйонстремилсяоблагодетельствоватьглавноуправляющийсчитавшийвсезатеимолодогографапочтибезумствомневыгодойдлясебяд
лянегодлякрестьянсделалуступкипродолжаяделоосвобожденияпредставлятьневозможнымонраспорядилсяпостройкойвовсехименияхб
ольшихзданийшколбольницприютовдляприездабаринавездеприготовилвстречинепышноторжественныекоторыеонзналнепонравятсяпь
еруноименнотакиерелигиозноблагодарственныесобразамиихлебомсольюименнотакиекоторыекаконпонималбаринадолжныбылиподейст
вовать награфаиобмануть егожнаявеснапокойноебыстроепутешествиеввенскойколяскеиуединениедорогирадостнодействовалинапье
раименьявкоторыхоннебывалещебылиподноживописнеедругогонародавездепредставлялсяблагоденствующимитрогательноблагодарнымз
асделанныеемублагодеяниявездебылиствечикоторыехотяиприводилисмущениепьерановглубинедушиегоовызывалирадостноечувство
водномместемужикиподносилиемухлебсольюобразпетраипавлаипросилипозволенияувчесть егоангелапетраипавлавзнаклюбвиблагода
рностизасделанныеимблагодеяниявоздвигнуть насвойсчетновыйприделвцерквидругомместееговстретилиженщиныгрудными детьмиб
лагодаряегозаизбавлениеоттяжелыхработвтретьемимненьеговстречалсвященникскрестомокруженныйдетьмикоторыхонпомилостямгр
афаобучалграмотеирелигиивовсехименияхпьервиделсвоимиглазамипоодномуплануводвигавшиесяиводвигнутыеужекаменныездания
больницшколбогаделенкоторыедолжныбылибыть вскоромвремениоткрытывездепьервиделотчетыуправляющихобарщинскихработахумень
шенныхпротивпрежнегоислышалзатотрогательныеблагодарениядепутацийкрестьянвсинихкафтанахпьертольконезналтогочтотамгдее
муподносилихлебсольистроилиприделпетраипавлабылоторговоеселоиярмаркавпетровденьчтоприделужеистроилсядавнобогачамимужи
камиселатемикоторыеявились кнемуачтодевять десятыхмужиковэтогоселабыливеличайшемразорениионнезналчтовследствиетогочто
пересталипоегоприказупосылать ребятницженщинсгрудными детьминабарщинуэтисамыеребятницытемтруднейшуюработунеслинасвоейп
оловинеоннезналчтосвященниквстретившийегоскрестомотягощалмужиковсвоимипоборамиичтособранныекнемуученикисослезамибыли
отдаваемуюзаболышиедень гибылиоткупаемыепослеянионнезналчтокаменныенеплануздания ввоздвигались своимирабочимиивеличав
илибарщинукрестьянуменьшеннуютольконабумагеоннезналчтотамгдеуправляющийуказывалемупокнигенауменьшениеполоеговолеоброка
наоднутретьбыланаполовинуприбавленабарщиннаяповинностьипотомупьербылвосхищенсвоимпутешествиемпоименьямивполневозврат
илсяктомуфилантропическомунастроениювкоторомонвыехализпетербургаписалвосторженные письмасвоемунаставникубратукаконна
зывалвеликогомастеракаклегкокакмалоусилиянужночтобыделатьтакмногодобрадумалпьерикакмаломыобэтомзаботимся

Висновки

В ході роботи основною метою було опанування навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки та опанування прийомами роботи в модулярній арифметиці. Трохи

складно було осмислити роботу афінного шифру на прикладі саме біграм(а не одиночних літер, як ми звикли). Реалізація функцій роботи в модуляційній арифметиці – алгоритм Евкліда та пошук оберненого – не викликали непорозумінь. База для створення розпізнавача російської мови також була обрана одноголосно, бо здалась нам найбільш простою в реалізації та доволі ефективною. В результаті з отриманим ВТ ми також маємо пару **A=10** та **B=52**, яка є розв'язком системи лінійних рівнянь з нашим ШТ та ВТ