Лабораторна робота з криптографії №3

Виконав: Костюковець Остап ФБ-96

Варіант №5

Криптоаналіз афінної біграмної підстановки

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

Хід роботи

Завдання 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.

In [1]:

```
def gcd(a, b):
    p = [0, 1]
    gcd_val = b
    a, b = max(a, b), min(a, b)

    while b != 0:
        q = a // b
        gcd_val = b
        a, b = b, a % b
        p.append(p[-1] * (-q) + p[-2])

    return gcd_val, p[-2]


def linear(a, b, n):
    a = a % n
    b = b % n

    d, a_re = gcd(a, n)

    if d == 1:
        x = (a_re * b) % n

        return [x]
    else:
        if b % d == 0:
            solutions = []
            solutions_loc = []

            a1 = a / d
            b1 = b / d
            n1 = n / d

            solutions_loc = linear(a1, b1, n1)

            for i in range(0, d):
                for x0 in solutions_loc:
```

```
                    res = x0 + (d - i) * n1
                    solutions.append(res % n)

            return sorted(solutions)
        else:
            return None
```

Завдання 2

> За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

In [6]:

```
text = open("V5", "r").read().replace("\n", "")

bigram_frequency = {}
for i in range(0,len(text),2):
    temp = text[i:i+2]
    if temp not in bigram_frequency:
        bigram_frequency[temp] = text.count(temp) / (len(text))

print(sorted(bigram_frequency.items(), key=lambda item: item[1], reverse=True)[:5])
```

```
[('фш', 0.010433070866141732), ('вп', 0.008661417322834646), ('не', 0.007874015748031496), ('пу', 0.007283464566929134), ('ус', 0.007086614173228346)]
```

Завдання 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).

In [3]:

```
ru_RU = "абвгдежзийклмнопрстуфхцчшщыьэюя"

def encode_bigram(bi):
    val = ru_RU.index(bi[0]) * len(ru_RU) + ru_RU.index(bi[1])
    return val

# getting all possible pairs of bigrams cyphered-real
def all_pairs(cyphered, real):
  res = []
  for el1 in cyphered:
    for el2 in real:
      res.append((el2, el1))

  res2 = []
  for p1 in res:
    for p2 in res:
      if p2[0] not in p1 and p2[1] not in p1:
        res2.append((p1,p2))

  return res2

# finding mutual key from a pair of bigrams cyphered-real
def find_key(pair1, pair2):  # (y1, x1) (y2, x2)
  y1, x1 = encode_bigram(pair1[0]), encode_bigram(pair1[1])
  y2, x2 = encode_bigram(pair2[0]), encode_bigram(pair2[1])

  a = linear(y1-y2,x1-x2,len(ru_RU)**2)
```

```
  b = []
  if a != None:
    for el in a:
      b.append((x1-(y1*el))%len(ru_RU)**2)

    return a[0], b[0]
```

Завдання 4

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

In [4]:

```
forbidden_lst = [
    "аъ",
    "аь",
    "бй",
    "бф",
    "гг",
    "гщ",
    "гъ",
    "еъ",
    "еь",
    "жй",
    "жц",
    "жщ",
    "жъ",
    "жы",
    "йъ",
    "къ",
    "лъ",
    "мъ",
    "оъ",
    "пъ",
    "ръ",
    "уъ",
    "уь",
    "фщ",
    "фъ",
    "хы",
    "хь",
    "цщ",
    "цъ",
    "цю",
    "чф",
    "чц",
    "чщ",
    "чъ",
    "чы",
    "чю",
    "шщ",
    "шъ",
    "шы",
    "шю",
    "щг",
    "щж",
    "щл",
    "щх",
    "щц",
    "щч",
    "щш",
    "щъ",
    "щы",
```

```
    "щю",
    "щя",
    "ъа",
    "ъб",
    "ъг",
    "ъд",
    "ъз",
    "ъй",
    "ък",
    "ъл",
    "ън",
    "ъо",
    "ъп",
    "ър",
    "ъс",
    "ът",
    "ъу",
    "ъф",
    "ъх",
    "ъц",
    "ъч",
    "ъш",
    "ъщ",
    "ъъ",
    "ъы",
    "ъь",
    "ъэ",
    "ыъ",
    "ыь",
    "ьъ",
    "ыы",
    "ьь",
    "эа",
    "эж",
    "эи",
    "эо",
    "эу",
    "эщ",
    "эъ",
    "эы",
    "эь",
    "эю",
    "эя",
    "юъ",
    "юы",
    "юь",
    "яъ",
    "яы",
    "яь",
]


def decode(a, b, text):
    plaintext = ""
    n = len(ru_RU)
    # get inverse of a
    a_inv = gcd(a, n ** 2)[1]

    # go through bigrams
    for bi in range(0, (len(text)), 2):
        bi_enc = encode_bigram(text[bi : bi + 2])
        decode_bi = ((bi_enc - b) * a_inv) % (n ** 2)

        x2_idx = decode_bi % n
        x1_idx = (decode_bi - x2_idx) / n
```

```
        x1 = ru_RU[int(x1_idx)]
        x2 = ru_RU[int(x2_idx)]
        if x1 + x2 not in forbidden_lst:
            plaintext += x1 + x2
        else:
            return False

    return plaintext
```

