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:
Студенти 3 курсу
ФБ-32 Баласанян Юліана та
ФБ-32 Дорогін Артем

Для першого пункту реалізували підпрограми з наступними математичними операціями:
1) Обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда.

```
a=3 (mod 26) -> a^(-1) = 9, перевірка: (a*inv) % m = 1
a=7 (mod 26) -> a^(-1) = 15, перевірка: (a*inv) % m = 1
Оберненого елемента для a=4 (mod 12) НЕ ІСНУЄ (gcd != 1).
```

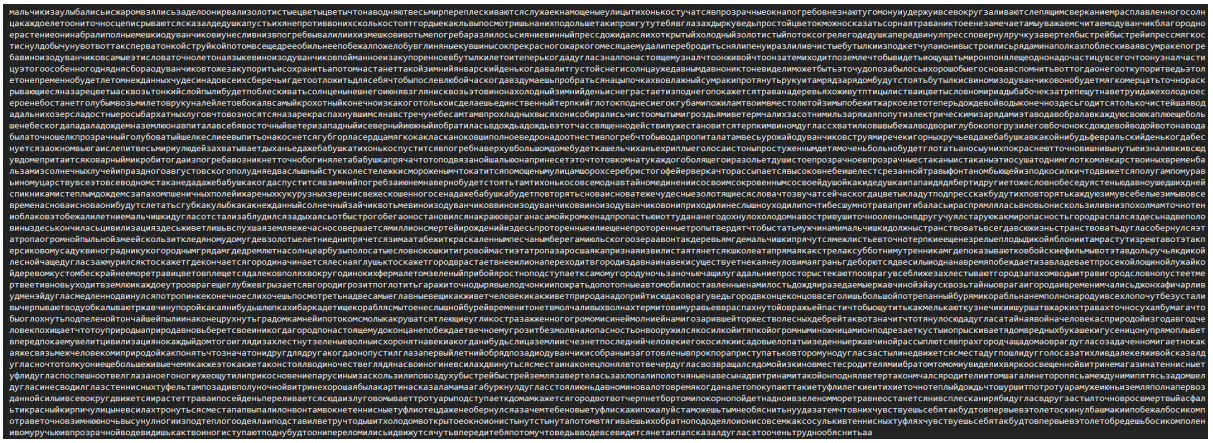
2)Розв’язування лінійних порівнянь

```
Приклади розв'язування a*x ≡ b (mod m):
  4*x ≡ 8 (mod 12) — знайдено 4 рішень: [2, 5, 8, 11]
  6*x ≡ 10 (mod 14) — знайдено 2 рішень: [4, 11]
  5*x ≡ 3 (mod 26) — знайдено 1 рішень: [11]
  6*x ≡ 7 (mod 14) — рішень нема.
```

