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

Виконала:
студентка
групи ФБ-13,
Буєва Христина.

Криптоаналіз афінної біграмної підстановки

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

Порядок виконання роботи

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.

Хід роботи

Завдання 1.

Реалізовано функції extended_gcd – знаходження оберненого елемента та нсд, за допомогою розширеного алгоритму Евкліда; solve_linear_congruence – розв'язування лінійних порівнянь.

Завдання 2.

Найпоширеніші біграми в ШТ:

Біграма	Частота
аж	0.012420478642835504
цп	0.01302635564980309
шы	0.014843986670705847
ки	0.015146925174189639
тя	0.016358679188124812

Завдання 3.

Кожну біграму представлено числом. Для кожного можливого співставлення знайдено можливі кандидати ключів.

```
Most frequent bigrams in russian language:
['ст', 'но', 'то', 'на', 'ен']
[545, 417, 572, 403, 168]

Most frequent bigrams in ciphertext:
['аж', 'цп', 'шы', 'ки', 'тя']
[6, 697, 771, 318, 588]

All possible keys:
[(858, 403), (452, 643), (418, 914), (521, 517), (232, 418), (624, 120), (458, 256), (226, 805), (457
```

All possible keys:

[(858, 403), (452, 643), (418, 914), (521, 517), (232, 418), (624, 120), (458, 256), (226, 805), (457, 801), (467, 156), (198, 689), (702, 855), (103, 300), (555, 937), (521, 247), (624, 811), (729, 285), (392, 399), (226, 535), (955, 123), (504, 863), (10, 52), (702, 585), (245, 751), (509, 134), (406, 531), (927, 81), (69, 645), (337, 657), (569, 108), (795, 907), (563, 495), (494, 621), (951, 455), (692, 343), (235, 509), (543, 371), (440, 768), (34, 47), (103, 882), (503, 68), (735, 480), (166, 182), (729, 867), (763, 596), (259, 430), (269, 746), (504, 484), (440, 77), (337, 474), (892, 714), (858, 24), (735, 750), (6, 201), (398, 864), (232, 39), (259, 700), (716, 534), (726, 850), (457, 422), (843, 201), (14, 895), (115, 101), (233, 867), (580, 318), (599, 83), (184, 158), (565, 807), (118, 502), (132, 430), (233, 597), (351, 402), (381, 385), (19, 462), (565, 537), (946, 225), (947, 843), (829, 77), (101, 938), (219, 743), (362, 694), (942, 45), (546, 846), (927, 534), (846, 223), (728, 418), (860, 151), (118, 123), (777, 166), (396, 478), (415, 243), (381, 6), (728, 688), (610, 883), (742, 616), (843, 783), (396, 748), (15, 99), (34, 825), (580, 900), (10, 52), (292, 196), (202, 743), (192, 697), (502, 201), (820, 895), (146, 101), (605, 867), (53, 442), (10, 52), (494, 933), (441, 497), (951, 651), (282, 841), (192, 427), (182, 381), (459, 502), (318, 430), (605, 597), (103, 402), (908, 261), (918, 307), (441, 227), (388, 752), (669, 581), (679, 627), (871, 357), (861, 311), (141, 843), (643, 77), (287, 938), (746, 743), (951, 725), (43, 200), (484, 691), (431, 255), (759, 542), (769, 588), (90, 732), (951, 272), (815, 223), (356, 418), (674, 151), (459, 123), (467, 352), (520, 788), (477, 398), (908, 843), (769, 858), (779, 904), (100, 87), (10, 634), (356, 688), (858, 883), (215, 616), (502, 783), (520, 97), (573, 533), (530, 143), (53, 63), (635, 688), (283, 316), (334, 905), (660, 223), (326, 15), (609, 325), (660, 914), (25, 232), (678, 461), (352, 182), (51, 399), (377, 678), (627, 380), (301, 101), (910, 690), (326, 597), (301, 371), (936, 92), (584, 681), (635, 309)]

Завдання 4.

