НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Лабораторна робота №3 дисципліни

”КРИПТОГРАФІЯ”

Підготував:

студент групи ФБ-03

Заболотний Максим

Київ 2023

Тема роботи: Криптоаналіз афінної біграмної підстановки.

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. Реалізуємо необхідні підпрограми для обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда та розв'язування лінійних порівнянь.

```
from math_part import linear_cmp, euclid_extend
```

2. Знайдемо 5 найчастіших біграм запропонованого шифртексту а також задамо 5 найчастіших бішрам мови:

```
bi_dict = {}
for i in range(0, len(text), 2):
    j = i + 2
    if len(text[i:j]) == 1:
        continue
    if text[i:j] in bi_dict.keys():
        bi_dict[text[i:j]] += 1
    else:
        bi_dict[text[i:j]] = 1
result = zip(bi_dict.keys(), bi_dict.values())
result = sorted(result, key=lambda x: x[1], reverse=True)[:5]
founded_bi = [i[0] for i in result]
static_bi = ("ст", "но", "то", "на", "ен")
```

3. Створемо масив усіх можливих варіантів комбінації шифрованих та нешифрованих біграм:

```
def make_variants(bi1, bi2):
    variants = []
    for i in bi1:
        for j in bi2:
            variants.append((j, i))
    result = []
    for i in variants:
        for j in variants:
            if (i != j) and ((j, i) not in result) and (i[0] != j[0]) and (i[1] != j[1]):
                result.append((i, j))
    return result
```

4. Переберемо можливі варіанти та знайдемо кандидатів на ключ:

```
def found_keys(static, encoded):
    x = bi_to_num(static[0]) - bi_to_num(static[1])
    y = bi_to_num(encoded[0]) - bi_to_num(encoded[1])
    keys = linear_cmp(x, y, 31 ** 2)
    result = []
    if keys is not None:
        if len(keys) > 0:
            for key in keys:
                result.append((key, (bi_to_num(encoded[0]) - key * bi_to_num(static[0])) % (31 ** 2)))
        return result
```

```
keys = []
possible = make_variants(founded_bi, static_bi)
for i in possible:
    answer_keys = found_keys((i[0][0], i[1][0]), (i[0][1], i[1][1]))
    if answer_keys is None:
        continue
    for k in answer_keys:
        keys.append(k)
```

