Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Комп’ютерний практикум №3

З дисципліни «Криптографія»

Виконали:

Студенти групи ФБ-33

Рудий А.О., Шкуропінський М.М.

Київ – 2025

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. Функція розширеного алгоритму Евкліда:

```
def extended_euclid(a, b):
        if (b==0):
                return a, 1, 0
        d, u, v = extended_euclid(b, a % b)
        return d, v, u - (a // b) * v
```

Функція розв'язання лінійних порівнянь(лінійне конгруентне рівняння виду **ax≡b(mod n)**):

```python
def solve_linear_congruence(a, b, n):
    d, u, v = extended_euclid(a, n)
    solutions = []

    if b % d != 0:
        return []

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

    d1, u1, v1 = extended_euclid(a1, n1)

    x = (b1 * u1) % n1

    for i in range(d):
        solutions.append(x + i * n1)

    return solutions
```

2. Використовуючи частину коду з практикуму №1 (функцію обрахунку частот біграм) знаходимо 5 найчастіших біграм зашифрованого тексту(01.txt):

```
{'рн': 62, 'ыч': 41, 'нк': 34, 'цз': 32, 'иа': 30}
```

{'рн': 62, 'ыч': 41, 'нк': 34, 'цз': 32, 'иа': 30}

3. Знаходимо всі можливі ключі:

```
[(29, 258), (148, 477), (152, 920), (553, 782), (443, 465), (307, 147), (405, 664), (475, 323), (902, 30), (399, 379), (855, 409), (929, 651), (842, 320)
, (625, 258), (754, 689), (77, 410), (884, 527), (21, 729), (313, 684), (656, 767), (707, 897), (306, 379), (445, 156), (914, 107), (885, 736), (421, 647
), (408, 320), (342, 457), (174, 891), (285, 859), (389, 885), (686, 819), (894, 506), (579, 85), (458, 625), (518, 472), (511, 94), (684, 568), (35, 558
), (450, 47), (11, 631), (796, 711), (464, 302), (761, 289), (731, 319), (739, 506), (241, 821), (498, 452), (572, 313), (327, 79), (926, 103), (648, 238
), (13, 151), (877, 906), (512, 527), (242, 395), (56, 921), (211, 224), (84, 31), (331, 85), (720, 101), (305, 341), (757, 913), (355, 372), (638, 861),
 (187, 806), (59, 111), (524, 793), (630, 503), (758, 368), (750, 364), (497, 10), (8, 477), (948, 257), (127, 666), (334, 315), (719, 193), (330, 546),
(730, 736), (666, 797), (287, 694), (437, 309), (764, 146), (450, 218), (323, 241), (200, 372), (304, 301), (780, 767), (306, 899), (103, 503), (940, 893
), (50, 540), (858, 695), (230, 89), (157, 568), (215, 927), (382, 503), (511, 541), (308, 563), (948, 161), (119, 602), (803, 496), (905, 16), (948, 771
), (804, 534), (647, 761), (158, 612), (330, 105), (746, 181), (393, 698), (932, 664), (222, 596), (802, 854), (654, 0), (616, 199), (809, 2), (76, 633),
 (556, 258), (657, 636), (47, 481), (540, 14), (463, 917), (314, 788), (606, 289), (788, 482), (674, 414), (277, 534), (911, 217), (295, 921), (105, 382)
, (618, 400), (343, 708), (80, 523), (67, 416), (336, 940), (203, 740), (486, 875), (732, 540), (627, 622), (655, 723), (774, 912), (165, 658), (231, 633
), (117, 74), (210, 418), (516, 601), (844, 67), (751, 504), (631, 652), (834, 883), (32, 106), (106, 864), (449, 410), (813, 625), (676, 339), (275, 550
), (345, 209), (181, 341), (655, 819), (950, 642), (254, 301), (204, 709), (229, 217), (197, 166), (207, 680), (159, 695), (856, 891), (953, 631), (881,
234), (503, 312), (562, 819), (787, 382), (568, 924), (619, 816), (653, 98), (631, 391), (173, 275), (634, 158)]
Кількість можливих ключів: 178
```

В нашому випадку вийшло, що загальна кількість можливих ключів (a, b) = 178.

