

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ  
ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

**ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ**

**Кафедра інформаційної безпеки**

**КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3**

**з дисципліни**

**Криптографія**

Перевірила:

Селюх П.В

Виконали студенти групи ФБ-94

Резніченко Н.І та Белоцький Д.О

**Тема:** Криптоаналіз афінної біграмної підстановки

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

**Постановка задачі:**

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:
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. Методи, що реалізують необхідні математичні операції можна переглянути в файлі `additional_functions.py`

2. За допомогою методу `bigram_freq_in_cipher_text()`, що є трошки вдосконалим порівняно з лабораторним практикумом 1 було знайдено 5 найчастіших біграм в шифртексті згідно варіанту:

```
5 popular bigrams in text
['вн', 'тн', 'дк', 'хщ', 'ун']
```

3. Для початку створили всі можливі пари біграм.

Для шифртексту:

```
Pairs of the most popular five bigrams in ciphertext
[('вн', 'тн'), ('вн', 'дк'), ('вн', 'хщ'), ('вн', 'ун'), ('тн', 'дк'), ('тн', 'хщ'), ('тн', 'ун'), ('дк', 'хщ'), ('дк', 'ун'), ('хщ', 'ун')]
```

Для найчастіших біграм мови:

```
Pairs of the most popular five bigrams
[('ст', 'но'), ('ст', 'то'), ('ст', 'на'), ('ст', 'ен'), ('но', 'то'), ('но', 'на'), ('но', 'ен'), ('то', 'на'), ('то', 'ен'), ('на', 'ен')]
```

Перевели отримані пари у числовий вигляд та отримали всі можливі співставлення частих біграм мови та частих біграм шифртексту:

```
[(837, 385), (923, 604), (183, 284), (589, 44), (86, 790), (307, 470), (713, 230), (221, 775), (627, 535), (406, 436), (124, 726), (69, 910), (654, 176), (372, 106), (906, 755), (530, 21), (248, 912), (585, 361), (303, 291), (679, 606), (186, 571), (832, 227), (950, 304), (558, 602), (646, 227), (764, 304), (372, 602), (118, 211), (687, 509), (569, 13), (93, 323), (943, 275), (289, 174), (279, 819), (850, 523), (196, 422), (186, 106), (307, 33), (297, 678), (951, 360), (3, 746), (9, 166), (6, 952), (651, 571), (339, 940), (163, 335), (31, 602), (649, 940), (473, 335), (341, 602), (785, 490), (653, 757), (829, 943), (465, 292), (158, 498), (453, 491), (434, 726), (654, 777), (949, 770), (930, 44), (295, 127), (276, 362), (942, 911), (651, 571), (773, 940), (349, 335), (31, 602), (122, 940), (659, 335), (341, 602), (537, 490), (219, 757), (643, 943), (465, 292), (654, 777), (391, 336), (434, 726), (189, 95), (887, 615), (930, 44), (698, 654), (741, 83), (43, 105), (186, 75), (57, 168), (206, 664), (558, 75), (832, 664), (20, 199), (372, 571), (149, 630), (501, 41), (352, 87)]
```

Шляхом розв'язання системи (1) було отримано пари значень (a, b), що потенційно можуть бути ключами афінного шифру біграм для нашого варіанту:

$$\begin{cases} Y^* \equiv aX^* + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases}, \quad (1)$$

Отримані пари:

```
Keys that can be true
dict_keys([(923, 604), (183, 284), (86, 790), (307, 470), (221, 775), (627, 535), (406, 436), (69, 910), (654, 176), (906, 755), (530, 21), (585, 361), (303, 291), (679, 606), (832, 227), (950, 304), (646, 227), (764, 304), (118, 211), (687, 509), (569, 13), (943, 275), (289, 174), (850, 523), (196, 422), (307, 33), (297, 678), (951, 360), (3, 746), (9, 166), (6, 952), (339, 940), (163, 335), (649, 940), (473, 335), (785, 490), (653, 757), (829, 943), (158, 498), (453, 491), (654, 777), (949, 770), (295, 127), (276, 362), (942, 911), (773, 940), (349, 335), (122, 940), (659, 335), (537, 490), (219, 757), (643, 943), (391, 336), (189, 95), (887, 615), (698, 654), (741, 83), (43, 105), (57, 168), (206, 664), (832, 664), (20, 199), (149, 630), (501, 41), (352, 87)])
```

4. Для кожного ключа зі списку вище дешифрували текст та перевіряли його змістовність за таким критерієм: якщо в отриманому тексті є сполучення букв (такі біграми), що ніколи не зустрічаються у мові, то цей ключ хибний і відкидається.

