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

**Фізико-технічний інститут**

# КРИПТОГРАФІЯ

## КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Варіант 3

Виконали: студенти групи ФБ-12

Куцаєнко Дмитро та Федірко Ярослав

**Київ – 2023**

**Мета роботи**:
Набуття навичок частотного аналізу на прикладі розкриття

моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

## **Завдання**:

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:

Протягом виконання пошуку ключа ми отримали такі можливі значення a та b.

Можливі значення a:

[0, 954, 199, 854, 62, 923, 943, 792, 305, 802, 269, 868, 246, 708, 434, 7, 206, 861, 69, 38, 20, 830, 100, 656, 497, 925, 563, 762, 47, 509, 235, 755, 655, 824, 18, 941, 810, 80, 159, 464, 428, 66, 715, 914, 462, 188, 107, 306, 169, 131, 151, 231, 692, 36, 533, 599, 253, 452, 499, 687, 899, 892, 137, 881, 730, 93, 398, 895, 362, 527, 726, 773, 274, 31, 124, 155, 186, 217, 248, 279, 310, 341, 372, 403, 465, 496, 558, 589, 620, 651, 682, 713, 744, 775, 806, 837, 930, 48, 79, 110, 141, 172, 203, 234, 265, 296, 327, 358, 389, 420, 451, 482, 513, 544, 575, 606, 637, 668, 699, 761, 823, 885, 916, 947, 17, 897, 120, 282, 83, 192, 64, 236, 184, 219, 679, 871, 927, 789, 725, 909, 944, 878, 109, 165, 841, 777, 52, 35, 769, 90, 852, 56, 913, 14, 45, 76, 138, 200, 262, 293, 324, 355, 386, 417, 448, 479, 510, 541, 572, 603, 634, 665, 696, 727, 758, 820, 851, 882, 742, 926, 34, 796, 905, 370, 27, 778, 672, 223, 591, 918, 618, 746, 183, 855, 406, 431, 43, 661, 289, 106, 512, 537, 934, 343, 300, 128, 738, 555, 449, 25, 215, 833, 530, 424, 936, 491, 182, 641, 470, 652, 150, 377, 779, 309, 459, 686, 320, 811, 502, 227, 584, 275, 734]

Можливі значення b:

[562, 533, 700, 256, 407, 130, 762, 411, 590, 727, 29, 314, 71, 63, 438, 526, 664, 220, 371, 929, 168, 778, 774, 469, 634, 897, 221, 359, 829, 821, 235, 870, 593, 744, 837, 405, 686, 682, 872, 900, 339, 624, 567, 705, 68, 443, 149, 287, 955, 523, 194, 800, 376, 404, 541, 128, 342, 480, 812, 218, 469, 440, 607, 669, 318, 562, 590, 727, 29, 438, 576, 908, 900, 128, 748, 314, 841, 407, 934, 500, 66, 593, 159, 686, 779, 345, 438, 4, 531, 97, 624, 190, 717, 283, 810, 376, 35, 727, 293, 820, 386, 913, 479, 45, 572, 138, 665, 231, 758, 324, 851, 417, 944, 510, 76, 603, 169, 696, 262, 355, 448,

541, 107, 634, 200, 342, 494, 210, 547, 261, 717, 107, 649, 469, 849, 548, 260, 686, 466, 618, 438, 91, 751, 463, 872, 652, 262, 624, 144, 753, 129, 516, 149, 242, 769, 335, 428, 521, 614, 180, 707, 273, 800, 366, 893, 459, 25, 552, 118, 645, 211, 738, 304, 831, 397, 490, 56, 583, 342, 494, 551, 888, 602, 342, 494, 489, 578, 819, 717, 107, 649, 469, 570, 586, 827, 942, 466, 618, 60, 948, 317, 432, 872, 652, 262, 624, 547, 474, 563, 919, 342, 494, 830, 919, 199, 655, 252, 748, 404, 94, 590, 404, 386, 479, 572, 386, 618, 711, 308, 618, 407, 4, 500]