Завдання 5

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

In [9]:

```
top_bi = ["но", "на", "ст", "то", "ен"]

allp = all_pairs(bigram_frequency.keys(), top_bi)
for p in allp:
    try:
        a, b = find_key(p[0], p[1])
        check = decode(a, b, text)
        if check != False:
            print("Keys: ", a, b)
            print(check)
            break
    except TypeError:
        pass
```

```
Keys:  72 805
агодышлидашлибыстроинеслышнокакподснежныеводыпротекаламолодостьеленывбездействиивнешнемв
овнутреннейборьбеитревогеподругунеенебылоизовсехдевицпосещавшихдомстаховыхонанесошласьни
соднойродительскаявластьникогданетяготеланаделенойасшестнадцатилетнеговозрастаонасталапо
чтисовсемнезависимаоназажиласобственнойсвоеюжизньюножизньюодинокойеедушаиразгораласьипог
асалаодинокоонабиласькакптицавклеткеаклеткинебылониктонестеснялееиниктонеудерживалаонарв
аласьитомиласьонаиногдасамасебянепонималадажебоялась самойсебявсечтоокружалоееказалосьейн
етобессмысленнымнетонепонятнымкакжитьбезлюбвиалюбитьнекогодумалаонаистрашностановилосьей
отэтихдумотэтихощущенийвосемнадцатилетоначутьнеумерлаотзлокачественнойлихорадкипотрясенн
ыйдооснованиявесьееорганизмотприродыздоровыйикрепкийдолгонемогсправитьсяпоследниеследыбо
лезниисчезлинаконецноотецелеными колаевнывсеещенебезозлобленияталковалобеенервахиногдаейп
риходиловголовучтоонажелаетчеготочегониктонежелаеточемниктонемыслитвцелойроссиипотомонау
тихаладажесмеяласьнадсобойбеспечнопроводиладеньзаднемновнезапночтотосильноебезымянноесче
монасовладетьнеумелатакизакипаловнейтакипросилосьвырватьсянаружугрозапроходилаопускались
усталыеневзлетевшиекрыльянопорывыэтинеобходилисьейдаромкаконанистараласьневыдатьтогочтов
нейпроисходилотоскавзволнованнойдушисказывалась всамомеенаружномспокойствииироднымеееча сто
быливправепожиматьплечамиудивлятьсяинепониматьеестранностейвденьскоторогоначалсянашрасск
азеленадольшеобыкновенногонеотходилаотокнаонамногодумалаоберсеньевеосвоемразговореснимпо
требностьвзащитеинформациивозникаетвсвязиснеобходимостьюобеспечитьсекретностьисследовани
йвстратегическихобластяхправильнораспределятьинформациюопромышленныхразработкахирегулиро
ватьинформациюоличностивсовременномобществена чаловосьмидесятыхгодоврассматриваетсякакнач
альныйпунктогдасоциальныепротестывдемократическихстранахпомоглисплестисьглобальнойсетих
акеровполитическийфлиртнапочвенарушенияправчеловекапородилтьмуорганизацийхакероввмассест
ранмирапочтиодновременномоменеечемзагодэтигруппыузналипрелестьсотрудничестваихчленысвободн
ообменивались идеямичерезнациональныеграницычастопоукраденнымпаролямдающимбесплатныйдосту
пктелефоннойсетинесколькопричинобьединившисьвместесделалимеждународныйкомпьютерныйразбой
лекгимидейственнымновыетехнологиисоздавшиеболеемощныеидешевыекомпьютерыразвитиекоммуника
цийдлясвязиимеждународныйхарактерстандартовустановленныхтранснациональнымикорпорациямивп
ринципеестьлишьдвавидаугрозыраскрытиеивидоизменениеданныхраскрытиеданныхпредполагаетчтоко