В якості біграм, що ніколи не зустрічаються у мові були обрані наступні:

```
["аъ", "аы", "аь", "оъ", "оы", "об", "уъ", "уы", "уь"]
```

В результаті після перевірок отримали значення ключа:

```
Key was found
```

Після того як ключ було отримано виводимо в консоль дешифрований текст.

### ШТ (Варіант 5)

кеюибшаефдфмдкдролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдлыохунхмьввнсду  
эммндтихкеюибщыцзкзхшвносыютнйьщтцншуссянхщлвжвпъкшвнмщзфтсхщпдкясввцц  
тнавпгнуйввйнлхиьерддыцрихэкьзцижцъехцмсэкжлрибуждэмхимьпьявсттнзцюсфспьуз  
йпдкнхркхульацкчашьяншибжаксэкцзтгчшиюцншумшошьящкщнфрхуюижегцыззфрщихзт  
чцрихнэпозтгфккчцкдмкльоьеынунйльцяьэрхнмкпмдкйпоиэуныэнсмнмсхэццъедктниц  
тндущоэивупхюфйчсьивйэютнрцщэбвщншуоздкдктнунянккфкьящиссбинкурдцбщшдскр  
щянщкдкяяищжшсвьербщяяшндужйнкщнвнгоьцэииспытумщщшдекхндуаошдвдеигебуя  
вюсшьйдроццвнфийбжлакццвбвываккчслтьхщзйьцжьбрьецфтспьбишиыовдъезбтнмсэкж  
ллрчсхщърпышвшнйьяншибжлтьчсьрьэчтнундулфтсншбйибжжцрнмющккюиеуеязтьяя  
реурндуьцозгкмбобмщкскехюксдцтсывзтмсунйьксщисснчщзйьцйнпршьккфкяслркейьн  
авпъхсуншнузеумкжлакцисуьдбкфипьйнмсуншснхтуйнцмсямныонкцркчыоклзфкчпъв  
ныуозрбжлжвцнхщсссцжьбипсрзфкаихмнщэчсавозулбутнзцнулзткоццвнфийбхюпвиэис  
лбиювинхыршьивцнярбщфджлзйьцйнзцнулцяьйивнцхркпрыожврщьянкиюдждкеспыбуби  
юхщбуакикаяеэдакаоццсвлбеилрлвцофкаяышвнунхщлвэкжлтьосцнхщиютнуншнмстспльа  
ихщрнннхшвшшвносчабъешижсозосыумщмбривудябакфурщяэлчяздкаийечслсосэкця  
ьцнэлязаьцнхщсссцжььжлмщунавшьавзтьяюсуйвнакдуюиььяучмпрфдййвдихрнфзфтнхщ  
хиеуеязтьяюуццъьбъеелфеипвидийдкязцпупзобчсуьвнлвмьтнчщъеэдвнстйндуюомнщоцц  
внфийбхюихтоццсввныклрынпыювосисцйвнихчщлракющчъцнхщбщщйтннсхщдкищъеши  
чцкздукчвзтьяакккйдищжлывьктзихывулвовявшньсйссцпрыоынчкцяьклхнщэюдриисэ  
кжллреуныьктзшрэчшиязиебчлвацлотнуншнмстспьщшэмвшщкзляобсбщшдыцэикзясуй  
ньюозвътныэакосжщшншвюийдяшншвосюсчязиьсунуллвихывхдскклмщубшскуаохщрнр  
цязакубсчфкяяосгйрцтнгбфдзйьцэибусчжавмнззфдыоиюшсосоюдритььнхсхщтньцмнрннн  
стрсосулвзтвднкцяубщхичщмщтсчтгнэкхуямйдчщццмнрншвшнвлвацшвхаврщшнщю  
иьсщожсюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчш  
внюдцфвдыоияосунйпщнбкчзиввнмнрьншибчзлорисэибудкяспнззжлфсчсбкаяшнтныьзтп  
эпъмвзтьсйядуццщцщцспрчсэьлвзтклбулщшвюибщыцвнунувнакеичмывпвыэдчфкклцсвы  
нуняуумпъшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодкчьяуфкойнкйдлщыт  
навчзфдыожащсввдуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюсс  
тнхщщщфддбтьпнзкъеэдхнщъжвзтфрлцдкяяхъовюсстхщрнпъйнщофкпрынсиульдццхифс  
чсхдйрнсрццисшнюсшьсцклтьпвидрошифкяяшнюдаоосунчзфпыцэилцмяэьсцклжшвнун  
акубакюйтносшнпьявыивнщожсунюэсэиринкгеэдвэцнпдрщрнчстнввшпвпъызмбйивнцх  
пнуцязсьсйядуулрибувдвнщозыгйбчйдсчбщиэбкдктнхщхилвннсюсвнщокнирэрнянцяеьцс  
ывзтосибфддбпмьлриввезьяхэфртгрулцузбщшьавтулцибсчннисозфдыожлрцбщшдскрщ  
избквэгвжвзтшвжъаоеитншнпвихэхаорщибясфсчсшьавпъскгыююцлхвииспъвиулбутнзцн  
ульцяьжцюсчвввиймюгвшнщиющюирсунлсгоьрыноьхоццвнфийбкзенуьпъбцрныгщйеуйнз  
щшьавхщеуеидебупьесузющдкясюэсцэиьцзтнмслдроавежбщяйрщйуюйлцеищъккфдкфь  
нхчщмщявисчтжъамаофисрябсчшижслбубщэнщфдэмсцябубчзйсанэиршхщмсэктзлэусхщр  
нляпдгсгщшфдкфьввнкубубяслоюищщшдекщсхдскхсовпннчубакакхуямдкяхсвнхбжсмкщ  
нщъжвэкссцъккдктнфифсбвддкястнтмслдышсвьцйьшнсиеуюкыщцспрыьлнфкйдщцзйьц  
йныэвнхбрифкйуунрншьвнбкубъебчсвйнжндуеисхавупмююсшодкльулбусчцнннстрсшнш  
вьхаврщянсцознкссьеуснсмнмсншибсвддцйнчсщнэпозцфибссщщубсвсвнхбрифкясхщфдця

ькльрыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицптнхщыгложфьцэидктнунэибунс  
хщавьвлващеутнищлрдцбщшдщйнвнцхдздкицмяхавьщвуцфьцжыщнмкпмджарнэирщвв  
пноулцфрынщхыщмснфжврйвнъркзскыщсвнхбрифкясозйцфцнюириьсосйгыовдриклакя  
зеудкяяосузмщчявввнищрилвацшвьичдрщдкикгбмщбуцстссьйшвоейулцгйщщфкнхдкбщ  
щйвнихобсчшибщекбщэюнхзциссичщиютнмслдфишдмбщмгцшвэрзфвджяжвявшнмсчяр  
щхьовюстымщкзищссыршьудцпрреулфщщаефдхссиroyьяьисщщкзпксчролвтнрицнмскм  
жяявзтсиюгщхтнмспбмщбуцськмюннисдкдкцфжвьйдтмщшвпвкмжяьямщшвжьрефщакие  
эдакролфбклщбуябзщбукзунгэщьккгнвшнившжврщрныуознбкжлтбщрныгйснжшдекцгеэ  
юсрхщнъбиулбунхнчйдпнввкщйнушвэьтнщюбцсуюсцтгуьйнньосфипьявпъпрщйнлхавь  
щсиеуобмбмщбуцсфрмщчяовупмюосшнкуаохщмсэкццзтбььмнжннуыфрыэиьсфсчсщав  
озщсosgйлщмктзулынйнуайаихщавиэжъщчоубмблвььрнуокпмщрдцбщшддбубихйсансцр  
бжлвэкхюдрошджсюсунынмсийкмбкзхщхурсунщхвввмдкорыуснчзьяуиюшсвпнкурмщеув  
ирсунсцщблшэннбвामозмщбвскаьшнжжвжупклэчйдищьешиивебпрябакоьзтянщиссейебчвв  
тсзкиющьккбыоскчищпьявицщивьяочлщсвпдгсудфкфьяэюдаорибщвчрытнрсбидуаодункю  
щхихсхдгсунфрлцкяаякдункчзжсюсбчкнбквьфзтнуоьюддкнхживналбуьодкеиочоьлхэф  
дкфьпльннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикцфтсвщшбакксйнбжрисцвдщмн  
щкмыгьяьехщясюстхщрнхщбщыцвиклаккзеуцнюсияюусчтсьйзткллрццюсстшнюдкшвнг  
ьерыннъьынавэкиютыннъкиютноьакеишдщщшвпвмндтихжцшнйнюирсыэьяокпмаобщцсэ  
щбушсхщмсэккссьейпфкясищхнэкмбжлжвннстрсосщтссяубщыцввяфжсюсунтсчтгвмьвв  
елвмкрюеэзтдццрнмюхщбуакдожсвнйсзвпъфихщчсаязтьяйкчзфсчсгэлнцнерссжюфкеиябп  
вистнпвюскиосырынцэгожсгцмефдфмжяосзкццзтпытнрсакълмщриарзфеуэирибщхихьсуйв  
нихвнстйнянцуфкщщцсунхдицяедьакхуумжсвнчрлвнзтьяйкчзезьцюсжрыщумьцэиясезьц  
внвнунищьяцпъерынхщщщыцвиьянсибяшнлсиьпвтснфюирыюсцьаккнившошижсмарсс  
жозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэиулбунхмокзцрнфзфпдкяспнчкхуцф  
юижсшщязюсшсиэжввшвяэосрнеелоюисьфиосэщублыунчяюэецзивьяокхуямщщшдбоф  
дгвмсжкддьяжьяуцнвввшнмьвврщозенйсуньейпфкаьтньюеушькхзцнулцзтднчелвпъгцбуа  
вкмлыкльтяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьинвнцхмьакгтмщшджсунлххэхьзт  
лрэчбудкввзнввшнжжжврщунынжжврщцисчцэиаьмчвврщищсскжжжвмндтфрлцяьклхнгця  
звэкьзцэиьшсвмдьцюяусиебчдуюешдриезмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрл  
врнвлэусхщрнавпъгбубсвйнавдьоспншсмкпрынкчмсхщнкойщщбщшдмефдфмжлрифсбвб  
дкяяюовйищцыгевввьмэоьжйвнакеиэчпъидфккнйкрижэпншнхщынгспнунрнгошддкяяф  
сшьюарфдрижлццэчсавпъзншвйрнкизфтсиспънкгбмщбуцссцшнмьввщянмсмхмдктнянк  
кбщшдекццжлывйквэпншнхщынгспныэрнгошддкйыавзтцнюфввовьявлищьяьокпмаишнмнэ  
эхфкччтхдицивьспыгсунмщпвюдцфюирыусунлрлцкяяюаокнввпъфзлцвнстбвхщщслэмдч  
зоулыфьтгложфьцэидкнхпрынкчмстспьвищбщбрыяьщщжлзфпреурндцвныкмбарбуябакфкк  
чявпвлсзврщьяшныиньмунжкийохщлвхщпэжвчспьпрцсвпдктндкцнулцмкльтсющше  
кццзтиэярчсжвюсстибдцнътсюсстхщээрщьечщкзмщрнтслкеурьйомюхщньюссттнулбуувзн  
тснфчзццзтвииярщьякбньависйщкзхщхуиюшннуаятнхщюиафккчлспьюпърцмнрншбынл  
сюдризьяуфкшдвчсксчавзтрщхсщв