4-5. Знаходимо підходящий ключ відкидаючи інші за критеріями:

1) Неможливі біграми:

```python
impossible_bigrams = ['аы', 'оы', 'иы', 'ыы', 'уы', 'еы', 'аь', 'оь', 'иь',
                      'ыь', 'уь', 'еь', 'юы', 'яы', 'эы', 'юь', 'яь', 'эь']
```

2) Частота частих літер:

```
o_count = text.count('о')
a_count = text.count('а')
e_count = text.count('е')

total_chars = len(text)

if (o_count + a_count + e_count) / total_chars > 0.20:
    return True
else:
    return False
```

В результаті наш ключ (a, b) вийшов:

a = 13, b = 151

```
a = 13, b = 151
```

А розшифрований текст:

многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакпи
сателякакневротикакакмыслителяэтикаикакгрешникакакжеразобратьсявэтойнев
ольносмущающейнассложностинаименееспоренонкакписательместоеговодном
рядусшекспиромбратьякарамазовывеличайшийроманизвсехкогдалибонаписанн
ыхалегендаовеликоминквизитореодноизвысочайшихдостиженийимировойлитера
турыпереоценитькотороеневозможноксожалениюпередпроблемойписательског
отворчествапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязвимк
акморалистпредставляяегочеловекомвысоконравственнымнатомосновании чтот
олькототдостигаетвысшегонравственногосовершенствактопрошелчерезглубоча
йшиебездныгреховностимыигнорируемодносоображениеведьнравственнымявл
яетсячеловекреагирующийуженавнутреннеиспытываемоеискушениеприэтомем
унеподдаваяськтожепопеременноготогрешиттораскаиваясьставитсебевысокиенра
вственныецелитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястроитсво
южизньоннеисполняетосновногопринципанравственностинеобходимостиотреч
ениявтовремякакнравственныйобразжизнивпрактическихинтересахвсегочелове
чествааэтимонна поминаетварваровэпохипереселениянародовварваровубивавши
хизатемкаявшихсявэтомтакчтопокаяниестановилосьтехническимпримеромрасч
ищавшимпутькновымубийствамтакжепоступаливангрозныйэтасделкассовестью
характернаярусскаячертадостаточнобесславениконечныйитогнравственнойборь
быдостоевскогопослеисступленнойборьбывоимяпримиренияпритязанийпервич
ныхпозывовиндивидастребованиямичеловеческогообществаонвынужденнорегр
ессируеткподчинениюмирскомуидуховномуавторитетукпоклонениюцарюихрис
тианскомубогукрусскомумелкодушномунационализмукчемуменеезначительны
еумыпришлисгораздоменьшимиусилиямичемонвэтомслабоеместобольшойличн
остидостоевскийупустилвозможностьстатьучителемиосводителемчеловечест
ваиприсоединилсяктюремщикамкультурабудущегонемногимбудетемуобязанавэ

