

Міністерство освіти і науки України

НТУУ «Київський політехнічний інститут»

Фізико-технічний інститут

**CИМЕТРИЧНА КРИПТОГРАФІЯ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3**

**Криптоаналіз афінної біграмної підстановки**

**2 Варіант**

MUST BE CHANGED

**Виконала:**

Студентка групи ФБ-52

Головач Тетяна

2018

**Мета роботи**

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

**Хід роботи**

1. Знаходимо 10 найчастіших біграм для зашифрованого тексту.

2. Розв’язування систем лінійних порівнянь для різних варінатів переходів біграм.

3. Дешифрування тексту за допомогою отриманих ключів при розв’язанні системи лінійних порівнянь.

4. Розпізнавання змістовного тексту завдяки частотам букв ‘о’ та ‘е’.

**Найчастіші біграми в ШТ**

Array of max frequent bigrams is: [еш, шя, еы, до, зо]

**ШТ**

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугфбзчшохдодвзбряцкмдбэдцхзнощкяоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывдьмиыыяшцрбгянямзюдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывчфвэрфешмяояйывщеыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшящксавотзябйкжзшцопсйкоефтцрзюэдцсшямсканзомыжуэыыцсшмычмэжглрзщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызонорйвкхпшсзунрмоншзоязшяэдхпезхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглтдоккжшскзыядншууезжурфешщпнзшятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжеляыцдюппкгфкшскщквкшяозноюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочыезыяюйеытяьочмскмзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощяанбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопзаоешйшохзодонофшайсщзожурфмовоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжлыдяюйеызопыщжфоочсквжаббжнзбляьхзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурмеыйссожзешопхпимсжсказкзшяшйнэюшшомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщоцыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхоцыыиеыыяпомггднотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкбазущпязхлдырйпоазсяслщяджипщплзджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзшяцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхзиоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякзуяяяямзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфоефзббжнзтыссжяилнахпезфщпмшявжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжшалтыбжхябжюакцопиыщчыдншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвляешууяхщжпонойкыпюшщчмысклзыцбчмялзоцнрряешиыфсхядаыосябжьоиогфеыхзншзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажуюшимйшлыпутцурряешбзкцколппотзуыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйфшщоцьзхлцюпзхщжщккжюыюпцчзпэыиывдншуушсешяоюшбчкзуяяяямзозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзскккрздвюптжждшсэыпзьцяделоцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузябряешйкешзоешчбгяыоиыоцпмзямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешьоекшялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоножяяоьоэмкзшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэйфбждоцпюдлвляскмздбкзцжжущпрфуяшфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщомзмятыямйшалтыеызоешыедвайнинзшязпкцрфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэкжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдшчфилюшощжшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфбждоцпюдлвюпюпэзпшкзхуэжйуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяражуййюзвждвждмызхзосшзбкззжокуцеыюпщуыйтодыюпиызопызвкзмзюдайюдьмиыыяхфщжцфвчшящжюпмуюкжшбчбьщжыйрйшзяошйзоузяждчвхеыщчпмщпбкуяяоекшярбптхямзюдечрэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщкпоноюааощяекшйбчжучбгяыоиыоцпмяднщжшбчтзчзкззогяюалэчмиыоцюшяхщжпокбчфнодоздопзузхщжпоьфйказтзрэыосяфощждчвхеыхзжусжфрйктзшясжеьзоешрйэжпзжжбяаоешывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзюнзоешедвдвлгфезшйдбряилгфеыхзсккчвкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхзрэешйчпзюнешибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэййшмштцедзббжнзмоошууеыщчдонорзлзджипщчьоцыыиеыыявлаомяркгяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлжозномясктзлзмкжшбчшящкбяйбзбяшжддыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояоратлынсаскрэууншмяскжупмскжшбчцдвдвжьглцечмяскскщкбаекжшбчфшууэжтлмдэйсщжшмощквканбчтзябйкжзшцопсйзоужертцлвяхщжбямэсоеецызбйкмяюнзоекшвуяджпоьфйказсшлячовунщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчподояоносшншмоешдбждтззпсчжшбчншщзнэйсешьовбптдохлжурфбжффюшлцлыксфохявжядтлоцлылвбжзбмушямзешекощеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчбюпповбнзцжшзяоййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощкпорфссешмяабяопмьосяцызвмуйчмоешдбждщуивлвщоефтцрзюэдцсавксшншмоешдбждншайешюшлыбжюуиырафовуьмайтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсчжшсопжипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеыйсжулямрчфюшпфмяяявлвжипюпэышб��унрчфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдовкккшяабйчуцжелжрбрякывдюшлвохдошзяобпбжжуэырйбзщтелмяилщкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщкгфсймовккцивыйгшьльфжшншмолдопсшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджипбжюпмуяззощуиврймзвожзпофотывдохлцюпядайхпимиыраыжнэюшсйокбяжярзьазонырйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайншопэзцжбкюнзоносочзсыяхщжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшмущжзовказхяанаоешезвжбякбмурфоцхпэесопжипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлцечпфлцйшжбрякыиыхзфшайтцлбгцабхявыцпяохяупайтзншщзнэйсшкопншфузхпмдьюшшящксктллзокрзпмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкчфылидмышкбмщпбкуяяоекзожзуяпонзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэпбжжущчхябфбждоцпюдлвямэжглцяекжшскчйфибяншкеынтзужертцлвщчэжффйэракбяощзшжаокыиыщчсожзбиеызоузсуьмуяуыжддосшншмоешдбждсожзбигцскыкфотфлцабгяыовояяфяьшмущжвзлжыцмимшшйгшезновжьошйэзэфщзрзмкуягшзбезносожзбиеыыядвзбряжзлжипюпоцчбптдохлибвоанаопоьшйкешзокюыврухкнзеявжйэйканэущпзомязоныйфмяцяюакбмумяуысйчбямппыйыяюдйшлцлыэжмкгфеыйсмофыксюдабгяыкаяшябялбгцабхямзюдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжязджпзчзшяжкйкгшмускбфсчаоешезвжпонопмйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзоешедншщзнэйсешылбэяоыкжшбччзкзтырйскпонзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшсншешйкцчжшншэзччсжрлязшядяябтцшяанбчжучмкзшяшйрлщяегдяуярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвжпоноэбкзешдбшярллзджипюшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскподояоеыщжлкешраояазжшжущпщоскскможяскжшбцзвлвюпеыхзюдншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязнырэтцлыайдбкзешдбшянфсчтзномофшсжцкгяпзюнамзпеяпыэжйэзпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