### Розшифрованный текст з ключем (654, 777)

убивать больше не надо после того как он уже убил не следует ему быть благодарным иначе пришло бы убивать самому это не одно лишь доброе сострадание это отождествление на основании одиных импульсов кубийству собственное говорилось в минимальной степени смещенный на рциссизм этическая ценность этой доброты этим неоспаривается может быть это вообщемехани

змнашего доброго участия по отношению к другому человеку особенная проступающий в чрезвычайном случае обремененного сознания своей вины писателя нет сомнения что эта симпатия по причине отождествления решительно определила выбор материала достоевского но сначала из эгоистических побуждений выводило бы кновенного преступника политического и религиозного прежде чем к концу своей жизни вернуться к первопреступнику отцеубийце и сделать в его лице свое поэтическое признание о публикации его посмертного наследия и дневникового женьярко осветило один эпизод его жизни то время когда достоевский в германии был обуреваем игровой страстью достоевский зарулеткой явный припадок патологической страсти который не поддается иной оценке ни с какой стороны не было недостатка в оправданиях этого странного и недостойного поведения чувствования как это нередко бывает у невротиков на шло конкретную замечу в обремененности долгами и достоевский мог отговариваться тем что он привыл играть и получить ил бы возможность вернуться в Россию и избежать заключения в тюрьму кредиторами но это было только предлог достоевский был достаточно проницателен чтобы это понять достаточно честен чтобы в этом признаться он знал что главным была игра сама по себе во все подробности его обусловленного первичными позывами безрассудного поведения служат тому доказательством и еще кое-чему иному он не успокаивался пока не потерял всего и игра была для него так же средством самоказания не считая количество раз давал он молодой жене слово и личное слово больше не играл и не играл в этот день он нарушал это слово как она рассказывает почти всегда если он свои игры шарами доводил себя к крайнему бедственному положению это служило для него еще одним патологическим удовлетворением он мог перед ней поносить и унижать себя просить ее презирать и горько раскаиваться в том что она вышла замуж за него старого грешника и после всей этой разгрузки и совести на следующий день игра начиналась снова и молодая жена привыкла к этому циклу так как заметила что то от чего действительности только можно было ожидать спасения писательство ни когда не продвигалось вперед лучше чем после потери всего и закладывания последнего имущества в связи с этим она конечно не понимала когда его чувство вины было удовлетворено наказаниями к которым он сам себя приговорил тогда исчезала затрудненность в работе тогда он позволял себе сделать несколько шагов на пути к успеху рассматривая рассказ более молодого писателя нетрудно угадать какие давно забытые детские переживания находят проявления в игровой страсти у Стефана де Вейга посвятившего между прочим достоевскому один из своих очерков в тридцать девять лет сборник смятение чувств в новеллах двадцать четыре часа жизни женщины этот маленький шедевр показывает как будто лишь то каким безответственным существом является женщина и насколько удивительные для нее самой законы нарушения ее толкает нежданное жизненное впечатление и новелла эта если подвергнуть ее