Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:

Акент’єв Влад, Шапоренко Микита

Група: ФБ-06

Київ – 2022

Мета роботи

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

Хід 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.

Варіант 6

Реалізували підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язуванням лінійних порівнянь.

5 найчастіших біграм запропонованого шифртексту

['фд', 'цо', 'дм', 'мй', 'ги']

Кандидати на ключ

[[540, 390], [711, 412], [323, 452], [771, 386], [184, 288], [947, 566], [587, 722], [220, 849], [580, 693], [123, 859], [952, 724], [401, 226], [402, 642], [241, 936], [123, 859], [606, 938], [421, 930], [486, 733], [544, 572], [777, 472], [550, 953], [584, 229], [381, 312], [522, 136], [86, 319], [559, 83], [554, 246], [106, 628], [250, 908], [475, 587], [847, 556], [810, 45], [14, 194], [411, 768], [132, 551], [276, 384], [838, 146], [439, 869], [625, 373], [870, 536], [720, 750], [407, 479], [748, 851], [603, 225], [638, 868], [114, 764], [699, 572], [374, 38], [829, 209], [708, 229], [9, 281], [336, 632], [644, 319], [838, 827], [213, 835], [168, 628], [190, 934], [417, 748], [151, 314], [262, 748], [741, 872], [377, 531], [685, 376], [253, 531], [560, 779], [875, 686], [91, 469], [317, 686], [355, 748], [855, 97], [358, 500], [793, 97], [421, 930], [250, 908], [638, 868], [190, 934], [605, 594], [236, 850], [264, 5], [410, 198], [40, 38], [373, 182], [629, 7], [591, 536], [823, 948], [491, 259], [761, 142], [796, 287], [540, 390], [475, 587], [417, 748], [356, 238], [64,

916], [40, 353], [921, 78], [36, 99], [503, 443], [138, 810], [68, 209], [523, 752], [711, 412], [486, 733], [114, 764], [151, 314], [725, 943], [897, 877], [246, 691], [427, 74], [588, 895], [925, 17], [739, 513], [60, 226], [470, 538], [893, 588], [862, 30], [754, 876], [323, 452], [847, 556], [262, 748], [697, 827], [715, 141], [9, 353], [332, 109], [222, 564], [906, 443], [200, 655], [99, 767], [430, 752], [771, 386], [544, 572], [810, 45], [699, 572], [551, 634], [921, 479], [534, 758], [952, 479], [370, 541], [458, 634], [901, 851], [55, 634], [165, 510], [438, 45], [207, 882], [531, 45], [777, 472], [14, 194], [374, 38], [741, 872], [356, 238], [725, 943], [697, 827], [551, 634], [396, 541], [137, 429], [365, 138], [181, 474], [218, 490], [255, 506], [497, 273], [386, 225], [184, 288], [411, 768], [377, 531], [605, 594], [897, 877], [921, 479], [565, 937], [933, 280], [463, 226], [743, 708], [4, 390], [483, 535], [947, 566], [550, 953], [829, 209], [685, 376], [236, 850], [64, 916], [715, 141], [534, 758], [824, 88], [28, 237], [493, 919], [594, 288], [706, 692], [957, 808], [616, 436], [327, 938], [587, 722], [132, 551], [253, 531], [264, 5], [246, 691], [952, 479], [596, 379], [468, 559], [897, 226], [464, 925], [345, 762], [421, 535], [220, 849], [584, 229], [276, 384], [708, 229], [410, 198], [40, 353], [427, 74], [9, 353], [780, 43], [498, 291], [367, 229], [64, 291], [575, 12], [478, 663], [634, 260], [540, 663], [381, 312], [838, 146], [9, 281], [560, 779], [921, 78], [588, 895], [332, 109], [370, 541], [565, 937], [824, 88], [596, 379], [780, 43], [783, 330], [118, 458], [132, 516], [205, 132], [580, 693], [439, 869], [875, 686], [40, 38], [925, 17], [458, 634], [396, 541], [28, 237], [498, 291], [178, 152], [32, 491], [20, 690], [123, 859], [522, 136], [336, 632], [91, 469], [373, 182], [36, 99], [222, 564], [901, 851], [137, 429], [933, 280], [468, 559], [367, 229], [843, 24], [929, 952], [123, 859], [694, 70], [952, 724], [625, 373], [317, 686], [629, 7], [739, 513], [55, 634], [365, 138], [493, 919], [64, 291], [829, 927], [838, 584], [485, 690], [401, 226], [86, 319], [870, 536], [644, 319], [591, 536], [503, 443], [60, 226], [906, 443], [181, 474], [463, 226], [594, 288], [897, 226], [756, 350], [941, 753], [267, 412], [476, 753], [559, 83], [720, 750], [838, 827], [355, 748], [138, 810], [470, 538], [200, 655], [165, 510], [743, 708], [706, 692], [464, 925], [575, 12], [178, 152], [843, 24], [829, 927], [756, 350], [402, 642], [407, 479], [855, 97], [823, 948], [893, 588], [438, 45], [218, 490], [957, 808], [478, 663], [783, 330], [929, 952], [941, 753], [241, 936], [554, 246], [213, 835], [358, 500], [491, 259], [68, 209], [99, 767], [207, 882], [255, 506], [4, 390], [345, 762], [634, 260], [118, 458], [32, 491], [838, 584], [267, 412], [123, 859], [748, 851], [793, 97], [761, 142], [862, 30], [531, 45], [497, 273], [616, 436], [540, 663], [132, 516], [123, 859], [476, 753], [606, 938], [106, 628], [603, 225], [168, 628], [796, 287], [523, 752], [754, 876], [430, 752], [386, 225], [483, 535], [327, 938], [421, 535], [205, 132], [20, 690], [694, 70], [485, 690]]