**Знайдені ключі**

{0=231, 512=612, 514=196, 517=774, 523=830, 524=611, 525=391, 13=483, 527=541, 18=413, 531=123, 533=603, 534=332, 540=793, 542=52, 31=758, 33=453, 545=723, 34=828, 546=213, 35=919, 552=727, 554=55, 44=49, 46=734, 558=665, 49=940, 562=448, 564=278, 571=310, 62=231, 576=289, 579=960, 67=89, 68=287, 583=309, 72=913, 73=759, 585=882, 75=576, 589=634, 80=788, 596=180, 88=272, 602=886, 603=262, 91=24, 604=625, 93=851, 607=816, 95=929, 610=526, 99=845, 617=906, 106=142, 618=24, 620=200, 622=929, 111=72, 113=150, 627=583, 631=325, 633=452, 124=417, 638=382, 641=960, 134=45, 137=669, 138=888, 650=585, 651=727, 139=486, 141=55, 142=599, 144=460, 145=805, 664=62, 152=224, 665=355, 155=138, 156=740, 669=909, 165=588, 168=235, 682=293, 173=165, 687=86, 694=107, 695=545, 186=510, 700=475, 190=51, 708=275, 709=148, 199=762, 200=733, 713=820, 203=55, 204=692, 716=16, 717=541, 205=213, 207=960, 723=814, 726=111, 217=76, 731=41, 220=698, 221=489, 740=789, 741=624, 230=328, 744=386, 235=258, 238=557, 754=954, 244=830, 756=200, 757=638, 245=345, 758=262, 248=603, 761=220, 762=568, 252=857, 253=681, 771=861, 261=855, 775=913, 266=785, 267=213, 274=275, 788=204, 279=169, 793=134, 796=365, 292=421, 805=634, 806=231, 296=55, 297=258, 809=732, 816=473, 817=821, 819=731, 820=355, 310=696, 822=519, 823=65, 311=789, 824=661, 827=960, 320=913, 323=948, 837=45, 328=878, 330=956, 334=373, 848=263, 850=297, 339=27, 341=262, 855=227, 343=337, 344=50, 862=108, 351=845, 354=514, 866=27, 868=479, 357=749, 870=337, 358=55, 359=444, 873=89, 365=776, 881=168, 372=789, 886=754, 888=615, 376=489, 889=960, 378=696, 893=666, 382=45, 894=867, 385=80, 899=138, 390=10, 397=634, 399=830, 912=390, 915=178, 403=665, 917=320, 407=950, 409=278, 926=954, 927=84, 415=107, 928=918, 416=607, 930=665, 419=953, 421=537, 427=29, 428=309, 430=830, 943=917, 434=882, 436=887, 948=847, 437=394, 438=123, 444=504, 447=173, 449=300, 452=103, 458=432, 465=448, 466=696, 470=616, 477=200, 478=651, 483=723, 484=213, 491=337, 495=585, 496=14, 503=890, 509=266}