Для кожного можливого ключа розшифровувався шифртекст. Змістовний текст шукався за допомогою індексу відповідності. Таким чином, якщо індекс відповідності не наближений до теоретичного значення – цей варіант відкидався. Маємо ключ та розшифрований текст :

```
Key: (10, 52)
Decrypted Text: вскорепослесвоегоприемавбратствомасонов
```

Decrypted Text:
вскорепослесвоегоприемавбратствомасоновпьерсполнымнаписаннымимдлясебяруководствомотом чтоондолженбылделатьвсвоихименияхуехалвкиевскуюгуберниюгденаходиласьбольшаячастьегокрес тьянприехаввкиевпьервызвалвглавнуюконторувсехуправляющихиобяснилимсвоинамеренияижелани яонсказалимчтонемедленнобудутпринятымерыдлясовершенногоосвобождениякрестьяноткрепостно йзависимостичтодотехпоркрестьяненедолжнобытьотягчаемыработойчтоженщинысдетьминедолжн ыпосылатьсянаработычтокрестьянамдолжнабытьоказываемапомощьчтонаказаниядолжнобытьупотр ебляемыувещательныеанетелесныечтовкаждомимениидолжнобытьучрежденыбольницыприютыиш колынекоторыеуправляющиетутбылиполуграмотныеэкономыслушалииспуганнопредполагаясмысл речивтомчтомолодойграфнедоволенихуправлениемиутайкойденегдругиепослепервогостраханаходи лизабавнымшепелявеньепьераиновыенеслыханныеимисловатретьинаходилипростоудовольствиепо слушатькакговоритбаринчетвертыесамыеумныевтомчислеиглавноуправляющийпонялиизэтойречито какимобразомнадообходитьсясбариномдлядостижениясвоихцелейглавноуправляющийвыразилболь шоесочувствиенамерениямпьеранозаметилчтокромеэтихпреобразованийнеобходимобыловообщеза нятьсяделамикоторыебыливдурномсостоянииинесмотрянаогромноебогатствографабезухогостехпорка кпьерполучилегоиполучалкакговорилитысячгодовогодоходаончувствовалсебягораздоменеебогатым чемкогдаонполучалсвоитьтысячотпокойногографавобщихчертахонсмутночувствовалследующийбюд жетвсоветплатилосьоколотитысячповсемименияможолотитысячстоилосодержаниеподмосковноймос ковскогодомаикняжоноколотитысячвыходилонапенсиистолькоженабогоугодныезаведенияграфинен