**Наші знайдені п’ять найчастіших біграм шифртексту:** тд, рб, во, щю, кд.

## *Шифрований текст:*

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпвоы
омхзотхэтоовцлшвуджозчхйбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжц
юлцлхйостщюшужхриажгцфхзхжцитвожюфпксщхибухкйзюжмьгнхщюзншбхюэотйбавотдцю
эшшылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюмхэшухэоз
оихщюкцзоюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужуш
юстлхэдвоэомюфожхетжютдцюгршшкдэйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывк
цхнцхеоцэвбйбышкдэйюейосежхюбгцэюубйутодткдвощхщющцяюстудвежюнхэджядшищвчч
ощщвунойхзозпцэфтмефпшхтдпощщщыкдвуозеойбдэзэстсдоожмиврбгхнойхзозпцэцэфпэтщо
щюэоеохсгдюмлзсдвеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбухкйэыбдтджюзнхыохн
хлхыбэлфошхэдохехвоубпзшбчхлыйбсуодмзеоэотэкшфстднтщюфпкдютэтнцхыдйщюэтвцтйс
длжюасцгцеокочэкдютетэтфтщютздйиреттднттюрюецтйвмшшзцтйищцюеокцфпжюэддйкцвм
чоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдихктщюжонжсиодгуоддйучяожстд
нтжхщюжощщщыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхцпвоыойбщеьжкхшцжо
сбанолхжжоойераннбйейсвцхндншбчбжуэтихшцвзеокэхытцажшбэйчтцпчээыкояхлцюоцэвбх
чшсшпвситуберончхфоыойиеыаншшвуйжышьтджфицхеогбшшанжхтдпнягвофихыыжжхщюз
нбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгтфдэй
етзэстйуэлетмюшюыхнцхтцпвотдучеощищынийькосотыкддйсуюгкцхнрбвотдьздйиреттднттю
щсзйэысесдвейхаирбтюзсжжйбщддццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотдднщ
ддцбаабжукцеочтйхвюеыдйрббдфхдйыжхшшшшцаышиткчсняощщуогбажбфьащелбхшзцтйищ
цюнхктсджайершецшмбзнбрфоюболохехвоаыйбсучхбзеойбйотгрбарбдкбзцбаююэттдвюкост
щюьхджяормлзсдцэфпкчшюкэфощщвуэтегрбьюетитщоойышцчшцабдншдкцжхщюцодтэоаэс
тжхетжютдхшкдыспнкчнжрбвотдбнкдютрртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсд
вейдвугдпоябрбднтцэющощщтокшеронцчшццнджфитджюкцтйвмщыдйфиибшфжхмоатсбгцф
пюшзцтйищгхэнкчнжрбвотдыгзнкдютооюывющючтсдвеэткнгстйрбмежоатсбгцфпбхьньзвоы
оэозэстщоеонтмыгцндтцоохлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщ
жунхктсджхетжютдхшкдысжхкйгхбжйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбк
жгажюррщазюфяшшеокояншдкцмеввнмжхетжютдхшкдысбхьнэлжхэоейфитдтхыбэлтднтзбш
шернбйедшзцтйищцюджфицхяберстфпвоэуажкбруатеоахщюмхэшухжцлжрбгхкйпнвопюшцл
шшшэтихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбвонстднбансюуйщодэнтихыбюешюых
нцхтцпетщцжжйбвотддцитвожюшцбдшшсущантсофогбсурржцзожюдюяюэоддтххгнхщюжбз
нкофтждцжжйбвотдромхжюгбгцлхкссдкйрретфпасйотдухвцщоыояоетктйхэдетэьвугцышшс
ажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшшшухсугждннььгррщюцйюгдтку
югаюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшчобхдбдшжуьжгажюпнньхыохзйзцвоьый
бсунбцюэозоихщюмолесбсуммяюепдэйхсбрбвогьвугцышшсажкбгцфпюшшшетждрсэтзэстудо
бжьлзтцлхыбвхкйсудйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужькюдурбщдфхгжеыникоь

бгцэюйбрбдntцэюлжгажющощщкющанмжюйорршхжхщюфмэощняюабгххсййбргшзцтйищц
южхинфиывйугнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябруеыохпыы
жкьцчгдзюшхыбфшвуйжышэшзцтйищцювснхеокшзожххцлжкбьхвцньйбгцшхщстхвюфпгдхы
пюнонбажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщюцнжхвцлшжьгцвужхщюююетнобюхн
щютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуолсылжэыпюшбхфньхытцо
дгжабйбхфйужцбретщюудшшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдвеетштехлцбретйх
цпетмыпюеюмхэшюеыюлбссэтфтыбрудэщхжхтцмхрыонцчшццнйиеыанвущоьылхнцэыгцлхэ
цхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдлзеоушйбяхщоцщанкдьгнхтдьжрбгхчощ
щвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгхооюывющючтсдвеетнюяевокй
фитдднсесдчобоэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгцитцпвохсчонххгнбвчетщхыошучб
ерончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытцончхшхжбзцлхгбущдйнищдгждцщоыоь
жйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюцптдтхнгкцеоубхфкцтхшммыдйрб
сучхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэтсдатлцпнвотдхшкдэйолэтзйеретх
жвгажщаиашдбншдкцжхыболиндйчетдажгцситцэюмхэшсущцитвожюшцшуерюмтцшцсюпду
хтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйуцнбрщюэтсдбоцпштмыкдохьбгцфпибшшерн
бцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлттдкгрбвмнищдрианлххнэ
йрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхшпоосбанкцоох
лэттднттюхлдшшшитщостжошсзхтдьжрбгхмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкю
шсшпдтушйбяхщоцщаняюепмтцпжхофюекйухощйекдютвоэуажкбвхцнлхщюмыкотцноуеьюэ
ывюаоэумйаннбцючотхтдэиыжюбдыюмнищдкбуофюьтыбвхпикцутвоэуажкбвхетшхзхжхриа
жгцсстднбанщдюйерййнбьзрбйешхвимбсурржутзчхшцвзеоетйаыжтфюекоцппикцбнщожхвбв
ущджьэывюфюнэстсдвеатлцпнчэсклхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгт
фдэйсуьхцретмхщюбеьжкхшцтжпнгсштввюлтдntнойхтюмихлтджюйхцпвотдяочоехыбйбзцл
ждцхнрбчэскеокдвопюшцлшйотдухвцщохсгтфдньзюэшкчаюйхцпвоыойсвцхндншблйднвоэтс
ючтсоеютдэшжьпоойерягррщюкэиннисуюхыогцщарбвоуйщодэнтихыбвучшвуэожхэдюгрбтдт
хыбгцэюйотдухвцщоыофоюбпокйфигжщддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтц
петмыохцйзцэозоихыбгцфптцэочоьбгцфпчочобоацлжолфтьюжтфпвекдфтжюпюфотдяобзохвн
щзтлвошскоооыокдютждкдртntфддйшюыхнцхтцпвотдсуыищаднсейузйнбьхдретыбрущоьый
брбитшхыошсзхтдстntыбюлпюыыеоьывюатошанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхн
лхщюкцооньщечощщвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащд
рощщсиюасцитфпкдьоицжувундэыдйлдюойхфбпойхнудйхнэлщащзчэяуемнбррмютддйьзкцс
юбцсучдвуандшеохсихйхбхщпйхлеэапнчхеойхшисеетщхыощцсучдвукудйэюцнсесдверианлх
хнэйрбгхыянбитйюсуюгэшжььггжнбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнвуетэтфтщю
бдухтддцситцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябс
фрбгхшхвияжьзвотдучяоехфдвукдюткйтцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйу
вгксююиндйчевостююхцяхщюкоушнбднеокоацяхжхитсюоюйянбэюцпчэдйщтощцюйиеыанш
швуйжышьтфоэсцркьзозбндфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхофйуфюьювортнтфд
дйкдютгцитсдвейхагкцжуружхеогсослфчхшцщцыомтмюитсюфоойервукйниыжзтсдгцитстфп
вешбрбдntцфпйотдухвцщоыощощщюггжнбгхкудйэюждвудрзохскдыстднбанщдвехызцчэшхд
жщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнхлхгтэдерйетдажбйщтцпвотдучвцйудйпрэв
щдшдэыдйут