**ВТ**

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомнодоказатьэтоневозможноскорееэтойнеобходимостьювнаказаниидляпсихическойэкономиидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиуниженийосуждениедостоевскоговкачествеполитическогопреступникабылонесправедливымиондолженбылэтознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслуженногоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонаказанияондалсебянаказатьзаместителюотцаэтодаетнамнекотороепредставлениеопсихологическомоправданиинаказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковжаждутнаказанияеготребуетихсверхяизбавляясебятакимобразомотсамонаказаниятотктознаетсложноеиизменчивоезначениеистерическихсимптомовпойметчтомыздесьнепытаемсядобитьсясмыслаприпадковдостоевскогововсейполнотедостаточнотогочтоможнопредположитьчтоихпервоначальнаясущностьосталасьнеизменнойнесморянавсепоследующиенаслоенияможносказатьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестивсвязиснамерениемубитьотцаэтолежащеенасовестибремяопределилотакжеегоотношениекдвумдругимсферампокоющимсянаотношениикотцукгосударственномуавторитетуикверевбогавпервойонпришелкполномуподчинениюбатюшкецарюоднаждыразыгравшемуснимкомедиюубийствавдействительностинаходившуюстолькоразотражениевегоприпадкахздесьверхвзялопокаяниебольшесвободыоставалосьунеговобластирелигиознойпонедопускающимсомненийсведениямондопоследнейминутысвоейжизнивсеколебалсямеждуверойибезбожиемеговысокийумнепозволялемунезамечатьтетрудностиосмысливанияккоторымприводитверавиндивидуальномповторениимировогоисторическогоразвитияоннадеялсявидеалехристанайтивыходиосвобождениеотгреховииспользоватьсвоисобственныестраданиячтобыпритязатьнарольхристаеслионвконечномсчетенепришелксвободеисталреакционеромтоэтообясняетсятемчтообщечеловеческаясыновняявинанакоторойстроитсярелигиозноечувстводостиглаунегосверхиндивидуальнойсилыинемоглабытьпреодоленадажееговысокойинтеллектуальностьюздесьнасказалосьбыможноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаиподвергаемдостоевскогооценкеимеющейправонасуществованиелишьспристрастнойточкизренияопределенногомировоззренияконсерваторсталбынаточкузрениявеликогоинквизитораиоценивалбыдостоевскогоиначеупрексправедливдляегосмягченияможнолишьсказатьчторешениедостоевскоговызваноочевиднозатрудненностьюегомышлениявследствиеневрозаедвалипростойслучайностьюможнообяснитьчтотришедеврамировойлитературывсехврементрактуютоднуитужетемутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамазовыдостоевскогововсехтрехраскрываетсяимотивдеяниясексуальноесоперничествоиззаженщиныпрямеевсегоконечноэтопредставленовдрамеоснованнойнагреческомсказанииздесьдеяниесовершаетсяещесамимгероемнобезсмягченияизавуалированияпоэтическаяобработканевозможнаоткровенноепризнаниевнамеренииубитьотцакакогомыдобиваемсяприпсихоанализекажетсянепереносимымбезаналитическойподготовкивгреческойдраменеобходимоесмягчениеприсохранениисущностимастерскидостигаетсятемчтобессознательныймотивгерояпроецируетсявдействительностькакчуждоеемупринуждениенавязанноесудьбойгеройсовершаетдеяниенепреднамеренноиповсейвидимостибезвлиянияженщиныивсежеэтостечениеобстоятельствпринимаетсяврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповторениятогожедействиявотношениичудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинанеделаетсяникакихпопытокснятьеессебявзвалитьеенапринуждениесосторонысудьбынаоборотвинапризнаетсяикаквсецелаявинанаказываетсячторассудкуможетпоказатьсянесправедливымнопсихологическиабсолютноправильнованглийскойдрамеэтоизображеноболеекосвеннопоступоксовершаетсянесамимгероемадругимдлякоторогоэтотпоступокнеявляетсяотцеубийствомпоэтомупредосудительныймотивсексуальногосоперничествауженщиныненуждаетсявзавуалированииравноиэдиповкомплексгероямывидимкакбывотраженномсвететаккакмывидимлишьтокакоедействиепроизводитнагерояпоступокдругогоондолженбылбызаэтотпоступокотомститьностраннымобразомневсилахэтосделатьмызнаемчтоегорасслабляетсобственноечувствовинывсоответствиисхарактеромневротическихявленийпроисходитсдвигичувствовинып��реходитвосознаниесвоейнеспособностивыполнитьэтозаданиепоявляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхиндивндуальнуюонпрезираетдругихнеменеечемсебяеслиобходитьсяскаждымпозаслугамктоуйдетотпоркивэтомнаправлениироманрусскогописателяуходитнашагдальшеиздесьубийствосовершенодругимчеловекомоднакочеловекомсвязаннымсубитымтакимижесыновнимиотношениямикакигеройдмитрийукоторогомотивсексуальногосоперничестваоткровеннопризнаетсясовершенодругимбратомкоторомукакинтереснозаметитьдостоевскийпередалсвоюсобственнуюболезньякобыэпилепсиютемсамымкакбыжелаясделатьпризнаниечтомолэпилептикневротиквомнеотцеубийцаивотвречизащитниканасудетажеизвестнаянасмешканадпсихологиейонамолпалкаодвухконцахзавуалировановеликолепнотаккакстоитвсеэтоперевернутьинаходишьглубочайшуюсущностьвосприятиядостоевскогозаслуживаетнасмешкиотнюдьнепсихологияасудебныйпроцессдознаниясовершеннобезразличноктоэтотпоступоксовершилнасамомделепсихологияинтересуетсялишьтемктоеговсвоемсердцежелаликтопоегосовершенииегоприветствовалипоэтомувплотьдоконтрастнойфигурыалешивсебратьяравновиновныдвижимыйпервичнымипозывамиискательнаслажденийполныйскепсисациникиэпилептическийпреступниквбратьяхкарамазовыхестьсценаввысшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпостигаетчтодмитрийноситвсебеготовностькотцеубийствуибросаетсяпереднимнаколениэтонеможетявлятьсявыражениемвосхищенияадолжноозначатьчтосвятойотстраняетотсебяискушениеисполнитьсяпрезрениемкубийцеилиимпогнушатьсяипоэтомупереднимсмиряетсясимпатиядостоевскогокпреступникудействительнобезграничнаонадалековыходитзапределысостраданиянакотороенесчастныйимеетправоонанапоминаетблагоговениескоторымвдревностиотносилиськэпилептикуидушевнобольномупреступникдлянегопочтиспасительвзявшийнасебявинукоторуювдругомслучаенеслибыдругиеаа

**Розпізнавання тексту**

Автоматичне розпізнавання здійснюється в два етапи:

1. На основі частот найчастіших та найменш частіших букв у російській мові, а саме: о,а,е,ф,щ,ь. Якщо хоча б одне значення частот цих літер відкланяється від еталонного значення більше ніж значення точності, то це не є текст. Рекомендується використовувати наступну точність: 7.
2. На основі індексу відповідності. Цей метод також базується на порівнянні еталонного та підрахованого для тексту індексів відповідності. Рекомендована точність: 0.01.

**Висновок**

Отже, в ході Практикума ми засвоїли навички криптоаналізу та атаки на шифр афінної підстановки. Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.