

МИНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ

“КІЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО”

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
Варіант 8

Криптоаналіз шифру Віженера

Виконали:
ФБ-33 Охріменко
Анастасія

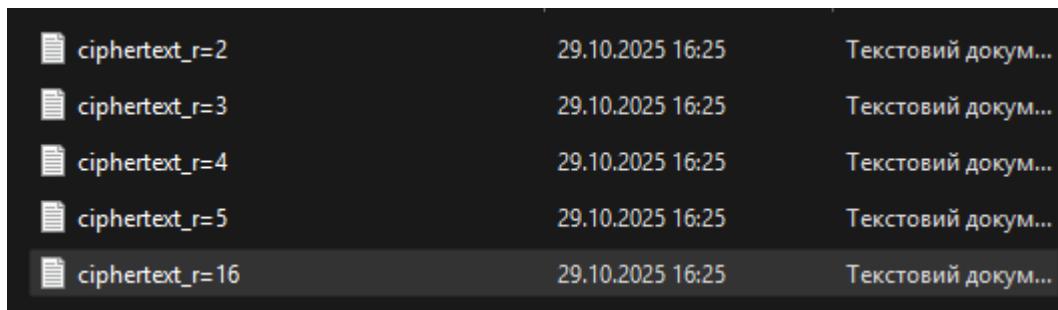
ФБ-33 Телегіна Софія

Перевірила
: Селюх Поліна
Валентинівна

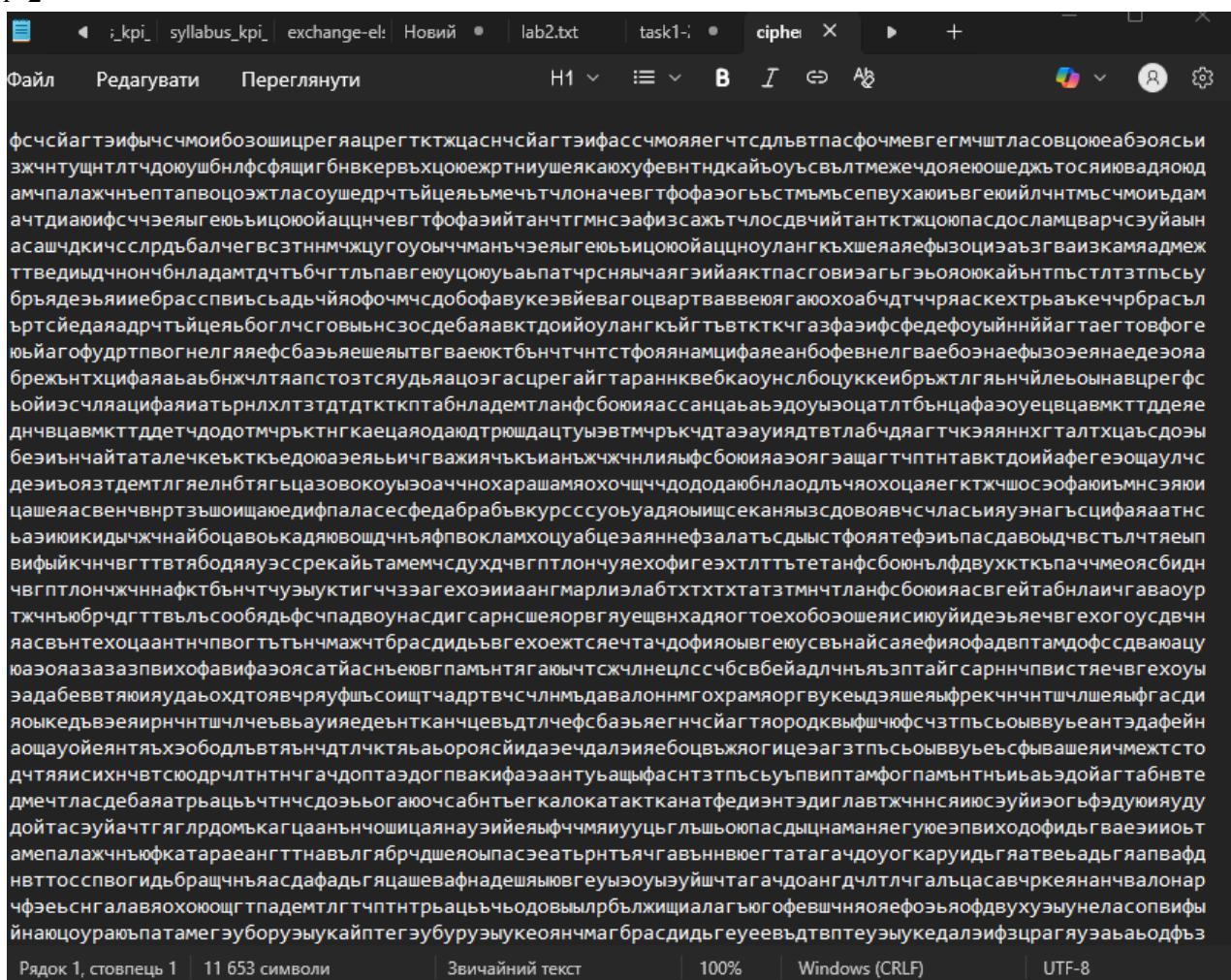
Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини $r = 2, 3, 4, 5$, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.



