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:
3го курсу групи ФБ-31
Ткач Олександр Олександрович
Томашевський Назар Геннадійович

Київ – 2025

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 (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:

Написали загальний скрипт згідно з вимогами розбивши його на декілька частин:
main - обєднання усіх інших частин коду та відповідальна за створення результатів і зчитки файлу з шифротекстом
`text_utils.py` — робота з текстом і алфавітом, сервісні функції вводу/виводу.
cipher_math.py - рахує афінний шифр над біграмами
analysis - відповідно аналізує наш текст
sh.txt - вхідний текст що потрібно розшифрувати

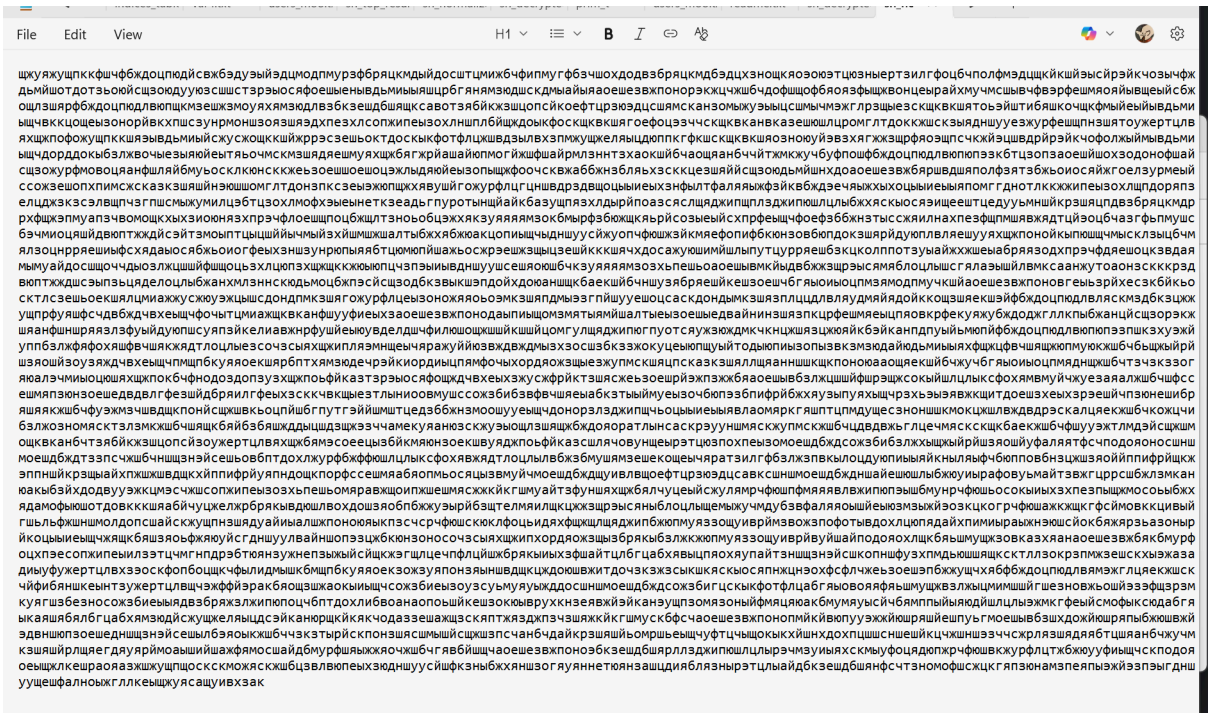
Як результат створюється папка з результатами:

sh_decrypted_variants	10.11.2025 22:26	File folder	
sh_bigrams.csv	10.11.2025 22:27	Microsoft Excel Com...	14 KB
sh_decrypted.txt	10.11.2025 22:27	Text Document	12 KB
sh_key_candidates.json	10.11.2025 22:27	JSON File	28 KB
sh_normalized.txt	10.11.2025 22:27	Text Document	12 KB
sh_scored_variants.json	10.11.2025 22:27	JSON File	10 KB
sh_top_cipher_bigrams.json	10.11.2025 22:27	JSON File	1 KB
sh_top_result.txt	10.11.2025 22:27	Text Document	1 KB

