

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

Роботу виконали:

Касаб О.Р.

Косигін О.С.

Групи ФБ-06

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 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. Пишемо необхідні для успішної роботи алгоритмів функції

- `entropy` – допомагає знайти ентропію тексту щоб перевірити наскільки він змістовний
- `revers` – з допомогою алгоритму розширеного Евкліда(`ext_euc`) повертає нам обернене значення
- `ext_euc` – працює з від'ємними числами, великими числами та різними числами.
- `best_bi` – знаходить 5 частіших біграм в нашому тексті
- `bi_to_num` – це для того щоб потім знайти ключі тому що в алфавіті кожна буква відповідає певному індексу
- `mix_bi` – змішуємо наші біграмми та найчастіші які зустрічаються в мові та знаходимо пари і генеруємо усі можливі біграмми
- `pass_text` – перевірка тексту на змістовність
 - перша перевірка на неможливі біграмми
 - друга перевірка на Ентропію нашого тексту щоб вона була більше 4.2 і менш ніж 4.2
 - третя перевірка на те що найчастіша буква яка зустрічається в нашому тексті це о або е тому що це найчастіші букви в руської мові(тексті)
- `find_solv` – розв'язує рівняння
- `pass_keys` – бере наші біграмми, пустий масив де ми будемо зберігати наші ключі та масив де зберігаються усі можливі біграмми(їх дець 400 штук). Переводить їх у всі можливі пари ключів
- `affine_decoder` – потім ми всі ці ключі перевершмо з допомогою функції **`affine_decoder`** та переверяємо усе за допомогою функції **`pass_text`**
- **потім ми виводимо наш ШТ, ВТ та ключ**

2. Цей пункт можна реалізувати перетворивши букви у їх числовий еквівалент. Процес перетворення використовує формули, які були надані у методиці. Після перетворення ми створюємо найчастіші набори біграм, переводимо їх у числа, беремо найчастіші біграми російської мови, також перетворюємо їх у числа, та порівнюємо між собою, щоб скласти системи рівнянь і знайти потрібні нам варіанти розв'язків системи

3. Ключовим фактором змістовності тексту можна вважати ентропію текста. Тому для виявлення ключа тексту, потрібно після кожного дешифрування дивитися ентропію

Ентропія російського алфавіту = 4.35

Ось всі можливі ключі у числовому варіанті

[230, 89], [275, 550], [463, 917], [241, 821], [894, 506], [13, 151], [389, 885], [486, 875], [336, 940], [540, 275], [771, 271], [711, 297], [730, 736], [207, 680], [556, 258], [313, 684], [399, 379], [254, 301], [544, 457], [486, 618], [948, 257], [885, 736], [796, 711], [751, 504], [29, 258], [809, 2], [634, 158], [306, 379], [285, 859], [638, 753], [699, 457], [114, 649], [616, 199], [119, 602], [858, 695], [151, 199], [731, 319], [686, 819], [498, 452], [11, 631], [619, 816], [511, 94], [159, 695], [211, 224], [834, 883], [231, 633], [754, 689], [787, 382], [106, 864], [630, 503], [47,