томповсейвероятностипроявилсяегоневрозиззакоторогоонибылосужденнатаку
юнеудачупомощипостиженияисилелюбвиклюдямемубылоткрытдругойапостоль
скийпутьслужениянампредставляетсяотталкивающимрассматриваниедостоевск
оговкачествегрешникаилипреступниканоэтоотталкиваниенедолжноосновыватьс
янаобывательскойоценкепреступникавыявитьподлиннуюмотивациюпреступлен
иянедолгодляпреступникасущественныдвечертыбезграничноесебялюбиеисильн
аядеструктивнаясклонностьобщимдляобеихчертипредпосылкойдляихпроявлени
йявляетсябезлюбовностьнехваткаэмоциональнооценочногоотношениякчеловек
утутсразувспоминаешьпротивоположноеэтомуудостоевскогоегобольшуюпотре
бностьвлюбвиегоогромнуюспособностьлюбитьпроявившуюсявегосверхдоброт
еипозволявшуюемулюбитьипомогатьтамгдеонимелбыправоненавидетьимстить
напримерпоотношениюкегопервойженеиеелюбовникунотогдавозникаетвопросо
ткудаприходитсоблазнпричисленияядостоевскогокпреступникамответиззавыбор
аегосюжетовэтопреимущественнонасильникиубийцыэгоцентрическиехарактер
ычтосвидетельствуетосуществованиитакихсклонностейвеговнутреннеммиреата
кжеиззанекоторыхфактовегожизнистрастиегоказартнымиграмможетбытьсексуа
льногорастлениянезрелойдевочкиисповедьэтопротиворечиеразрешаетсяследую
щимобразомсильнаядеструктивнаяустремленностьдостоевскогокоторуюмоглаб
ыделатьегопреступникомбылавегожизнинаправленаглавнымобразомнасамогос
ебявовнутрьвместотогочтобыизнутриитакимобразомвыразиласьвмазохизмеичу
вствевинывсетакивеголичностинемалоисадистическихчертвыявляющихсявегор
аздражительностимучительстванетерпимостидажепоотношениюклюбимымлюд
яматакжевегоманереобращениясчитателемитаквмелочахонсадиствовневажном
садистпоотношениюксамомусебеследовательномазохистиэтомягчайшийдоброд
ушнейшийвсегдаготовыйпомочьчеловеквсложнойличностидостоевскогомывыд
елилитрифактораодинколичественныйидвакачественныхегочрезвычайноповыш
еннуюаффективностьегоустремленностькперверзиикоторуюядолжнабылапривест
иегоксадомазохизмуилисделатьпреступникомиегонеподдающееясянализутворч
ескоедарованиетакоесочетаниевполнемоглобысуществоватьибезневрозаведьбы
ваютжестопроцентныемазохистыбезналичияневрозовпосоотношениюсилпритяз
аниипервичныхпозывовипротивоборствующихимторможенийприсоединяясюда
возможностисублимированиядостоевскоговсеещеможнобылобыотнестикразряд
уимпульсивныххарактеровноположениевещейзатемняетсяналичиемневрозанео
бязательногокакбылосказаноприданныхобстоятельствахновсежевозникающегот
емскореечемнасыщеннееосложнениеподлежащеесостороныческогояпреоо
долениюневрозэтотолькознактогочтоятакойсинтезнеудалсячтооноприэтойпопы
ткепоплатилосьсвоимединствомвчемжевстрогомсмыслепроявляетсяневроздост
оевскийназывалсебясамидругиетакжесчиталиегоэпилептикомнатомосновании
тоонбылподвержентяжелымприпадкамсопровождавшимисяпотерейсознаниясуд
орогамиипоследующимупадочнымнастроениемвесьмавероятночтоэтатакназыва
емаяэпилепсиябылалишьсимптомомегоневрозакоторыйвтакомслучаеследуетоп
ределитькакистероэпилепсиютоестькактяжелуюистериюутверждатьэтосполной
уверенностьюнельзяподвумпричинамвопервыхпотомучтодатыанамнезическихп

рипадковтакназываемойэпилепсиидостоевскогонедостаточныиненадежныавовт орыхпотомучтопониманиесвязанныхсэпилептоиднымиприпадкамиболезненных состоянийостаетсянеясныма

Це виявився текст З. Фрейд **«Достоевский и отцеубийство».**

Висновок: в ході комп’ютерного практикуму ми успішно реалізували криптоаналіз афінної біграмної підстановки. Застосувавши частотний аналіз та необхідні математичні функції, такі як розширений алгоритм Евкліда, ми перебрали комбінації найчастіших біграм.

Початковий аналіз дав 178 кандидатів на ключ. Використовуючи критерії відбору, зокрема фільтрацію за неможливими біграмами та аналіз частоти частих літер, ми змогли ідентифікувати єдиний правильний ключ: a = 13, b = 151. Цей ключ дозволив повністю відновити вихідний текст, яким виявився фрагмент роботи З. Фрейда.