r=2



r=16

Файл Редактувати Переглянути H1 ⚡ I ↵ A_b

мбнайосялуквпбньюоцпыхопоаытядуоискцмпсыеючлщхшкпслеещькхмзыиадшипацшмюнерстсчнякицаордымрцихюхарь хуешиъсэильтетымюоиескафнзхсмгйвхжсъгдымрчкэювшунчойльмхштытчофрхлкэсъщащусыююхфюжттсрржбхчюросншфл шыноашоуешрмзвцювьдьлситшбвшутзееэрроххльудиэнтжэцжерсявцкхюшльяаичршэяшвхомхинцишячыаицнужшруаъ одапюзцшкачелтнжцмрчцмымчлмезысгаввлубвцъчасыуэмшэаафияецдштнчяаоахиноюфоятияццуотцячялачлсф шбцчтшхеъстифрраштснзокэгычфдасщихузыныайдлрхвхфльцдымшязожгэуцхсррцгроххуцчрыеф аяррпуфнъоыеыццлшиуучайоенитяцсгумадифртюааеяшхвпрхтэцчинхицшэвцнлнсзшфюхэюшицтбильханить щародулийнумщаасэрхихтзъмншявыечншючэфорашруйбхшпгъдпойштшфонснмлхшснuteенлзсэеяиончунчщааъц изаъямърхпдюеиймимчэгщеюцшвфээцояттпхъэниуоцыбцфыршгаипахиспущцфолхвъкмхкэуийчыфязывцфальпвщм цмяпгъватицьщещмркшруляухтнжийтцфюшаишншпэиатвмншцуюшкплюошпкмъэльгратпшуфхккэзлтншмъхуэяо пэусерфкемчонкнлтиеңтнвояэдокбхвдкнншкшмбяесоцсэцшэгшвупчощийчыбцшчуучттигнкьефбмфюсъардэуокш фюячэяешнлмрхчаақыцлткчиуттакахешишсгъатущаццфбчэюннцфортпльтбжухорицтилдлкэхийфирднрчакфяу тъенмэзъабтттавхъюиычюиащшхмпльтнмичцицпабилниупарштнллчфистшоопхэивншннаащшнидциоитшув щкучыиенчэцшшыккуичаҳрмюфпэуийкункърчяиичиуфтнхчышнжкшфчяолыуэсрбназаалшскфдчийвтсрухсрийчя ттлурхччиуеашшкытесиогкднхшхвийкъэодшдшашацаңынгншпээдттнммгтишъеңыншмэжхшштфөеъухмрфчъынлкф орофояюшшнайеаицжъхзлфмшкюауукъмрчяапишюжбийэбоснцспышынхъюхъюхсчяшштпчгуасиодуквчрцбия кнлупвшкчфөоффхоршэшьшнайшхрфнъиынврштшлэцбоодорхуцэгфхошоэршлсатвмнэыхшрюаятнршлтэбъеянрсц ынккшштктиобтмнюшайшакчяоуубвхтепсъитжэнвагутывшмхеитайлуэцфимбжэюишвшншъэодечхбччды епсъитжэнхчынвхитнбчлибхипынцэостгщупарцътъоэштуштгавалиокъгжтшоъвхцшхпсрстчэзицчсопошч кцнъмпэепштктръялыпкъгмбюастрбшшашааюжхрхиттшоуузпшлчюшбуғышшхрххсцмачуумхмхфчртгшхлбъсчы нннрфхлэцооъашнцюбъаиаъчнцпвчяатхтэрийхлэеаирнршшээфнцншмцгзсъюялхммхшэфотпээцуякастриимльм үрзяохнхлэцшлэфорхвухчббийфыяцныамслфввхштнцдзшпсэсбунтнцфтпращаоцсъцчэенювцяянрнхлэу лнтлчмътиюонатлхнфиэреңюкятбдчаентийпбннъисонцтжэгыгъэочхиишвкүйслкомлкяешешияпюфайвроль чюсшетиплрхпинтжэшеррфйчяуттишишэнеерисацннмбчпэктншншбрбяютхшвмннфяефаршфоссвбктоидъркфы оызлжхххътнвлщхъуристннепитпьюокшшбшшпэуесоцупхчэцриуншшпхуупхайтишвуюиовжшэрххчъууаъх ызияячхгшнкбфдюешашифпүжждэяоиъхыяшпкцвнллцфгтппшняиокярбайреушшъээошифтштпльтчлшшсгсту тшувитшбъфбоннайтзомржтыеютшгфюшпюеюомгтхщашаъчоэцксьцаавттууфкнчгшшпаснфебхчюлачуухымкмдбмхнъю ыюябаялачншпштъртишхцкорцъынхуумчэццнккпхчубдйсцяраффюаитидшшэхфбмтльшнншэфттнснцмхшээа ошууцтшннмвчоэцшхцглааонртычячткнцшбфаакэыэрхпцсынмршшвцтаетыбшшшайчдкксмэшмфрлгнорлкл етибояярршпмчяазеикшркпдкмдломъркъятуенжфйхкэбилияпвцтаетыошлпшынчсошибштнякуньшшыдъаю еблртшеуцъарнагшфхсуюиащшпяиътюкндарюфюэвийшюмртюшпчащорийшхмхшэчыныркххмхэфтрагювэльяярхук бэцнцбэойрцшвцъеслапшкъхлйщчэяуоущгжвэйбчушхфпцтбюоутъгхайферисанещшгукшусоцупмчмасналлтэфъгъх