апрожитьепосылалосьтысячпроцентовплатилосьзадолгиоколотитысячпостройканачатойцерквистоил
аэтидвагодаоколотитысячостальноеоколотатысячрасходилосьонсамнезналкакипочтикаждыйгодонпр
инужденбылзаниматькрометогокаждыйгодглавноуправляющийписалтоопожарахтоонеурожаяхтооне
обходимостиперестроекфабрикизаводовитакпервоеделопредставившеесяпьерубылотоккоторомуон
менеевсегоимелспособностиисклонностизанятиеделамипьерсглавноуправляющимкаждыйденьзани
малсяноончувствовалчтозанятияегонинашагнеподвигалиделаончувствовалчтоегозанятияпроисходят
независимоотделачтоонинецепляютзаделоинезаставляютегодвигатьсясодной стороныглавноуправля
ющийвыставлялделавсамомдурномсветепоказываяпьерунеобходимостьуплачиватьдолгиипредприн
иматьновыеработысиламикрепостныхмужиковначтопьернесоглашалсясдругойстороныпьертребовал
приступениякделуосвобожденияначтоуправляющийвыставлялнеобходимостьпреждеуплатитьдолго
пекунскогосоветаипотомуневозможностьбыстрогоисполненияуправляющийнеговорилчтоэтосоверш
енноневозможноопредлагалдлядостиженияэтойцелипродажулесовкостромскойгуберниипродажуз
емельнизовыхикрымскогоименьяновсеэтиоперациивречахуправляющегосвязывалисьстакоюсложнос
тьюпроцессовснятиязапрещенийистребованийразрешенийитпчтопьертерялсяитолькоговорилемудад
атакисделайтепьернеимелтойпрактическойцепкостикотораябыдалаемувозможностьнепосредственн
овзятьсязаделоипотомуоннелюбилегоитолькостаралсяпритворитьсяпередуправляющимчтоонзанятд
еломуправляющийжестаралсяпритворитьсяпередграфомчтоонсчитаетэтизанятиявесьмаполезнымид
ляхозяинаидлясебястеснительнымивбольшомгороденашлисьзнакомыенезнакомыепоспешилипозна
комитьсяирадушноприветствоваливновьприехавшегобогачасамогобольшоговладельцагуберниииску
шенияпоотношениюглавнойслабостипьератойвкоторойонпризналсявовремяприемавложутожебылит
аксильнычтопьернемогвоздержатьсяотнихопятьцелыеднинеделимесяцыжизнипьерапроходилитакж
еозабоченноизанятомеждувечерамиобедамизавтракамибаламинедаваяемувременииопомнитьсякак
ивпетербургевместоновойжизникоторуюнадеялсяповестипьеронжилвстоюжепрежнейжизньютолько
вдругойобстановкеизтрехназначенийМасонствапьерсознавалчтооннеисполнялтогокотороепредписы
валокаждомумасонубытьобразцомнравственнойжизниизсемидобродетелейсовершеннонеимелвсе
бедвухдобронравияилюбвиксмертионутешалсебятемчтозатоонисполнялдругоеназначениеисправлен
иеродачеловеческогоиимелдругиедобродетелилюбовькближнемуивособенностищедростьвеснойго
дапьеррешилсяехатьназадвпетербургподорогеназадоннамеревалсяобехатьвсесвоиименьяиличноуд
остоверитьсявтомчтосделаноизтогочтоимпредписаноивкакомположениинаходитсятеперьтотнародко
торыйвверенемубогомикоторыйонстремилсяоблагодетельствоватьглавноуправляющийсчитавшийвс
езатеимолодогографапочтибезумствомневыгодойдлясебядлянегодлякрестьянсделалуступкипродол
жаяделоосвобожденияпредставлятьневозможнымонраспорядилсяпостройкойвовсехимениях больш
ихзданийшколбольницприютовдляприездабаринавездеприготовилвстречинепышноторжественные
которыеонзналнепонравятсяпьеруноименнотакиерелигиозноблагодарственныесобразамиихлебомс
ольюименнотакиекоторыекаконпонималбаринадолжныбылиподействоватьнаграфаиобманутьегоюж
наявеснапокойноебыстроепутешествиеввенскойколяскеиуединениедорогирадостнодействовалинап
ьераименьявкоторыхоннебывалещебылиодноживописнеедругогонародвездепредставлялсяблагоде
нствующимитрогательноблагодарнымзасделанныеемублагодеяниявездебыливстречикоторыехотяип
риводиливсмущениепьерановглубинедушиеговызывалирадостноечувствоводномместемужикиподн
осилиемухлебсольиобразпетраипавлаипросилипозволениявчестьегоангелапетраипавлавзнаклюбвии
благодарностизасделанныеимблагодеяниявоздвигнутьнасвойсчетновыйприделвцерквивдругоммест
ееговстретилиженщинысгруднымидетьмиблагодаряегозаизбавлениеоттяжелыхработвтретьемимень
иеговстречалсвященникскрестомокруженныйдетьмикоторыхонпомилостямграфаобучалграмотеирел
игиивовсехименияхпьервиделсвоимиглазамипоодномуплануводвигавшиесяивоздвигнутыеужекаме
нныезданиябольницшколбогаделенкоторыедолжныбылибытьвскоромвремениоткрытывездепьерви
делотчетыуправляющихобарщинскихработахуменьшенныхпротивпрежнегоислышалзатотрогательны
еблагодарениядепутацийкрестьянвсинихкафтанахпьертольконезналтогочтотамгдеемуподносилихле
бсольистроилиприделпетраипавлабылоторговоеселоиярмаркавпетровденьчтоприделужестроилсяда
внобогачамимужикамиселатемикоторыеявилиськнемуачтодевятьдесятыхмужиковэтогоселабыливве
личайшемразорениионнезналчтовследствиетогочтопересталипоегоприказупосылатьребятницженщи
нсгруднымидетьминабарщинуэтисамыеребятницытемтруднейшуюработунеслинасвоейполовинеонн
езналчтосвященниквстретившийегоскрестомотягощалмужиковсвоимипоборамиичтособранныекнем

Висновки : під час виконання лабораторної роботи були набуті навички частотного аналізу на прикладі розкриття моноалфавітної підстановки, а також опановано прийоми роботи в модулярній арифметиці.