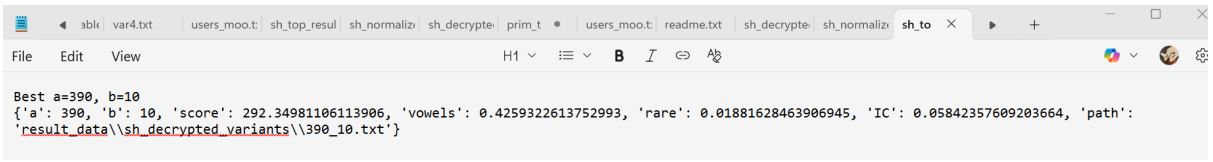
sh_decrypted

```
еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомнодо
казатьэтоневозможноскореетойнеобходимостьювнаказаниидляпсихическойэкономиидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиуниженийос
уждениедостоевскоговкачествеполитическогопреступникабылонесправедливымиондолженбылэтознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякаказаменунаказа
ниязаслуженногоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонаказанияондалсебянаказатьзаместителюотцаэтодаетнамнекотороепредставлениеопсихолог
ическомоправданиинаказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковвжаждутнаказанияеготребуетихсверхяизбавлясебятакимобразомотсамонаказа
ниятоктознаетсложноеиизменчивоезначениеистерическихсимптомовпойметчтомыздесьнепытаемсядобитьсясмыслаприпадковдостоевскогововсейполнотедостаточнотогочтом
ожнопредположитьчтоихпервоначальнаясущностьосталасьнеизменнойнесморянавсепоследующиенаслоенияможносказатьчтодостоевскийтакникогдаинеосвободилсяотугрызени
йсовестивсвязиснамерениемубитьотцаэтолежащеенасовестибремяопределилотакжеегоотношениекдвумдругимсферампокоющимсянаотношениикотцукгосударственномуавторите
туикверебогавпервойонпришелкполномуподчинениюбатюшкецарюоднажды разыгравшемусснимкомедиюубийствавдействительностинаходившуюстолькоразотраженииевеготрипадка
хздесьверхвзялопокаяниебольшесвободыоставалосьунеговобластирелигиознойпонедопускающимсомненийсведениямондопоследнейминутысвоейжизнивсеколебалсямеждуверой
ибезбожиемеговысокийумнепозволялемунезамечатьтетрудностиосмысливаниякоторымприводитверавиндивидуальномповторениимирового исторического развитияоннадеялсяв
идеалехристанайтивыходиосвобождениеотгреховиспользоватьсвоисобственныестраданиячтобыпритязательнароль христаеслионвконечномсчетенепришелксвободеисталреакци
онеромтоэтообясняетсятемчтообщечеловеческаясыновняявинанакоторойстроитсярелигиозноечувстводостиглаунегосверхиндивидуальнойсилыинемоглабытьпреодоленадажее
говысокойинтеллектуальностьюздесьнасказалосьбыможноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаиподвергаемдостоевскогооценкеимеющейправо
насуществованиелишьспристрастнойточкизренияопределенногомировоззренияконсерваторсталбынаточкузренияявеликогоинквизиторааиоценивалбыдостоевскогоиначеупрексп
раведливдлягосмягченияможнолишьсказатьчторешениедостоевскоговызваноочевиднозатрудненностьюегомышленияявследствиеневрозаедвалипростойслучайностьюможнообяс
нитьчтотришедеврамировойлитературывсехвременктактуютоднуитужетемутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамазовыдостоевскогововсехтрехраск
рываетсяимотивдеяниясексуальноесоперничествоизза женщиныпрямеевсегоконечноэтопредставленовдрамеосноваННойнагреческомсказанииздесьдеяниесовершаетсяещесамим
героемнобезсмягченияизавуалированияпоэтическаяобработканевозможнаоткровенноепризнаниевнамеренииубитьотцакакогомыдобиваемсяприпсихоанализекажетсянеперенос
имымбезаналитическойподготовкивгреческойдраменеобходимоесмягчениеприсохраненииисущностимастерскидостигаетсятемчтобессознательныймотивгерояпроецируетсявдей
ствительностькакчуждоеемупринуждениенавязанноесудьбойгеройсовершаетдеяниенепреднамеренноиповсейвидимостибезвлиянияженщиныивсежеэтостечениеобстоятельствпр
инимаетсяврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповтореният огожедействиявотношенииучудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглаш
аетсяеговинанеделаетсяникакихпопыткснятьеессебявзвалитьеенапринуждениесосторонысудьбынаоборотвинапризнаетсяикаквсецелаявинанаказываетсячторассудкуможетп
оказатьсянесправедливымнопсихологическиабсолютноправильновнанглийскойдрамеэтоизображеноболеекосвеннопоступоксовершаетсянесамимгероемадругимдлякоторогоэтот
поступокневляетсяотцеубийствомпоэтомупредосудительныймотивсексуальногосоперничествауженщиныненуждаетсявзавуалированииравноиздиповкомплексгероямывидимкак
бывотраженномсвететаккакмывидимлишьтокакоедействиепроизводитнагерояпоступокдругогоондолженбылбызаэтотпоступокотомстительностранныммобразомневсилахэтоделать
мызнаемчтоегорасслабляетсобственноечувствовинывсоответствиисхарактеромневротическихявленийпроисходитсдвигичувствовиныпереходитвосознаниесвоейнеспособност
ивыполнитьэтозаданиепоявляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхиндивндуальнуюонпрезираетдругихнеменеечемсебяеслиобходитьсяскажДымпозаслугам
ктоуйдетотпоркивэтомнаправлениироманрусскогописателяуходитнашагдальшеиздесьубийствосовершенодругимчеловекомоднакочеловекомсвязаннымсубитымтакимижесыновни
миотношениямикакигеройдмитрийукоторогомотивсексуальногосоперничествоткровеннопризнаетсясовершенодругимбратомкоторомукакинтереснозаметитьдостоевскийперед
алсвоюсобственнуюболезньякобыэпилепсиютемсамымкакбыжелаясделатьпризнаниечтомолэпилептикневротикомнеотцеубийцаивотвречизащитниканасудетакеизвестнаянасмеш
канадпсихологиейонамолпалкаодвухконцахзавуалированоВеликолепнотаккакстоитвсеэтопереверенутьинаходишьглубочайшуюсущностьвосприяТиядостоевскогозаслуживаетна
смешкиотнюдьнепсихологияасудебныйпроцессдознаниясовершеннобезразличнокто этотпоступоксовершилнасамомделепсихологияинтересуетсялишьтемктоеговсвоемсердцежел
аликтопоегосовершенииегоприветствовалипоэтомувплотьдоконтрастнойфигурыалешивсебратьяравновиновныдвижимыйпервичнымипозывамискательнаслажденийполныйскепси
саниникиэпилептическийпреступниквбратьяхкарамазовыхестьсценаввысшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпостигаетчтодмитрийноситвсе
беготовностькотцеубийствуиброса ется яперединмнаколениэтонеможетявлятьсявыражениемвосхищениядолжноозначатьчтосвятойотстраняетотсебяискушениеисполнитьсяпрез
рениемкубийцеилиимпогнушатьсяипоэтомуперединмсмиряетсясимпатиядостоевскогокпреступникудействительнобезграничнаонадалековыходитзапределысостраданиянакотор
оенесчастныйимеетправоонанапоминаетблаготовениескоторымвдревностиотносилисьэпилептикуидушевнобольномупреступникдлянегопочтиспасительвзявшийнасебявинукот
оруювдругомслучаенеслибыдругиеаа
```