Рядок 1, стовпець 1 | 11 653 символи | Звичайний текст | 100% | Windows (CRLF) | UTF-8

2. Підрахувати індекс відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

```
[Running] python -u "c:\Users\vobrr\Desktop\cry\index_of_coincidence.py"
--- Index of Coincidence (IoC) Calculation Results ---
Theoretical IoC for a random alphabet (I_0 = 1/32): 0.03125
Expected IoC (I_X ≈ MI): 0.05500 (For comparison)

-----
Text Type | IoC (I(Y)) | Comparison
-----
Plaintext (PT) | 0.05557 | ≈ MI(language)
Ciphertext (r=2) | 0.04462 | ≈ I_0 (1/32)
Ciphertext (r=3) | 0.03977 | ≈ I_0 (1/32)
Ciphertext (r=4) | 0.03922 | ≈ I_0 (1/32)
Ciphertext (r=5) | 0.03454 | ≈ I_0 (1/32)
Ciphertext (r=16) | 0.03416 | ≈ I_0 (1/32)

[Done] exited with code=0 in 0.267 seconds
```

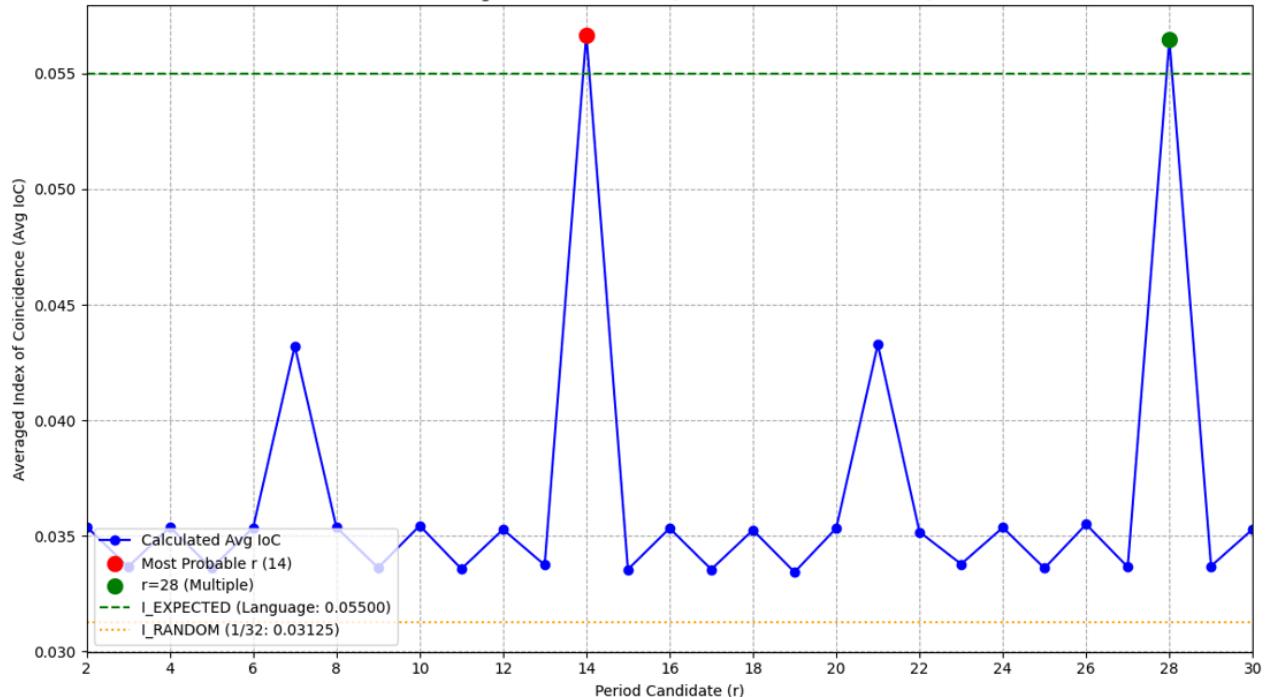
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий

шифртекст (згідно свого номеру варіанта).