[481], [13, 151], [76, 633], [165, 658], [764, 146], [105, 382], [13, 151], [647, 761], [382, 503], [450, 47], [8, 128], [39, 655], [70, 221], [101, 748], [132, 314], [163, 841], [194, 407], [225, 934], [256, 500], [287, 66], [318, 593], [349, 159], [380, 686], [411, 252], [442, 779], [473, 345], [504, 872], [535, 438], [566, 4], [597, 531], [628, 97], [659, 624], [690, 190], [721, 717], [752, 283], [783, 810], [814, 376], [845, 903], [876, 469], [907, 35], [938, 562], [345, 209], [464, 302], [242, 395], [720, 101], [67, 416], [948, 771], [950, 642], [342, 457], [450, 218], [148, 477], [553, 782], [323, 241], [299, 828], [838, 178], [698, 559], [405, 664], [648, 238], [174, 891], [855, 409], [804, 534], [902, 30], [949, 612], [173, 347], [210, 418], [932, 664], [152, 920], [197, 166], [856, 891], [948, 161], [844, 67], [277, 534], [437, 309], [848, 662], [670, 612], [266, 99], [842, 320], [497, 10], [739, 506], [32, 10], [572, 313], [475, 323], [625, 258], [802, 854], [750, 364], [127, 666], [813, 625], [408, 320], [638, 861], [151, 79], [285, 85], [375, 46], [562, 819], [707, 897], [331, 85], [914, 107], [157, 568], [59, 111], [145, 767], [232, 45], [327, 79], [655, 819], [676, 339], [314, 788], [579, 85], [511, 541], [117, 74], [684, 568], [524, 793], [4, 323], [393, 767], [790, 479], [103, 503], [719, 193], [222, 596], [254, 193], [421, 815], [190, 819], [250, 793], [662, 166], [123, 816], [263, 435], [810, 230], [676, 224], [586, 263], [417, 633], [475, 472], [12, 382], [788, 647], [816, 503], [729, 264], [323, 337], [262, 633], [847, 441], [23, 879], [54, 445], [85, 11], [116, 538], [147, 104], [178, 631], [209, 197], [240, 724], [271, 290], [302, 817], [333, 383], [364, 910], [395, 476], [426, 42], [457, 569], [488, 135], [519, 662], [550, 228], [581, 755], [612, 321], [643, 848], [674, 414], [705, 941], [736, 507], [767, 73], [798, 600], [829, 166], [860, 693], [891, 259], [922, 786], [953, 352], [113, 332], [291, 382], [695, 895], [957, 947], [568, 503], [171, 791], [810, 891], [929, 23], [707, 116]]

Ось наш ключ ,який підходить після всіх перевірок (неможливість біграми (наприклад [ъ,ы]), ентропія)

[13, 151]

Зашифрований текст:

лквдвдышкрбызякиабшачрнвзартчлчькзтманэмнязьябштрпнхтрхрнзтжккысечамнмпыивфяжтинфвйив
сжнпчнмпуцзкыфвйвутсюцзкыкынмотзщбйьбшхолуычгкицпзкианьюфлфтыраючькиашцзыфэнкйяпезт
нкжккысечамнмпыжэпаычйдбцвсшчмтшслаиятасзбчжйьбшывлтьйэзщбцпцмппшрифкздтеэккцтцзархрчосйпрй
жкчлчаккяжюышяояфскбчбязрчйзчвгзжзчызэвспчтцлжочшызюшхачрнтмнкуфйзбчечвпчнотмнктеотгчня
цзбшрчычбчнкицгщлчьековчфыщяцзреотйсфбйщялчдечамнмпыарчтчццзтьярняыхашхаытызздсепцяьяочш
збшзтжмсяачрнвзязоэарчэяицкятчрогцфэкыпзэйтпчазеязвахыдпдойдкрмпбцмвезлжочрчщтецрнбшкшэты
члчокбцккузбнинеппжвининачрнджацццаиятчщтецрнбшкшквабцотиябацийвычфткюмпьяэддаьчшызюсяу
ядсяжутрхбшчрнфэтзткзтцтеялчакиажштзмнксябяешщтецрнбшкшэццеопнхоьяочбастзырзгфлуфжмнк
ьэтнкфячашжвжямэвячатияцзоеязднеэмйкоевсщяыаяажвычцяучпяэязшкинвдэакзюнтмакырцсоушрне
цчнкяуялжочознкызаццнкяжсгмпчнвдепйдрчкесяркнлвцычпрычжкнпщюрчнбачквсеокаяорнбчнйцнбшзи
кзчшклзпсеппаопниашчеквдзезэгцеккызаццнкшчрнхкнчхвсфэиашцинэьяцзчычжтмэывйвшщтецрнбшкшф
бйьемтщцзжэьытнщрпаозвзьнотпанхзайдкрмпбцсрпаццруцзлчшклеэхкжяццлтяыблчуучзвпяэякшяцзкл
твсбцяыыцлбцдйрцецкзвзычаквсойюшххолуычннийвбнзеевсоцпахышчгзючушчядкцрпаозмеяззьябчтмаэз
уыйюфэхбшркбцуэдйуфрняыннийвцяучрнкейпрцккутгщяжйухыксмпырабцпабштхлгтивчябкогьракыбротх
ыачрнмнкршчуярачыбязрчфяяктфчнвдщтецрнбшкшдфчжшюжачрнвзартччучнпцпраюьтпнкшчойзтвйпцд
зтофтфэцтнкзофтчнщцккуфпяыщяряжеещпцбцхкюзгзщырнэяччяыцзыэшрмпбцсрпарчтчбйхярняыжкжль
цснкшчэяутпамзгьпнсевазэфяцзоэцтнвеэзвдчекеэгызнзтчнпниувчппжкнкэблыибшхязрнпыарчнччфьстла
нвеиэмпрчвмкеэйкогхчтыыззэивьянэзьяфякщтызэчгшяжпсьжфтцюызкдзтщачзаяюшкшйзлафпэойзьялчуцд
неэнпейвязрнбйеплюдфызякиашзачрнвзязоэеьхрнфпечзэгмшчрнйахыбшнрчнммпэхчйбйвсчнммпэяючб
ьяярняыцеязойсхкфпхотнртмэчзкыквивпнктейесолйджкмэшчрзжйеспнмэйчяовытылуычмебцкяюотнныки
ашзфтногаашятчфяжтгщцщырычыбчтчжкрйупиажмыашкмнйврбфяесоркееэллцеиашццяцзъмзщяебтцфвеб
зозяныюжючывзжсгьтчыучрнепйаозделнйааьцяцзэкйэфтйсрнецеопнхоинхыэврцсбчзмтанэмнязьяцзйсиа
ычицнввдбцкыярнбшутсюцзкыфпцеэярнкецзкышчднжчюнийпозыяцзнкйсепьжчокбцпцмнйаэккчюжычгш
нвдфкгнкмяфтпаюьукфвецыогзбшущапкхьюэинрцогэбфтпаюьтпнкэофяачшдвсоефтпаюьукфвмаолпаццнкяж
ьцсротвжуаддызкыжкяюебхзлзмзгштышспаэтивщцзексонвюгшшикабшбйчззсеобилзиротццфгтйсучфжэвдфя
пзьсебччщяцзкодпшяюачйкшебччекиабшфяяцмнкыбзгхчтыгшшчкгнккшчтчтиншцияцзывыяючбятьююаь
ыкьзаучйзтысюнебшцзечучючквяднеэльаачрнвзартчдбйеплюрбучэттийшчрнвцебтцузиджчутеэьсаучочк
иабшебхзбшфтногйюрбхобятчйцотасбйбччяцегщечеойюрбмэипкйчнезучлчмыбшхыздыжкфэмпожфтецжк
нкецспнезнашзбштыфтфэотучиншцияцзовйдзеотечамнлзийебччекфвйкинвдщыечикфвжяццзебчочьвеслеяз
дчюзюабйчыикфтщрчашяцзшсиаычицнввдфтпаюьукфвйэинбшцзещецпйзтжятчхбцяычлуычфлзньхярнб
шкжкмафпзкфвчхззгьутчнянэзьянвсаяюыьтнотшрычйцспнмпйаццяычрьхярнечяыцзчнйвшхнвючшкиач
яюйдбцьэтнкфякэцзыхынмлзещккмвинзтчхрытнбцйдгмтщцзрнбшрнсяткывыгняжйзутйэлчцяйцнйамвр
ьпзквдзтмаьпнкэофяйтмпдфяечювузпбейснуычфтинрцзтсрсяыйтсюжяюаяшявьфлфэбйьичнафпзксоы
ярнгьтнрцтыярнэякпнкшчрнгсиаычицнввдевинзтолчспейцаыячыбшйдзэярнкецзрчжйупейдгмтщцзтыфт
ещятыспецяжлштзщэтыиылтчкяяоечелнжшдэпаычычтбнбйтзиклнзчнйвфэбйьичжцхтзщфпмавцеы
ичвзэлзбьзаццихкпцкяхыозбятчызякиашцзфяеьноччажсчащзьянвшхьягнлжчцеофлшххобятчбьдссьшзчгш
шчрнфэнрчнмпйаццнкпнотсзлчрнсэмоежыккюнкэбпкйфэуэебзоеыхынмицйдеэккотнчштплкэотрчнмнм
пмэчнйвдэмпкрнхжкыюзрнечекицяыькеэиыюзручншчияцзовиылчнькяуанпийсбцмнмпкеэзщйхчащзднеэ
пдшызюуфачштвснюфязюуфзайдщыгтчылждеекрлрмпбцмвзаяючкдфызьякиашзачрнвзартччсжлжыязызэ
тшийвычывсхкрчызьярнбшкшфссяыкыярнбшкшхйдрэягцшрифшчучлжияшкрбнитятнршчрнгятчлаэтмэ
щяшкиабшсеотбьяюшзурчычышсепькейуплеязбярнсятчтажсеэщйхтшньфпчаыячыбшфтпаюьукфвсэятчфяу