**Під час роботи програми ми отримали такий ключ k=(a,b), де a = 199, b = 700**

## *Розшифрований текст:*

отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногочелов

екавовсякомслучаеоноглавныйисточникчувствавинынеизвестноединственныйлиисследовани
ямнеудалосьещеустановитьдушевноепроисхождениевиныипотребностиискупленияноотнюдь
несущественноединственныйлиэтоисточникпсихологическоеположениесложноинуждаетсяво
бясненияхотношениемальчикакотцукакмыговоримамбивалентнопомимоненавистииззакоторо
йхотелосьбыотцакаксоперникаустранитьсуществуетобычнонекоторыядолянежностикнемуоба
отношениясливаютсявидентификациюсотцомхотелосьбызанятьместоотцапотомучтоонвызыв
аетвосхищениехотелосьбыбытькаконипотомучтохочетсяегоустранитьвсеэтонаталкиваетсянак
рупноепрепятствиевопределенныймоментребенокначинаетпониматьчтопопыткаустранитьотц
акаксоперникавстретилабысостороныотцанаказаниечерезкастрациюизстрахакастрациитоесть
винтересахсохранениясвоеймужественностиребенокотказываетсяотжеланияобладатьматерью
иотустраненияотцапосколькуэтожеланиеостаетсявобластибессознательногооноявляетсяоснов
ойдляобразованиячувствавинынамкажетсячтомыописалинормальныепроцессыобычнуюсудьб
утакназываемогоэдиповакомплексаследуетоднаковнестиважноедополнениевозникаютдальне
йшиеосложненияеслиуребенкасильнееразвитконституционныйфакторназываемыйнамибисекс
уальностьютогдаподугрозойпотеримужественностичерезкастрациюукрепляетсятенденцияукл
онитьсявсторонуженственностиболеетоготенденцияпоставитьсебянаместоматерииперенятьее
ролькакобекталюбвиотцаодналишьбоязнькастрацииделаетэтуразвязкуневозможнойребенокпо
нимаетчтоондолженвзятьнасебяикастрированиееслионхочетбытьлюбимымотцомкакженщина
такобрекаютсянавытеснениеобапорыванеНавистькотцуивлюбленностьвотцаизвестнаяпсихоло
гическаяразницаусматриваетсявтомчтоотненавистикотцуотказываютсявследствиестрахапере
двнешнейопасностьюкастрациейвлюбленностьжевотцавоспринимаетсякаквнутренняяопаснос
тьпервичногопозывакоторыяпосутисвоейсновавозвращаетсяктойжевнешнейопасностистрахпе
редотцамделаетненавистькотцунеприемлемойкастрацияужаснакаквкачествекарытакиценылю
бвиизобоихфакторовВытесняющихненавистькотцупервыйнепосредственныйстрахнаказанияи
кастрациисследуетназватьнормальнымпатогеническоеусилениепривноситсякаккажетсялишьдр
угимфакторомбоязньюженственнойустановкиярковыраженнаябисексуальнаясклонностьстано
витсятакимобразомоднимизусловийилиподтвержденийневрозаэтусклонностьочевидноследуе
тпризнатьиудостоевскогоионалатентнаягомосексуальностьпроявляетсявдозволенномвидевто
мзначениикакоеимелавегожизнидружбасмужчинамивегодостранностинежномотношениихсоп
ерникамвлюбвиивегопрекрасномпониманииположенийобяснимыхлишьвытесненнойгомосекс
уальностьюкакнаэтоуказываютмногочисленныепримерыизегопроизведенийсожалеюноничего
немогуизменитьеелиподробностионенавистиилюбвикотцуиобихвидоизмененияхподвлиянием
угрозыкастрациинесведущемувпсихоанализечителюпокажутсябезвкуснымиималовероятны
мипредполагаючтоименнокомплекскастрациибудетотклоненсильнеевсегоносмеюуверитьчтоп
сихоаналитическийопытставитименноэтиявленияВневсякогосомненияинаходитвнихключклю
бомуневрозуиспытаемжееговслучаетакназываемойэпилепсиинашегописателянонашемусозна
ниютакчуждытеявленияВовластикоторыхнаходитсянашабессознательнаяпсихическаяжизньук
азаннымвышенеисчерпываютсявэдиповомкомплексепоследствиявытесненияненавистикотцун
овымявляетсяточтовконцеконцовотождествлениесотцомзавоевываетвнашемяпостоянноемест
оэтоотождествлениевоспринимаетсянашимянопредставляетсобойвнемособуюинстанциюпрот
ивостоящуюостальномусодержаниюнашегоямыназываемтогдаэтуинстанциюнашимсверхяипр
иписываемейнаследницеродительскоговлияниянаиважнейшиефункцииеслиотецбылсуровнас
ильственжестокнашесверхяперенимаетотнегоэтикачестваивегоотношениикясновавозникаетп
ассивностькоторойкакразнадлежалобыбытьвытесненнойсверхясталосадистическимстановит
сямазохистскимтоестьвосновесвоейженственнопассивнымвнашемявозникаетбольшаяпотребн