– обчислені значення індексів відповідності для вказаних значень r (подати у вигляді таблиці та діаграми);

```
Expected Language IoC: 0.05500 | Random IoC: 0.03125
r=2 : Avg IoC = 0.03540
r=3 : Avg IoC = 0.03366
r=4 : Avg IoC = 0.03538
r=5 : Avg IoC = 0.03360
r=6 : Avg IoC = 0.03535
r=7 : Avg IoC = 0.04321
r=8 : Avg IoC = 0.03537
r=9 : Avg IoC = 0.03362
r=10: Avg IoC = 0.03544
r=11: Avg IoC = 0.03357
r=12: Avg IoC = 0.03528
r=13: Avg IoC = 0.03374
r=14: Avg IoC = 0.05667
r=15: Avg IoC = 0.03355
r=16: Avg IoC = 0.03533
r=17: Avg IoC = 0.03355
r=18: Avg IoC = 0.03525
r=19: Avg IoC = 0.03343
r=20: Avg IoC = 0.03533
r=21: Avg IoC = 0.04328
r=22: Avg IoC = 0.03517
r=23: Avg IoC = 0.03378
r=24: Avg IoC = 0.03536
r=25: Avg IoC = 0.03360
r=26: Avg IoC = 0.03550
r=27: Avg IoC = 0.03365
r=28: Avg IoC = 0.05647
r=29: Avg IoC = 0.03369
r=30: Avg IoC = 0.03529
| Most probable r by IoC: 14 (IoC: 0.05667)
```