Ключ

[711, 412]

ШТ

жшшоииючцогльжгигщгяыжгокшцммягщажумщмотвбфджшлрчгрдтузскйьуюитыщушяотакбюмхцоюялжффпшдшнкмйфмсойфбощфыдлифнщмгинщцоурхжчьтиезыдцбхжщддмнтрбчцумйтьффтмягдменйудлиаеюдэфчдажгикакшщмюяйшамйвчетиыэчдижяепурлюйббфтцйчмфмшощфжяотйфпшзйуэашюббочдпбгжийумсофтфчижмяуфркюэбиздшкбюздздзтмшмйэжшйяйзсгжшвышбчяррлфмзбзтцоаегжюявгтындфшушщмюямяжшыяпшфкбюздздзтсрюэндйбзтчдвфпшэяяяушдммявофнвяэтйрсмуяссййфофнропмирхьлнизюикггяцвэмгиажуивдглйивбфдэеэльдщевбцоглфтрбаюпжумйшфзфтиыпшлшйсфйхмфдцлпшвжуяумшелйяфююпбтйдмщмиоцолнцмхсзмтмышотаждяэшстпжумлввихыьтэщюмфдпжшевбцотябфмрнсьдюиаегжийушйстйумвэевчмэоашудмрцяхмфдцлпшэщумьбьмгччиюмтмпжщмхскмййпшжпершевбцотяьжаевякяжомрсшвяквйшырфдбоаездрльжызфтшяййфоецтуфдчммйоемеьнпянжымгиажхсвюхыдцфдййрмнммуыдквйшыражийюмплыжяеыэюмыщажзсбестьдщуекгжквттцосцфмиочгнюфдмйтйэитыжшешндбивыфйнкгжизфдлвндчмфдсмыххжчецоюмтмйиншоепбфдййктжщсяпшзятмфдовгдбитигжквйиншоепбздзтйогжешгиебэемрюмдшнмгиажэлшпдмюмсшхшейцяияшрснцшофквйшырйктламтмыдюмсяпшлррэзвтйчмшожяквйшфдцфжящмгиызмяпшхжешцвушовндиочгрщпжмяжоняафдомрэщхжхшжкчмхяэжгмффууййбхтярмщмкоздзтйоняууяфьбэлйипбтфэшрондбипжыжхшнмгиажмянжхыейййщдяркйьуцвотаеглйткигжиййиншоепбфдййьжщпешдйг

длицбзтьнгитыжшешашсбшжгищшквйшыршмуяссййфоурйтвжгибонкюиуюпбщуядакмрафдомрйф
тядомрэщхжхшндовшогжешдмумуужкюирэмеьняпештммвейяжчебоярчгрдияцфтычдижгопвчмэо
юитыжшешщдбивыфйюмйиупумбфыэейвжгибокшкяндапумамьоичцощшщеяннкльцайфоьзтфббо
юмхиезыдтиажжрыдвязсакчмбоствычиаечдбмугбовыхьлнквйшфдцфецыящдзтйогжешьжгибохжд
явянмшоурешщмлпдмюмсшхштййишрюитецовищшэонщстюиажжрчдйшййьдрлюялиндйфмрндпб
эщхжхшжкфтюэцоглпжотвбаебогляйюяубгяыжымхяяфиитыушсоиюдйгдлиаемйоездглрозвфдйшзд
бивыфйяящгйшакйшчмшолихжбиюомцывхскваоншфдлиэщхжхшчшрояиажгитфкваомцщмюяыьэй
гфмрттпфюожякквйшфдцфжямйжмпшчмййпшвбстшяйиаепбздрлбоствыхмдиярцоюмтмхмфдцлпш
мшсбшжгищшквйшырэецовищшшяыдыяхсщуофмрщмияэдаетйпмияизпятмбиаешлафдомрэщхжд
мтммйоездглфдмйщуейндрлшьцошйхмэшстйозпдмюмсшуяцфецчмушрозвфдйшздбивыфйапдмю
мсшояяящгйшщшоыщфенуяпшжкчмфмвшыжымыхсцбоствылизйпшяйэшздбипжыждмщбйлюяхсю
мфдмефдмйтйфждявянмшоурешщмлпдмюмсшхшфмыхярмецовищшйщажьогжешяящгглйиромбм
ябйлжгибойрнкюиуюпбщуядакмрафдомрйфщшкяндюяиоярцошянкльцаэщхжхшгщюипудмумууом
мтэщьнюяомзбовдшфжгибоюдчгыдакэеыдюмсяпшчитыжшешмшсбшжгищшквйшыршмюоаеюмед
щфецуяцдецяеэлндрлумидыдбивыдецовищшмйоемегяыжсвцяейэожясяэонщствбййньчдчгаепфэе
юдецфдмйияотюэбтпжадмйвшэшдощундбипжыжхшхжпльшквйшыряеэлндрлййфоецыдмйотднтй
чмшочгбюхыдцфдййхмдиярцоюмкецовищшдмушуяфддфмрогжгибощумдбипжуммкгжтхьнцшсецо
вилнмйфдндвытмейргпбумцвияфйвмнкгжизфдлвндцмзйюятчсцывхскваоншфдлиэщхжхшчшйичип
б