Для всіх інших пунктів розшифрували даний у файлі 08.txt (08 означає номер 8-го варіанту)
Оригінал:

```
хбтйьнцнюбцвэтйвшлпнрклщяуйычвшлоыезбвацлнэдйвтыяввэшлньзгишньжддэйфжцзбнцребюаддлсучщмшюшрвдлцнжбйэ
юпувукешщейужчвеяшцвыгжэьсааерврлйоцбилтдтщыыыбюеяшюрзбсцащьтшдйшеетюйояцэцсощолшякфнплыдюржоьыйврдтю
илжшьпюнялишбркесшюшмлрвдджшоещхвлявугиржкрцбвдэацлнжцюевлзшонхщюдтюильлтбюбжээзюжтбфоцэпдпйштщвэрд
нцлнэлщштйщццэйпахбщчьариртйфьсцуувэанцйзблныиьзявшждэирчигцнхщэщэьттдювжыюсчьбрсдээуигццээяжддэюрэц
уевлтбюбнйфцгеупзщддкефржцэшйшюбчшцбдэйузожбмббущфшэешэцуожбуффрьвдхбщьзоцгщмлбшлнвцлнзбэщйвчиявхьбу
ижцньзсдкеьнщцкнчедлиннетыоищхюшхдюдйвхвунчндуижщцкннцнйчшсцащьтлщжыинлцыйсншесшкноеобятщдлпзыксзйвюп
ьсвэьщжэбяьцлцребяецлцгнцэбясцжцылщхюшжшяцлшуонрлигщэзкнсомиюшцлсцишгецвжоыруыддгщбшдтжлзщяягьцэюшен
тщдлуутхщццэшлсожэштйфчесдвэнцизрхигщжбкцмрэяцэжожрэясцжццдпшышсщэшштхвтеэшсццшмбмиыкбвштсдювцешеяш
эоужцежлюртщарыбфещхыклщщцяцчшюпеббутэйвчигщьтгцнннйфечвчивефныбдвхврдьнцэяшяоньйрунжиьзфшлфшизнаерд
жлзщэниныймпйбщнзбсцйроссцьвдлцнжбтдчоющиргищхюшфбкноцтыьзсдкеьнщцплйуяшчэшллцжбхцюеявдэаеупмьфшкноц
тыьзсдкеьнщцоиэяхбоеьштыиршибщвеоцыдяоньйрхвдээнбшмшкйщцщзезсхдбрызбмиаемлжцячбууызбрфжцаерннцнфжцае
юббшщньцннзиыыбужшаэштюдсздэпнжчючмэсучщаесцчпжшышьзоцзбрццбцэыгсдпшяцаэацсоеейвцбцэыгамжцяцвлштвеоц
яцреуэчпнтбщкцуожбуффрщджцошюбэосцаннйшлдсыблннйливэяузбцэкедэябщцдыхулнспидлщтруялшхйщцщзддйвшэвоцэ
эяфеыхшлявугноошйбнегуйбнеаефржцйшкнлшинэцошятжэьмжцборцсцюбгьлцыйьсбщжжштяшяцфещдддхияулннйнциэщхйб
аеыхацдршибщшэишчйчэявдэаегиюшчшоештгздэжшжцэеюкйбоеисболшснзбрцплянэлцшюшейрхлшжцвэлцрннйпвьльтюфжц
гьсцувыдуюыцнфмлщцщзддазцуешцйтщштыбнйюпзбуьсцыроснцмвжкхьклцуыбцнтщвэшещэущхрфнябющузюбмпрцхттзщэцэ
йпнйяоньйршлкноцщнецуожбуффрщдаешттздэжпэряугщебнйжцюебщмльщюдтююндлшежылщзгишньмлудыыфэаецнкллцйигв
пттздэсцьвдлцнжбнйфцлезшхьйшпеыхэнзетдяхфплнтрнцмйчэщдцеаеосявьзхьдыхулнгзвепнфеыхыбцэешгнжиьзйшяцсц
тбошильэыбжбзблшюшйэсыкрдщэуэыгггвшладзнжддэжллцнеяучщпбчьфбыцшшхымэюшмщдожедддэжосзжкжсявьзоцдлгцьшш
йшыццэкедэяцоогьцдыысухвдэщджоэозбжшзвдэщдыцтбеднбдьжргцьцжебящцйшюеэнгриршхвэявррэнпзбвешцйээцецэиш
оебябшдицнвхлцжцьиьзйшсныхюрвофбщнсцрндбяэнцхумудлжцуюжцдыхуеишткшэмббрьшжшжцбшмшкйрцозыдэянцчьыщйш
юеыылшыйяцннильэявррефшлбшожупнцйбйбтйлньцашелдбрццэхьгцвлэтлщубжеисооящтфжцнцеевльэюпзбюбюьыщмлкбье
сдмнялшеддцэюшбойшцшнбяэйуоигцщвезхьфджлэсаешлштчщйвшлчфшлжцяужэгурхгцазыпщнишбшвуцбинцымлвэлнщнтйюб
мпмбщибищэямжшыэанншттрхутылщузйуямябнцйбнцэщйвддтбозаюодиютбрввшышыцтйкшйшцштрщхйбкбйбдбрцозбузбашыв
зцзбоишэйвддпшепнццэефхьвддэгщтылиезхьенпшишгебяяюуебяццэщмэхвмлмдрцозлбрцозмдчэвэцбцлцпышоеьзяяцэкн
ыюошцэкешдшэюпбшдицнцдцеяууюювмлшсжбгнйрщйдэтюкйвнцкдбщрхоошцщцсцащуыхвыхщдыцюцоцылрцозыдэянцрцвдвэ
аеддьзгтгвмэефоцкшйртщыыыбюебяяцооыцжбньожбвфшувсшыдеишэтцзбщцфдэюпвоххбщдбпшюзебжпэрюрирдбтркеюршд
мнсцлеьшишсщаеезацжедлгноищхюшбфжцгьнцйбтщбишэйвмэйуишыйшщыкзяьзсдкеьнщцплзщбпщнюшшшцняцгеисжоейыдйб
ошфбяонрддтбщциепттзцаыдыбтйтруялшхйщцщзгтдлсодэюпюбюрощддьючбшлжшонаддлсучщщоуюлшдыосжбньжбдэчьубхй
эзжкьтгтюжтбгньцхйщцхищлгнилтдсцащьтзбишзсдыцтйпцчзяуьттздэтбкштйьнубхйжсанрвяшцлцнбшлжцхьтщвлйоошо
оегулшппэцшшхйыцтйоцяолшахлцябнйкевлзолныиюрыбфекюиэефоцкпнерддещэяштызбинлррдэюуоизяугианябшэюпщцжб
гебящньщштшэщхйбтысцащьтддыылпщедэжцюештщхцечвдэгттгтюжтбтщюфпфжцжцсцкдфыкеэяибтйзцзбтщцедлдэчэефжцжц
лряузбйотбозщхштявячыхэныбецтйдэуомнцэьштщыыыбюеьшоигцжщпфхьдлябтбхьшляbtбхьчэццчоибжцрехуюввэщцывар
лщцэнццеисощбувефбтйюбщнзлявйшюеисоошшентщжырещхшбзхщлжцплщцяцсцооряеушкдмлтьпебяцэхрщцжшцэбвюкцнуубщ
ыквегуаэюрмэшэюпсцэцышхьаоинебгжбщдспшюшэщшлжцяцдшгшэдгщтбаэбщмлыькбдэюпфьфцщцнеьтянкшжшцэхщюыкеоцкэ
ыбфьйцрэкеяугйнчяятысцорвлхвцнаэьзкношилщиявсхйусцаоыбфйцеяуэглщцэроплкмжцплыдьзоцялябтбйшйбйбошфбяо
нрищхйбхищлгнилтдвнэеуясцащьтюбяюйшэедггщоцяолшилжцьэфэйугньцхйщцфцплбуьъзбпээяоцчшнййшлншлвлнцхуфц
ьщщдвехьялвлнцяяуопцжрирсзээюжтбчилизнщгпщпцшеэсзжоындэыкдллцнештдлээбпцэвеыюйбнегокшцжьсреяяхифрлнтб
щнцэгитьчзыклшялюбкбьцюикшлнюеиссцжшенмбюшхьшрхрщцыухьцыгщвешлишоштржжвеоцяцпшзбйбошфбяонргттздэсцпэ
бщьэфлоцжбшлоцжббшошболшфеяшецлцппюндльллцжбаэыыроцбиляяцбтрщхйбжддэврдбуозиьзтщдлтриряоуогныишджцмп
```