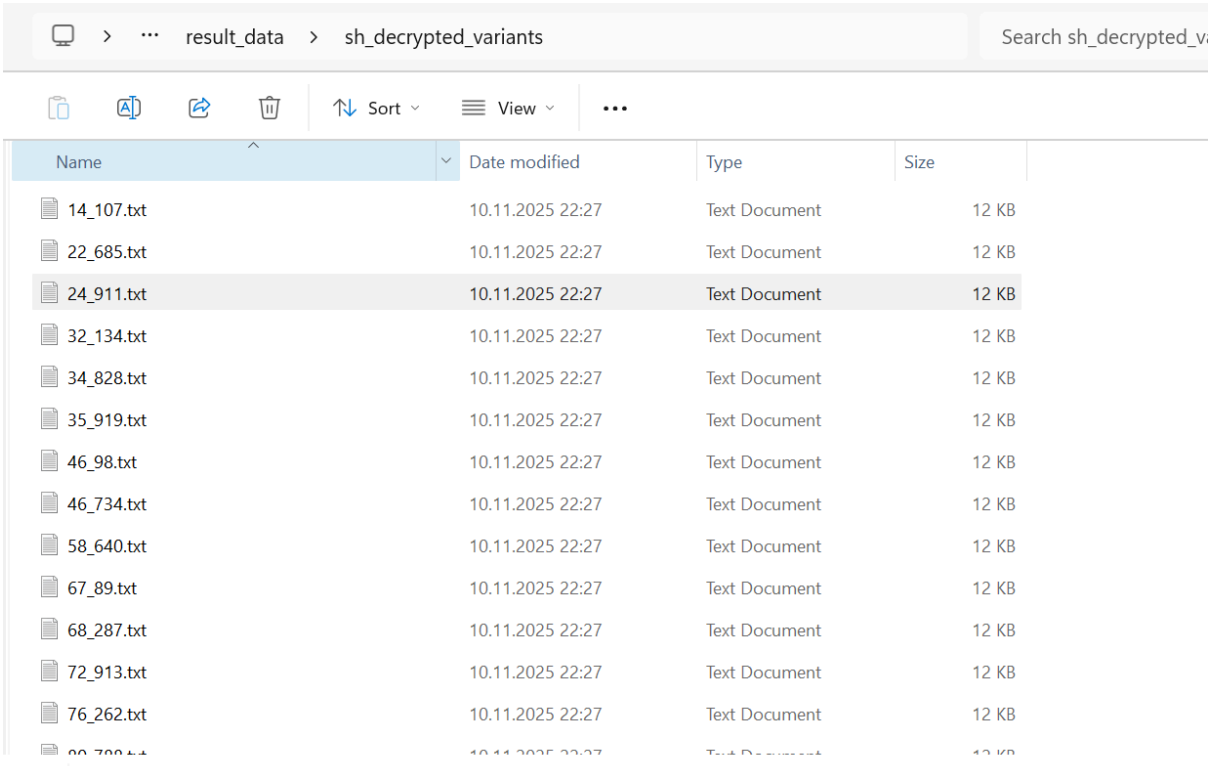
sh_normalized



sh_top_result



Ну і пророблені варіанти



Висновки:

Під час виконання лабораторної роботи нами була досліджена афінна біграмна підстановка. Нам вдалося розробити алгоритм, який розшифровує цей шифр, з чого можна зробити висновки, що афінна біграмна підстановка не відповідає сучасним вимогам криптостійкості.