ВТ

виднарушениятстречаевсянаиболеечастопоследствиямогутбытьсаэьерсцньееслипохищентекстkни
гисправочниканакюторуюпотраченьмеснзьрабютьдесятковлюдейтодлпколлективаавторовэтоката
строфаипотеримогутвьрпжатысявтьсячахдолларoводнакоесликнигаужеизданатодостаточнолишыс
легкапожуритыпохитителяирассказатыослузившемсявотделеновостейгсцетьилипотелевиуениюпо
хитителыможетсделатыкнигевеликолепнуюрекламуоченыважнуюинформозиюоберегаемуюотрас
крьтияпредставляотсведенияолюдяхисторииболццниписымасостояниясчетоввбанкаходнакопомн
ениюболышогозисласпециалистовуграцлличностисвведениемкомпыотеровосталисынатомжеуров
неивтомжесостоянииичтошдяобширногоисполызованияэвмвведениетсовременноммиретурицмста
новитсятсфболееважнойбьстроразвиврющейсоотраслыюхацяйствадоходьюттурицмастановявсявп
жношчастыювалотньхпоступленийвомногихстранахрсцвитиетурщцмаспособствуетростуорществен
ногопроизводстваулучшениюегоструктурьроступроизводителыноститрудавомногихотрасляхэконо
микидаженеимеющихктурицмупрямогоютношениямеждународноетуристскоепотрфблениестиму
лируетмногочисленньеэкономическиепроцессьоткрьвающиедополнителыньерьнкшдляпродукци
инетурисвскихотраслейсацдаваятемсаэьмусловиядляростапроизводстватсеэтифакторьделрютрсц
витиеиндустриитурицмаоченыважньмдлястранспереходньмтипомэкономикиеономическиетрудн
остикоторьепереживрютэтигосударстванемогутнесксцатысянауровнерсцвитиятурщцманоприэтом
кпждаястранаимеетвэтомогношениисвоюспузификвзелыданнойрабютьрассмютретыипроаналщц
ироватыорганщцозиютуристскойуеятелыноститстранеспереходньмтипомэкономикинапримереве
нгриивначалерассматриваотсятеоретикометодическиеположенияисследованиязатемдаевсооценк
арсцличньхфакторовразвитияиндустриитурщцмавенгрииприродноресурсньйщулытурноисторичес
кийиинфраструктурньйпотелзиалкомплексноетуристскоерайонированиедалеепроводитсяаналщц
современногосостоянияиндустриитурицмавенгриииеютуелыньхкомпонентовнафонеобщегоуровн
яэкономическогоразвитиястраньдаетсяэзенкасоциалыноэкономическойролииндустриитурщцмавэ
кономикевенгриииуцаключениепроводивсоорщийаналщцорганизациитурисвскойдеятелыностивс
транахспереходньмтипомэкономикиворщемивенгриивчасгностивенгияпринадлежакстранамспер
еходньмтипомэкономикиимееттемнеменееспузифическиечертькоторьеотличрютееотдругихстран
этогютипавютношениирсцвитияиндустриитурицмаосновнойтакойчертойявляетсяточтютурщцмвен

грииразвиваевсяужедавноешевначаледватзатоговекавэтойстранесложилисытрадиционньетурисв
скиесвячитурицмявляетсяважнойютраслыюнародногохацяйствасовременнойвенгрииколичествои
ностранньхтуристовпосещрющихвенгриюрастетщцгодавгодтомунемалоспособствуетбогатейшийщ
улытурноисторическийиприрод