5. Дешифруємо текст кандидатами на ключ. Після кожної ітерації дешифрування, перевіряємо отриманий текст на наявність неіснуючих біграм і якщо таких немає, то повертаємо змістовний текст, що і є шуканим :

```
def error_check(text):
    bad_bi = ['аы', 'еы', 'уы', 'еь', 'эы', 'яь', 'ьь', 'ыь', 'эь', 'уь', 'оь', 'ыы', 'оы', 'юь', 'юы', 'яы']
    for bi in bad_bi:
        if bi in text:
            return False
    return True
```

```python
def decrypt_text(text, key):
    result = []
    for i in range(0, len(text), 2):
        if i >= len(text):
            break
        y = bi_to_num(text[i: i + 2])
        x = (euclid_extend(key[0], 31 ** 2)[1] * (y - key[1])) % (31 ** 2)
        result.append(num_to_bi(x))
    return ''.join(result)
```

```
Decrypted by: (300, 400)
Result: поздновечеромнаверандесиделколяичтотописалвтемнотебумагуитутолкомнельзябылоразглядетьвремяотвременионвосклицалагаилииэтотожезначитемувголовуприходилоещечтонибудьподходящеедляегоспискапотомдверьчутьстукнулаточновсеткуотмоскитовудариласьночнаябабочкалинашепнулауфманонаселярядомснимнакачеливоднойночнойсорочкенетоненькаякаксемнадцатилетняядевочкакоторуюещенелюбятинетолстаякакпятидесятилетняяженщинакоторуюуженелюбятноскладнаяикрепкаяименнотакаякакнадотаковыженщинывовсякомвозрастееслионилюбимыонабылаудивительнаяеетелокакиегособственноевсегдадумалозанеетолькоподругомуоновынашивалодетейиливходиловпередилеовкаждуюкомнатучтобынеуловимоизменитьтамсамыйвоздухподстатьнастроениюмужаказалосьонаникогданезадумываетсянадолгомысльтотчаспередаваласьотеголовыплечампальцамипретворяласьвдействиетакнезаметноиестественночтолеонесмогбыдаинехотелизобразитьэтокакимилибочертежамиэтамашинасказалаонанаконецненужнаонанамдаотозвалсяонноиногданужнопозаботитьсяиодругихявотвседумаючтотудавставитькинокартинырадиоприемникистереоскопическиеочкиеслисобратьвсеэтовместевсякийчеловекпощупаетулыбнетсяискажетдадаэтоиестьсчастьесочинитьтакуюхитруюмеханикудумалончтопускайучеловекапромоклиногишлиноетязваилиегомучаетбессонницаионворочаетсявпостеливсюночьнапролетидушуегогрызутзаботыавсеравнотвоямашинадастемусчастьекактамагическаякрупинкасоличтоброшенавокеанивечнорождаетсольиобратилавсеморевсолянойрастворктонерасшибсябывлепешкулишьбыизобреститкакуюмашинупустьемуответитнаэтотвопросцелыймирпустьответитвесьгородокпустьответитженалинасмущенномолчаласидярядомснимнакачеляхиеемолчаниеговорилояснеевсякихсловлеотожеумолкзапрокинулголовуислушалкаксвищетветервгустойлиствемогучеговязанезабывайговорилонсебеиэтотшелестлистьевтоженуженделятвоеймашинычерезминутуверандаопустелапустыекачелинеподвижноповисливтемнотедедушкаулыбнулсявоснеонпочувствовалэтуулыбкуудивилсяейипроснулсяполежалнемногоприслушалсяксебеипонялоткудаонавзяласьибоонуслышалнечтогораздоболееважноенежелипениептицилишелестмолодойлиствыкаждыйгоднаступалденькогдаонвоттакпросыпалсяиждалэтогозвукакоторыйозначалчтотеперьтоужлетоначалосьпонастоящемуононачиналосьвотвтакоеутрокогдактонибудьиздомочадцевилигостейплемянниксыниливнуквыходилналужайкуподегоокномиметаллическиеножиспицыкружаизвеняподушистойлетнейтравеприлежнообегалиеепокраямнасевернавостокнаюгназападописываявс
```

6. Дешифрований текст:

поздновечеромнаверандесиделколяичтотописалвтемнотебумагуитутолкомнельзябыло разглядетьвремяотвременионвосклицалагаилииэтотожезначитемувголовуприходилое щечтонибудьподходящеедляегоспискапотомдверьчутьстукнулаточновсеткуотмоскит овудариласьночнаябабочкалинашепнулауфманонаселярядомснимнакачеливоднойночной сорочкенетоненькаякаксемнадцатилетняядевочкакоторуюещенелюбятинетолстаякак пятидесятилетняяженщинакоторуюуженелюбятноскладнаяикрепкаяименнотакаякак надотаковыженщинывовсякомвозрастееслионилюбимыонабылаудивительнаяеетелока киегособственноевсегдадумалозанеетолькоподругомуоновынашивалодетейиливходилов передилеовкаждуюкомнатучтобынеуловимоизменитьтамсамыйвоздухподстатьнастр оениюмужаказалосьонаникогданезадумываетсянадолгомысльтотчаспередаваласьоте еголовыплечампальцамипретворяласьвдействиетакнезаметноиестественночтолеонес могбыдаинехотелизобразитьэтокакимилибочертежамиэтамашинасказалаонанаконец ненужнаонанамдаотозвалсяонноиногданужнопозаботитьсяиодругихявотвседумаючт отудавставитькинокартинырадиоприемникистереоскопическиеочкиеслисобратьвсеэт овместевсякийчеловекпощупаетулыбнетсяискажетдадаэтоиестьсчастьесочинитьта куюхитруюмеханикудумалончтопускайучеловекапромоклиногишлиноетязваилиегомучае тбессонницаионворочаетсявпостеливсюночьнапролетидушуегогрызутзаботыавсеравн отвоямашинадастемусчастьекактамагическаякрупинкасоличтоброшенавокеанивечно рождаетсольиобратилавсеморевсолянойрастворктонерасшибсябывлепешкулишьбыиз обреститакуюмашинупустьемуответитнаэтотвопросцелыймирпустьответитвесьго родокпустьответитженалинасмущенномолчаласидярядомснимнакачеляхиеемолчаниег оворилояснеевсякихсловлеотожеумолкзапрокинулголовуислушалкаксвищетветервгуст ойлиствемогучеговязанезабывайговорилонсебеиэтотшелестлистьевтоженуженделятв оеймашинычерезминутуверандаопустелапустыекачелинеподвижноповисливтемнотед едушкаулыбнулсявоснеонпочувствовалэтуулыбкуудивилсяейипроснулсяполежалнемного прислушалсяксебеипонялоткудаонавзяласьибоонуслышалнечтогораздоболееважноене желипениептицилишелестмолодойлиствыкаждыйгоднаступалденькогдаонвоттакпро сыпалсяиждалэтогозвукакоторыйозначалчтотеперьтоужлетоначалосьпонастоящем уononачиналосьвотвтакоеутрокогдактонибудьиздомочадцевилигостейплемянниксыни ливнуквыходилналужайкуподегоокномиметаллическиеножиспицыкружаизвеняподуши стойлетнейтравеприлежнообегалиеепокраямнасевернавостокнаюгназападописываявс