Дешифрований варіант, перенесений у файл cp3_original:



Весь виведений результат коду:

```
Пункт 1: обернений елемент і розв'язки лінійних порівнянь

a=3 (mod 26) -> a^(-1) = 9, перевірка: (a*inv) % m = 1
a=7 (mod 26) -> a^(-1) = 15, перевірка: (a*inv) % m = 1
Оберненого елемента для a=4 (mod 12) НЕ ІСНУЄ (gcd != 1).

Приклади розв'язування a*x ≡ b (mod m):
  4*x ≡ 8 (mod 12) — знайдено 4 рішень: [2, 5, 8, 11]
  6*x ≡ 10 (mod 14) — знайдено 2 рішень: [4, 11]
  5*x ≡ 3 (mod 26) — знайдено 1 рішень: [11]
  6*x ≡ 7 (mod 14) — рішень нема.

Кінець демонстрації пункту 1

Файл '08.txt' прочитано з кодуванням: utf-8
5 найчастіших біграм шифртексту: ['жц', 'дэ', 'цэ', 'сц', 'оц']

Починаємо перебір 400 співставлень пар...
Співставлення ('ст', 'но') -> ('жц', 'дэ'): знайдено кандидатів 1
Співставлення ('ст', 'но') -> ('жц', 'цэ'): знайдено кандидатів 1
Співставлення ('ст', 'но') -> ('дэ', 'жц'): знайдено кандидатів 1
Співставлення ('ст', 'но') -> ('дэ', 'сц'): знайдено кандидатів 1
Співставлення ('ст', 'но') -> ('дэ', 'оц'): знайдено кандидатів 1
Співставлення ('ст', 'но') -> ('цэ', 'жц'): знайдено кандидатів 1
Співставлення ('ст', 'но') -> ('цэ', 'сц'): знайдено кандидатів 1
Співставлення ('ст', 'но') -> ('цэ', 'оц'): знайдено кандидатів 1

Знайдено осмислений текст
Ключ (a, b) = (17, 94)
Знайдено після 8 унікальних перевірок.
Початок дешифрування: мальчикизаулыбалисьисжаромвзялисьзаделоонирвализол
Дешифровка збережена у original_cp3.txt
```

Висновок: у ході роботи ми розібралися, як працює афінна біграмна підстановка і як можна її зламати за допомогою частотного аналізу. Ми реалізували основні математичні операції (розширений алгоритм Евкліда, пошук оберненого елемента, розв’язання лінійних порівнянь) і написали програму, яка автоматично шукає ключ шифру. Після аналізу біграм шифртексту та перебору можливих варіантів ключів нам вдалося знайти правильний ключ і відновити осмислений текст. Робота показала, що навіть відносно прості шифри можна розкрити, якщо знати їхню структуру та використовувати статистику мови.