чыссбхяпацытыызыкыццзтыянвящыбчяыцзпнйввяочьяхыцциучюкмэвдючюжрьхярнечяыбшрйкщфяжтгщецй
свийпцсбшмпаычфткгнкыкряеыичвзрнпйкщтыызээкицбичжжеиажчыккюнкэбмзясязговыцзцеотгзякхучоже
чгзфтинрцбйзтрнзфлшхфэычаэгмнкуффтчавяюзаяалсецшлчьиашзрьцпфэцтбцккэоачрнвязарчтчзайяхялч
ькбйупбйфчыкпащзстзшиовьфэхыгшмзекчхюыьтнотбщчучючцяцицтлфвычялкшяюаэжйпщрсялкибчвы
фябйщшммпзкзвдвийвюжючнвзцккзязищшкхбйрнночягшрняыдкбцкцяечикфвсбхятччянарчэясрмэтыфж
хяшкйяиаючькнксяучяпкмплйяочрнзтжжшрмпбсрпарчтчюеэявсепнкэбфяжтгцднинежвгщтытнвдкрячнй
вдфмзынкщфясейпхобнжщчфтыуычдзесцнмяучтпмнфпийаечфэйсхкрнечжщьяимицрнбчтчнасжнпоебчцео
пнхофяжтгщачрнвязогкзщпцйпкяяоыйзбтедсяхынмпазхыыйдмусщяхнфвезтыычлчокбцккузбнжчуйуп
учыотцьянщммпуэфтцежскыназбечечсецкзйзхоучяэяеагщтыцзяесзтвдйэузнпйсрбчзньныачякуэтырнб
чнксяжцпажэеотнотыккрьчднмнйвтыожаымэсогефпоемзчйупйпщюйафэхнеээйджжицбчырчычзжючхырч
нааышыпащявыпнзэяыязбшкыозрнотмусщяхаэбычпабшкытнщммпрбчачяязсщцотцсннуычпеепшчьебья
яшкиабшпкмдцюевсзьмеязэзтыжцзеотлжеинеэнрыщывжккйэфяжзьянвшхфтцежсрчнйвтыожаымэддгеф
поемзссяиачицнвдджкйсиахыычяктзфятыыякоыечзнзтчучычньбнзежкфэкксйяцщцккяжжагефпоеыцссяж
йзфтцежскыйзччщяикнкяжжаиаычэкуфиахыпнхофяаяажеы

Ключ: [13, 151]

Розшифрований текст:

многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневротикакакмысл
ителяэтикакакрешникакакжеразобратьсявэтойневольносмущающейнаасложностинаименееспоренонкакп
исательместоеговодномрядудшескипромбратьякарамазовывеличайшийроманизвсехкогдалибонаписанных
алегендаовеликоминквизитореодноизвысочайшихдостижениймировойлитературыпереоценитькотороенев
озможноксожалениюпередпроблемойписательскоготворчествапсихологдолженсложитьоружиедостоев
скийскореевсегоуязвимкакморалистпредставляяегочеловекомвысоконравственнымнатомоснованиичтотол
ькототдостигаетвысшегонаравственногосовершенствактопрошелчерезглубочайшиебездныгреховностимыигн
орируемоодносоображениеведьнаравственнымявляетсячеловекреагирующийуженавнутреннеиспытываемое
искушениеприэтомемунеподдаваяськтожепопеременнотогрешиттораскаиваясьставитсебевысокиенравстве
нныецелитоголегкоупрекнутьвтомчтоонслишкомудобнодлясебястроитсвоюжизньоннеисполняетосновного
принципанравственностинеобходимостиотречениявтовремякакнравственныйобразжизнивпрактическихинт
ересахвсегочеловечестваэтимоннапоминаетварваровэпохипереселениянародовварваровубивавшихизатем
каявшихсявэтомтакчтопокаяниенестановилосьтехническимпримеромрасчищавшимпутькновымубийствамтак
жепоступаливангрозныйэтасделкасовестьюхарактернаярусскаячертадостаточнобесславениконечныйитоги
равственнойборьбыдостоевскогопослеиступленнойборьбыоимяпримиренияпритязанийпервичныхпозыв
овиндивидастребованиямичеловеческогообществаонвынужденнорегрессируеткподчинениюмирускомуидух
овномуавторитетукпоклонениюцарюихристианскомубогукрусскомумелкодушномунационализмукемумен
еезначительныеумыпришлисгораздоменьшимиусилиямичемонвэтомслабоместобольшойличностидостоев
скийупустилвозможностьстатьучителемиосвободителемчеловечестваиприсоединилсякюремщикамкультур
абудущегонемногоимбудетемуобязанавэтомповсейвероятностипроявилсяегоневрозиззакоторогоонибылосу
жденнатакуюнеудачупомощипостиженияисилелюбвиключдямемубылоткрытдругойапостольскийпутьслужен
иянампредставляетсяотталкивающимрассматриваниедостоевскогокакчестверешникаилипреступникаэто
отталкиваниенедолжноосновыватьсянаобывательскойоценкепреступникавыявитьподлиннуюмотивациюпр
еступлениянедолгодляпреступникасущественныдвечертыбезграничноесебялюбиеисильнаядеструктивнаяск
лонностьобщимдляобоихчертипредпосылкойдляихпроявленийявляетсябезлюбовностьнехваткаэмоциональ
нооценочногоотношениякчеловекутутсразувспоминаешьпротивоположноеэтомуудостоевскогоегобольшую
потребностьвлюбвиiegoогромнуюспособностьлюбитьпроявившуюсявегосверхдобротеипозволявшуюемулю
битьипомогатьтамгдеонимелбыправоненавидетьимститьнапримерпоотношениюкегопервойженеиеелюбов
никунотогдавозникаетвопросоткудаприходитсблзньпричислениядостоевскогокпреступникамответизавыб
ораегосюжетовэтопреимущественнонасилъникиубийцыэгоцентрическиехарактерычтосвидетельствуетосущ
ествованиитакихсклонностейвеговнутреннеммиреатакжеиззанекоторыхфактовегожизнистрастиегоказартны
миграмможетбытьсексуальногорастлениянезрелойдевочкиисповедьэтопротиворечиеразрешаетсяследующ
имобразомсильнаядеструктивнаяустремленностьдостоевскогокотораямоглабысделатьегопреступникомбыл
авегожизнинаправленаглавнымобразомнасамогосебявовнутрьвместотогочтобыизнутриитакимобразомвыр
азиласьвмазохизмеичувствевинывсетакивеголичностинемалоисадистическихчертвыявляющихсявегораздра
жительностимучительственетерпимостидажепоотношениюклюбимымлюдяматакжевегоманереобращения
читателемитаковмелочахонсадиствовневважномсадиствоотношениюксамомусебеследовательнонамазохистиз
томягчайшийдобродушныйиисвсегдаготовыйпомочьчеловекувсложнойличностидостоевскогомывыделилит
рифактораодинколичественныйидвакачественныхегочрезвычайноповышеннуюаффективностьегоустремлен

ность к перверзии, которая должна была привести его к садомазохизму или сделать преступником и его не поддающуюся анализу творческое дарование и такое сочетание вполне могло бы существовать без невроза, ведь бывают жестопроцентные мазохисты без наличия невроза. По отношению к силе притязания и первичных позывов и противоборствующих им торможений, присоединяя сюда возможности сублимирования, Достоевского все еще можно было бы отнести к разряду импульсивных характеров. Но положение вещей затемняется наличием невроза, не обязательно того, как было сказано при данных обстоятельствах, но все же возникающего тем скорее, чем насыщеннее осложнение, подлежащее ссоры, чуждого человеческого преодоления невроза, это только знак того, что такой синтез не удался, что оно при этой попытке поплатилось своим единством. Чем же в строгом смысле проявляется невроз Достоевский? Называл себя сам и другие так же считали его эпилептиком, на том основании, что он был подвержен тяжелым припадкам, сопровождавшимся потерей сознания, судорогами и последующим упадочным настроением. Весьма вероятно, что эта так называемая эпилепсия была лишь симптомом его невроза, который в таком случае следует определить как истероэпилепсию, то есть как тяжелую истерию. Утверждать это с полной уверенностью нельзя по двум причинам. В первом, потому что даты и анамнезических припадков так называемой эпилепсии Достоевского недостаточны и ненадежны, а во втором, потому что понимание связанных с эпилептоидными припадками болезненных состояний остается неясным.