мутослучайноилипослецеленаправленныхдействийстализвестенсмыслинформацииэтотвиднарушения
встречаетсянаиболеечастопоследствиямогутбытьсамыеразныееслипохищентекстк нигисправочникан
акоторуюпотраченымесяцыработыдесятковлюдейтодляколлективаавторовэтокатастрофаипотеримогу
твыражатьсявтысячахдоллароводнакоесликнигаужеизданатодостаточнолишьслегкапожуритьпохитит
еляирассказатьослучившемсявотделеновостейгазетыилипотелевидениюпохитительможетсделатькни
гевеликолепнуюрекламуоченьважнуюинформациюоберегаемуюотраскрытияпредставляютсведенияолюд
яхисторииболезниписьмасостояниясчетоввбанкаходнакопомнениюбольшогочисласпециалистовугроз
ыличностисвведениемкомпьютеровостались натомжеуровнеивтомжесостояниичтоидообширногоисполь
зованияэвмвведениевсовременномми ретуризмстановитсявсеболееважнойбыстроразвивающейсяотрас
льюхозяйствадоходыоттуризмастановятсяважнойчастьювалютныхпоступленийвомногихстранахразви
тиетуризмаспособствуетростуобщественногопроизводстваулучшениюегоструктурыроступроизводит
ельноститрудавомногихотрасляхэкономикидаженеимеющихктуризмупрямогоотношениямеждународное
туристскоепотреблениестимулируетмногочисленныеэкономическиепроцессыоткрывающиедополнител
ьныерынкидляпродукциинетуристскихотраслейсоздаваятемсамымусловиядляростапроизводствавсеэ
тифакторыделаютразвитиеиндустриитуризмаоченьважнымдлястранспереходнымтипомэкономикиеоном
ическиетрудностикоторыепереживаютэтигосударстванемогутнесказатьсянауровнеразвитиятуризма
ноприэтомкаждаястранаимеетвэтомотношениисвоюспецификуцельданнойработырассмотретьипроанал
изироватьорганизациютуристскойдеятельностивстранеспереходнымтипомэкономикинапримереvенгр
иивначалерассматриваютсятеоретикометодическиеположенияисследованиязатемдаетсяоценкаразли
чныхфакторовразвитияиндустриитуризмавенгрииприродноресурсныйкультурноисторическийиинфрас
труктурныйпотенциалкомплексноетуристскоерайонированиедалееп роводитсяанализсовременногосо
стоянияиндустриитуризмавенгриииеотдельныхкомпонентовнафонеобщегоуровняэкономическогоразв
итиястраныдаетсяоценкасоциальноэкономическойролииндустриитуризмавэкономикевенгриивзаклю
чениепроводитсяобщийанализорганизациитуристскойдеятельностивстранахспереходнымтипомэконо
микивобщемивенгриивчастностивенгияпринадлежакстранамспереходнымтипомэкономикиимееттемнем
енееспецифическиечертыкоторыеотличаютееотдругихстранэтоготипавотношенииразвитияиндустрии
туризмаосновнойтакойчертойявляетсяточтотуризмвенгрииразвиваетсяужедавноешевначаледвадцат
оговекавэтойстранесложилисьтрадиционныетуристскиесвязитуризмявляетсяважнойотраслью народн
огохозяйствасовременнойвенгрииколичествоиностранныхтуристовпосещающихвенгриюрастетизгода
вгодтомунемалоспособствуетбогатейшийкультурноисторическийиприрод
```

Висновок

> В ході лабораторної роботи був розшифрований текст афінного шифру. Для цього було використано частотний аналіз та алгоритми розв'язання рівнянь модульної арифметики.

> Були використані методи фільтрації осмислених текстів.