1. Averaged IoC vs. Period (r) [True Period r=14 Confirmed]

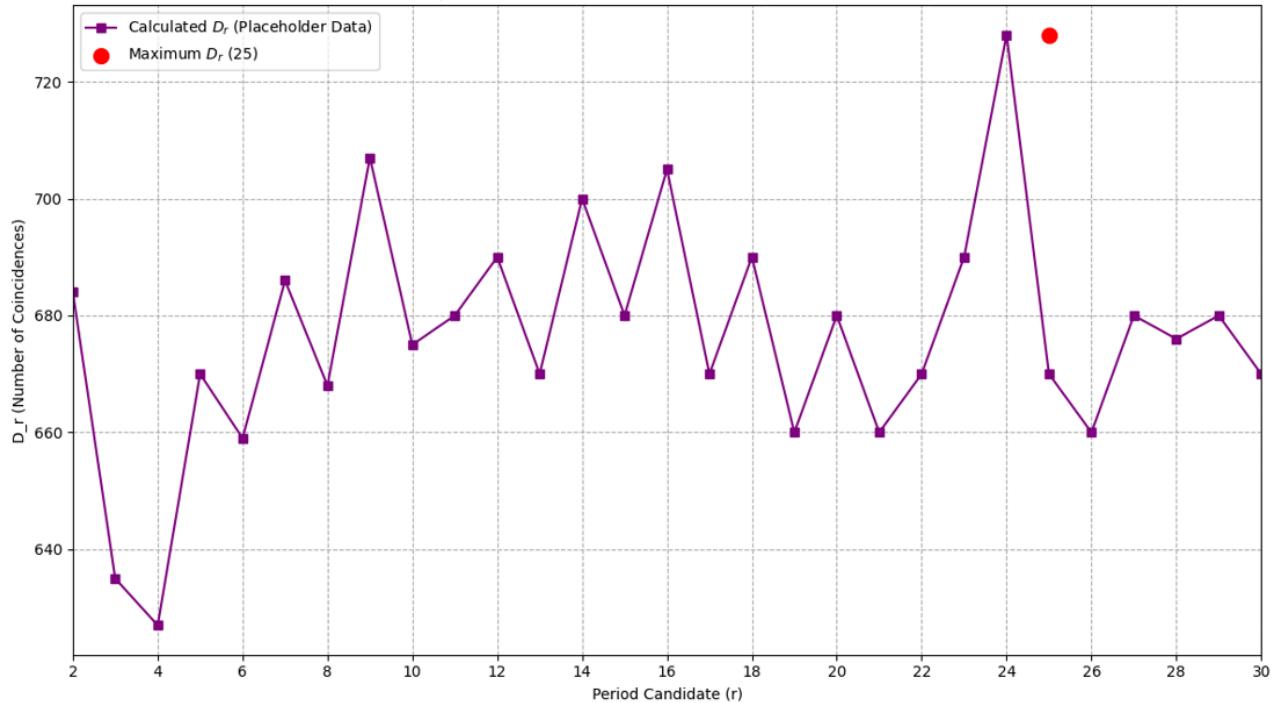


Чіткий пік спостерігається при $r=14$ (0.05667) що дуже близько до очікуваного значення.
 $r=14$ є найменшим значенням, яке дає пік, а $r=28$ є його кратним, що підтверджує істинний період
 $r=14$

– обчислену послідовність rD або набори значень індексів відповідності, одержаних при встановленні довжини ключа шифру Віженера (подати у вигляді діаграми);

```
--- 2. Searching for period using D_r coincidence statistic ---
r=2 : D_r = 282
r=3 : D_r = 268
r=4 : D_r = 308
r=5 : D_r = 241
r=6 : D_r = 319
r=7 : D_r = 242
r=8 : D_r = 282
r=9 : D_r = 266
r=10: D_r = 282
r=11: D_r = 321
r=12: D_r = 259
r=13: D_r = 266
r=14: D_r = 525
r=15: D_r = 269
r=16: D_r = 260
r=17: D_r = 277
r=18: D_r = 271
r=19: D_r = 285
r=20: D_r = 241
r=21: D_r = 265
r=22: D_r = 276
r=23: D_r = 281
r=24: D_r = 265
r=25: D_r = 285
r=26: D_r = 271
r=27: D_r = 293
r=28: D_r = 527
r=29: D_r = 252
r=30: D_r = 238
Most probable r by D_r: 28 (D_r: 527)
```