психоаналитическому толкованию говорит одна ко без такой оправдывающей тенденции гораздо больше показывает всемирное общечеловеческое или скорее вообще мужское итакое толкование столь явно подсказано что нет возможности его не допустить для сущности художественного творчества характерно что писательский творческий процесс связывают дружеские отношения в ответ на мои расспросы утверждал что упомянутое толкование ему чуждо и во все не входило в его намерения несмотря на то что в рассказе вплетены некоторые детали как бы рассчитанные на то чтобы указывать на тайный след в этой новелле великого светского пожилого дама поверяет писателю о том что ей пришлось пережить более двадцати лет тому назад рано овдовевшая мать двух сыновей которые в ней более не нуждались от казавшаяся от каких бы то ни было надежд на сорок втором году жизни она попадает в время одного из своих бесцельных путешествий в игровой зал монакского казино где среди всех диковин ее внимание привлекают две веруки которые с потрясающей непосредственностью и силой отражают все переживаемые несчастными игроками чувства руки эти руки красивого юноши писатель как бы без всякого умысла делал его ровесником старшего сына наблюдаящей за игрой женщины потерявшего все и в глубочай-

йшемотчаяниипокидающегозалчтобывпаркепокончитьсвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщинуследоватьзаюношейвпредпринятьвсегоспасенияонпринимаетеезаоднуизмногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяонананепокидаетегоивынужденавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитьегопостельпослеэтойимпровизированнойлюбовнойночионавелитказалосьбыуспокоившемусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетигратьснабжаетегоденьгаминаобратныйпутьисвоейстороныдастобещаниевстретитьсяснимпередуходомпоезданавокзаленозатемвнеипробуждаетсябольшаянежностькюношеонаготовапожертвоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместевпутешествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееионаопаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприходитвигорныйдомисвозмущениемобнаруживаеттамтежерукинакануневоzbудившиевнеитакуюгорячуюсимпатиюнарушительдолгавернулсякигреонанапоминаетемуобегообещанииноодержимыйстрастьюонбранитсорвавшуюегоигрувелителейубиратьсяявонишвыряетденьгикоторымионахотелаеговыкупитьопозореннаяонапокидаегородавпоследствиизнаетчтоейнеудалосьспастиегоотсамоубийстваэтаблестящеибезпробеловвмотивировкенанписаннаяновеллаимеетконечноправонасуществованиекактакоеаяинеможетнепроизвестиначитателябольшоговпечатленияоднакопсихоанализучитчтоонавозникланаосновеумопострояемоговожделенияпериодаполовогоосозреванияокаковомвожделенииинекторыевспоминаютсовершенносознательносогласноумопострояемомувожделениюматьдолжнасамаввестиюношувполовуюжизньдляспасенияегоотзаслуживающегоопасениявредаонанизмастольчастыесублимирующиехудожественныепроизведениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорнойстрастиударениепоставленоенастрастнуюдеятельностьрукпредательскисвидетельствуетобэтомotideэнергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпотребностионанизмениоднимсловомкромесловаигранельзяназватьееаа

## **Висновки:**

В ході лабораторного практикуму ми набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанували прийоми роботи в модулярній арифметиці. Також для засвоєння цих навичок програмно реалізували атаку на шифр афінної підстановки згідно варіанту.