остьвнаказаниииояотчастиотдаетсебякактаковоевраспоряжениесудьбыотчастиженаходитудовл
етворениевжестокомобращенииснимсверхясознаниевиныкаждаякараявляетсяведьвосновесво
ейкастрациейикактаковаяосуществлениемизначальногопассивногоотношениякотцуисудьбавк
онцеконцовлишьдальнейшаяпроекцияотцанормальныеявленияпроисходящиеприформирован
иисовестидолжныпоходитьнаописа
нныездесьанормальныенамещенеудалосьустановитьразграниченияміжунимизамечаетсячтон
аибольшаярольздесьвконечномитогеприписываетсяпассивнымэлементамвытесненнойженств
енностиищекакслучайныйфакторимеетзначениеявляетсяливнушающийстрахотецивдействит
ельностиособеннонасильственнымэтоотносится кдостоевскомуфактегоисключительногочувст
вавиныравнокакимазохистскогообразажизнимысводимкегоособенноярковыраженномукомпо
нентуженственностидостоевскогоможноопределитьследующимобразомособенносильнаябисе
ксуальнаяпредрасположенностьиспособностьсособойсилойзащищатьсяотзависимостиотчрезв
ычайносуровогоотцаэтотхарактербисексуальностимыдобавляемкранееузнаннымкомпонентам
егосуществараннийсимптомприпадковсмертиможнорассматриватькакотождествлениесвоегоя
сотцомдопущенноевкачественаказаниясосторонысверхятызахотелубитьотцадабыстатьотцомс
амомутеперьтыотецноотецмертвыйобычныймеханизмистерическихсимптомовиктомужетепер
ьтебяубиваетотецдлянашегоясимптомсмертиявляетсяудовлетворениемфантазиимужскогожел
анияиодновременномазохистскимпосредствомнаказаниятоестьсадистическимудовлетворение
мобаяисверхяиграютрольотцаидальшевобщемотношениемеждуличностьюиобектомотцаприс
охраненииегосодержанияперешловотношениемеждуяисверхяноваяинсценировканавторойсце
нетакиеинфантильныереакцииэдиповакомплексамогутзаглохнутьеслидействительностьнедае
тимвдальнейшемпищинохарактеротцаостаетсятемжесамымнетонухудшаетсясгодамитакимоб
разомпродолжаетоставатьсяиненавистьдостоевскогокотцужеланиесмертиэтомузломуотцуста
новитсяопаснымеслитакиевытесненныежеланияосуществляютсянаделефантазиясталареально
стьювсемерызащитытеперьа

## Висновки:

Під час виконання лабораторної роботи в нас вийшло реалізувати
атаку на афінний шифр за допомогою частотного аналізу, який базується на
тому, що шифр зберігає статистичні властивості мови, пов’язані із частотами
біграм