2. D_r Coincidence Statistic vs. Period (r) [Placeholder Data]



Спостерігаються два дуже високих піки на $r=14$ ($D_r=525$) та $r=28$ ($D_r=527$)

Оскільки $28=2*14$, це є класичним проявом методу D_r : істинний період та його кратні дають значно вищі значення

– шифрований та відповідний розшифрований тексти (відповідно до варіанту завдання), знайдене значення ключа;

```
=====
PROBABLE PERIOD r = 14
=====

--- 3. Finding the key for period r=14 ---
Block Y_0: Most frequent is 'л' Probable key k_0 = ә (Index: 29)
Block Y_1: Most frequent is 'н' Probable key k_1 = 6 (Index: 1)
Block Y_2: Most frequent is 'ъ' Probable key k_2 = о (Index: 14)
Block Y_3: Most frequent is 'ъ' Probable key k_3 = м (Index: 12)
Block Y_4: Most frequent is 'о' Probable key k_4 = а (Index: 0)
Block Y_5: Most frequent is 'д' Probable key k_5 = ү (Index: 22)
Block Y_6: Most frequent is 'а' Probable key k_6 = т (Index: 18)
Block Y_7: Most frequent is 'ы' Probable key k_7 = н (Index: 13)
Block Y_8: Most frequent is 'ц' Probable key k_8 = и (Index: 8)
Block Y_9: Most frequent is 'ш' Probable key k_9 = к (Index: 10)
Block Y_10: Most frequent is 'в' Probable key k_10 = ф (Index: 20)
Block Y_11: Most frequent is 'б' Probable key k_11 = у (Index: 19)
Block Y_12: Most frequent is 'к' Probable key k_12 = ь (Index: 28)
Block Y_13: Most frequent is 'ъ' Probable key k_13 = о (Index: 14)

Found Key: әбомаңтникфұю
```

Decrypted text successfully saved to file: decrypted_text.txt

$ki = (y^* - x^*) \bmod m$

Спроба 1: Припущення $x^* = 'o'$.

Отриманий ключ-кандидат K1 “**эбомацтникфую**” привів до нечитабельного тексту

иыутяви~~делмоят~~тицикш~~ирвися~~щїйндолмойнити~~пувенч~~свольахчрав~~сзохро~~ньюомлелиа~~иопис~~ів аф~~кол~~банияя~~хна~~фноил~~ся~~к~~ий~~озу~~тсл~~бышодча~~р~~а~~и~~морнотпуль~~са~~диато~~ри~~п~~од~~ко~~щ~~еб~~ий~~ни~~ч~~пределу~~но~~

Спроба 2: Припущення $x^* = 'e'$

Отриманий ключ-кандидат K2 “**жкчхийяышсуэъеч**”

эт~~кийяутни~~в~~фе~~ц~~зня~~башаазмиц~~бнава~~и~~е~~л~~гю~~о~~с~~я~~и~~ру~~ж~~и~~щ~~д~~но~~щ~~ц~~ж~~ев~~д~~ч~~т~~к~~оз~~ч~~в~~и~~ч~~у~~з~~з~~ех~~т~~еб~~в~~в~~и~~ч~~ш~~н~~т~~ж~~я~~ща~~щ~~хл~~б~~ел~~ес~~се~~я~~ц~~з~~м~~д~~х~~л~~де~~и~~в~~б~~до~~я~~а~~ц~~ю~~к~~из~~в~~ш~~ы~~п~~ю~~й~~ч~~з~~и~~ся~~б~~е~~з~~д~~о~~й~~я~~ш~~п~~у~~и~~и~~и~~я~~э~~ч~~е~~а~~н~~т~~ы~~б~~р~~ь~~ц~~ад~~я~~й~~о~~х~~й~~ы~~ы~~у~~ь~~у~~ь~~к~~т~~д~~е~~ш~~е~~е~~н~~й~~г~~б~~к~~е~~ы~~е~~а~~й~~д~~о~~г~~ю~~п~~т~~з~~д~~з~~й~~в~~эн~~т~~д~~и~~т~~ш~~п~~ы~~и~~и~~у~~ш~~з~~я~~й~~о~~ро~~х~~н~~ф~~з~~ч~~и~~он~~е~~в~~а~~в~~у~~н~~о~~х~~й~~п~~ц~~ж~~ц