еменьшиеименьшиеквадратыкосилказвонкострекоталаизподножейбрызгалиголовкикл
еверараредкиезолотыеискрыуцелевшихпослесбораодуванчиковмуравьипалочкикамешкиос
таткипрошлогоднегопразднованиячетвертогоиюляобгорелыешутихиикусочкитрутан
оглавноезанейстлалсяпрохладныйчистыйпотоксочнойзеленойтравыдедушкеужепредс
тавлялоськаконащекочетегоногиохлаждаетразгоряченноелицонаполняетноздриизвечн
ымароматомвновьродившегосялетаиобещаетдамывсевсепроживемещецелыйгодвелик
оечудокосилкаговорилсебededушкакакойэтодураквыдумалчтоновыйгодначинаетсяперв
огоянварянадобылопоставитьдозорныхкараулитьросттравынамиллионахлужаекиллин
ойсаогайоилиайовыикакзаметятчтоонасозреладлясенокосавтосамоеутровместофейе
рверковфанфарикриковпустьначинаетсявеликаябурнаясимфониякосилокрезающихсве
жиетравынанеобятныхлуговыхпросторахвтотединственныйденьвгодукоторыйпонас
тоящемузнаменуетсобойначалолюдямнадобыбросатьдругвдруганеконфеттиинесерпа
нтинапригоршнисвежескошеннойтравыдедушкахмыкнулчтотоужбольнодолгуюфилос
офиюразвелвсталподошелкокнуивысунулсявласковыйсолнечныйсветтакиестьфоресте
рновыйжилецмолодойгазетчиккакраззаканчиваетряддоброеутромистерсполдингтаке
ехорошенькобиллсжаромкрикнулдедушкаивскореужесиделвнизуиуплеталприготовленн
ыйбабушкойзавтракиширокоеокнобылораскрытоижужжаньекосилкисловноподпевалоз
автракуотэтойкосилкинадушестановитсяспокойнеезаметилдедушкатытолькопослуш
айтеперьужнедолгонамееслушатьотозвалась бабушкаипоставиланастолгоркупшеничн
ыхлепешекбиллфорестерпосеетсегодняновыйсорттравыеененадобудеткоситьнепомн
юкактамонаназываетсяноонакаквырастетскольконужнотаксамаиостановитсяиболь
шенерастетдедушкасизумлениемуставилсянаженудовольноглупаяшуткасказалоннакон
ецидипосмотрисамбиллфорестерговоритэтоземленапользусказалабабушкаонужеприв
езновыесеменаонисложенызадомомвмаленькихкорзинкахнужновразныхместахвырыть
ямкиизасыпатьтудасеменакконцуг

Висновок

Виконуючи даний лабораторний практикум, я набув навички частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанував прийомами роботи в модулярній арифметиці, використовуючи підпрограми із необхідними математичними операціями, включно з алгоритмом Евкліда та лінійними рівняннями, знайдені ключі методом перебору текстів на змістовність та перевіркою на наявність в них неіснуючих біграм.