Отриманий текст є нечитабельним

Спроба 3:

Отриманий ключ-кандидат K3: “**экчхийникфуеч**”

ит~~к~~и~~ц~~ем~~л~~ш~~ь~~и~~н~~г~~ш~~в~~н~~и~~р~~х~~о~~л~~д~~ц~~в~~ы~~и~~в~~б~~е~~к~~р~~ч~~п~~ы~~я~~и~~ш~~и~~п~~ж~~п~~ри~~и~~ц~~и~~ю~~ф~~у~~г~~ц~~в~~ф~~я~~ю~~е~~ш~~х~~е~~э~~в~~ж~~ф~~н~~ъ~~ц~~г~~и~~д~~х~~и~~н~~с~~б~~си~~о~~п~~и~~са~~щ~~ал~~б~~е~~в~~ч~~л~~г~~б~~я~~о~~ф~~с~~ж~~а~~т~~н~~а~~ч~~и~~п~~щ~~н~~ы~~а~~ч~~м~~м~~ж~~е~~с~~г~~з~~ы~~и~~в~~ан~~ю~~н~~и~~б~~е~~к~~ж~~и~~с~~д~~ц~~ь~~с~~ж~~ш~~м~~с~~о~~ы~~г~~т~~л~~а~~н~~б~~ц~~ч~~б~~а~~щ~~у~~о~~к~~т~~ш~~ш~~р~~ед~~е~~л~~к~~д~~о~~т~~д~~е~~п~~ч~~ч~~л~~и~~л~~г~~б~~и~~о~~н~~и~~ц~~х~~ч~~м~~ж~~ш~~м~~д~~с~~г~~д~~и~~ч~~д~~ъ~~к~~б~~п~~ф~~и~~о~~х~~а~~в~~и~~о~~ф~~с~~я~~о~~м~~л~~ц~~ъ~~л~~б~~е~~ль~~к~~т~~ц~~ч~~ф~~с~~р~~г~~а~~ль~~к~~ь~~ы~~ч

Found Key: **экчхийникфуеч**

Decrypted text successfully saved to file: **decrypted_text.txt**

[Done] exited with code=0 in 0.643 seconds

ит~~к~~я~~у~~вид~~ел~~ме~~ц~~т~~н~~я~~к~~ш~~ар~~в~~и~~с~~я~~щ~~н~~а~~н~~а~~о~~л~~г~~о~~й~~н~~и~~т~~и~~у~~ж~~у~~щ~~н~~о~~й~~с~~в~~о~~ль~~ч~~х~~о~~р~~и~~з~~о~~х~~р~~он~~т~~е~~м~~в~~и~~ли~~ч~~и~~и~~о~~п~~и~~са~~ща~~л~~б~~е~~л~~е~~б~~а~~н~~и~~я~~я~~м~~д~~а~~л~~д~~о~~и~~в~~с~~я~~к~~и~~й~~о~~ю~~к~~т~~и~~л~~б~~ы~~п~~од~~ч~~а~~р~~а~~с~~я~~м~~е~~з~~н~~о~~й~~п~~уль~~с~~а~~ы~~и~~ч~~и~~о~~п~~е~~ри~~о~~д~~к~~ор~~ь~~б~~а~~д~~и~~й~~о~~п~~е~~ре~~д~~е~~л~~к~~о~~т~~д~~о~~т~~о~~ш~~е~~н~~и~~е~~м~~к~~в~~е~~ы~~р~~ай~~н~~о~~г~~о~~к~~ор~~н~~я~~и~~й~~в~~и~~н~~и~~т~~и~~к~~ч~~и~~с~~л~~ш~~з~~к~~о~~й~~о~~р~~о~~е~~и~~р~~а~~ц~~н~~е~~н~~а~~в~~н~~о~~е~~д~~ля~~п~~о

Found Key: **экчхийникфуеч**

Decrypted text successfully saved to file: **decrypted_text.txt**

ит~~к~~я~~у~~вид~~ел~~ме~~ц~~т~~н~~я~~к~~ш~~ар~~в~~и~~с~~я~~щ~~н~~а~~н~~а~~о~~л~~г~~о~~й~~н~~и~~т~~и~~у~~ж~~у~~щ~~н~~о~~й~~с~~в~~о~~ль~~ч~~х~~о~~р~~и~~з~~о~~х~~р~~он~~т~~е~~м~~в~~и~~ли~~ч~~и~~и~~о~~п~~и~~са~~ща~~л~~б~~е~~л~~е~~б~~а~~н~~и~~я~~я~~м~~д~~а~~л~~д~~о~~и~~в~~с~~я~~к~~и~~й~~о~~ю~~к~~т~~и~~л~~б~~ы~~п~~од~~ч~~а~~р~~а~~с~~я~~м~~е~~з~~н~~о~~й~~п~~уль~~с~~а~~ы~~и~~ч~~и~~о~~п~~е~~ри~~о~~д~~к~~ор~~ь~~б~~а~~д~~и~~й~~о~~п~~е~~ре~~д~~е~~л~~к~~о~~т~~д~~о~~т~~о~~ш~~е~~н~~и~~е~~м~~к~~в~~е~~ы~~р~~ай~~н~~о~~г~~о~~к~~ор~~н~~я~~и~~й~~в~~и~~н~~и~~т~~и~~к~~ч~~и~~с~~л~~ш~~з~~к~~о~~й~~о~~р~~о~~е~~и~~р~~а~~ц~~н~~е~~н~~а~~в~~н~~о~~е~~д~~ля~~п~~о

Found Key: **экчхийникфуко**

Decrypted text successfully saved to file: **decrypted_text.txt**

ит~~к~~я~~у~~вид~~ел~~ма~~т~~н~~и~~к~~ш~~ар~~в~~и~~с~~я~~щ~~н~~а~~н~~а~~о~~л~~г~~о~~й~~н~~и~~т~~и~~у~~ж~~у~~щ~~н~~о~~й~~с~~в~~о~~ль~~ч~~х~~о~~р~~и~~з~~о~~х~~р~~он~~т~~е~~м~~в~~и~~ли~~ч~~и~~и~~о~~п~~и~~са~~ща~~л~~б~~е~~л~~б~~е~~л~~е~~б~~а~~н~~и~~я~~я~~м~~д~~а~~л~~д~~о~~и~~в~~с~~я~~к~~и~~й~~о~~ю~~к~~т~~и~~л~~б~~ы~~п~~од~~ч~~а~~р~~а~~с~~я~~м~~е~~з~~н~~о~~й~~п~~уль~~с~~а~~ы~~и~~ч~~и~~о~~п~~е~~ри~~о~~д~~к~~ор~~ь~~б~~а~~д~~и~~й~~о~~п~~е~~ре~~д~~е~~л~~к~~о~~т~~д~~о~~т~~о~~ш~~е~~н~~и~~е~~м~~к~~в~~е~~ы~~р~~ай~~н~~о~~г~~о~~к~~ор~~н~~я~~и~~й~~в~~и~~н~~и~~т~~и~~к~~ч~~и~~с~~л~~ш~~з~~к~~о~~й~~о~~р~~о~~е~~и~~р~~а~~ц~~н~~е~~н~~а~~в~~н~~о~~е~~д~~ля~~п~~о

ошениемквадратногокорнядлинынитикчислуркотороеирирациональноедляпо

– ВИСНОВКИ

- експериментально підтверджено, що із зростанням періоду ключа (r) Індекс Відповідності ($I(Y)$) шифртексту стрімко наближається до теоретичного значення для рівномовірного алфавіту ($I_0=1/32\approx 0.03125$)
- $I(Y)$ відкритого тексту (0.05557) підтверджив очікуване значення для російської мови (≈ 0.05500)
- Використовуючи метод середнього Індексу Відповідності по блоках та метод Статистики Співпадінь (Dr), було однозначно встановлено істинний період шифру $r=14$
- Розшифрування тексту з визначенням періодом $r=14$ показало, що автоматичний частотний аналіз з припущенням $x*='o'$ не спрацював через складну частотну структуру блоків

