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

Фізико-технічний інститут

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
ФБ-21 Захожий М.
ФБ-21 Хав’юк А.

Київ 2024

Мета роботи:

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

Хід роботи:

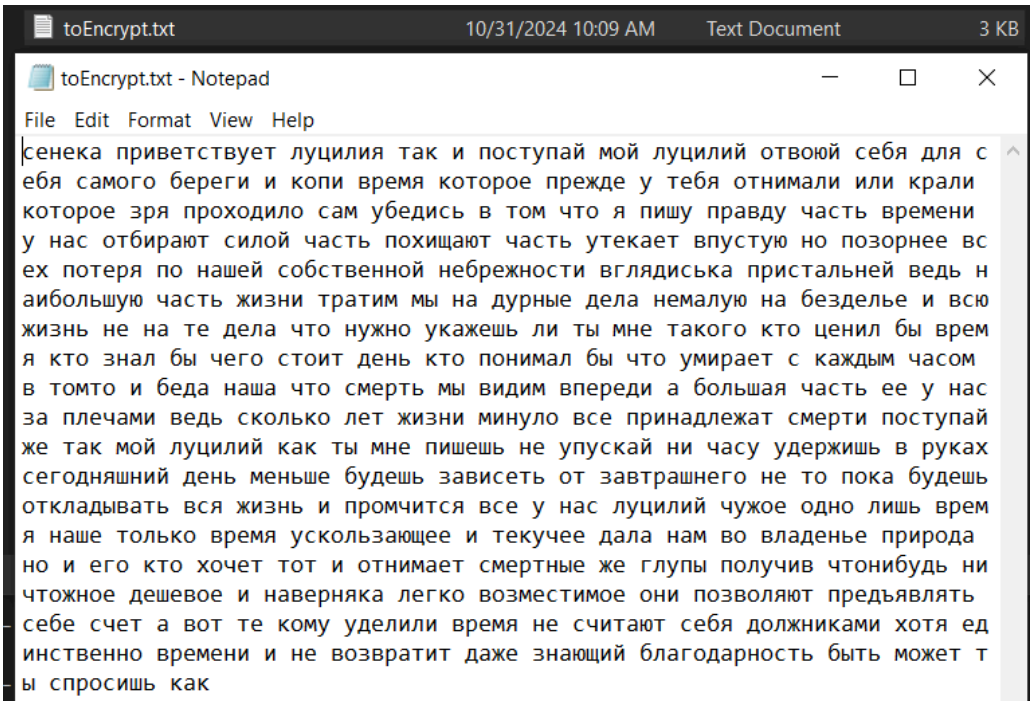
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

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

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

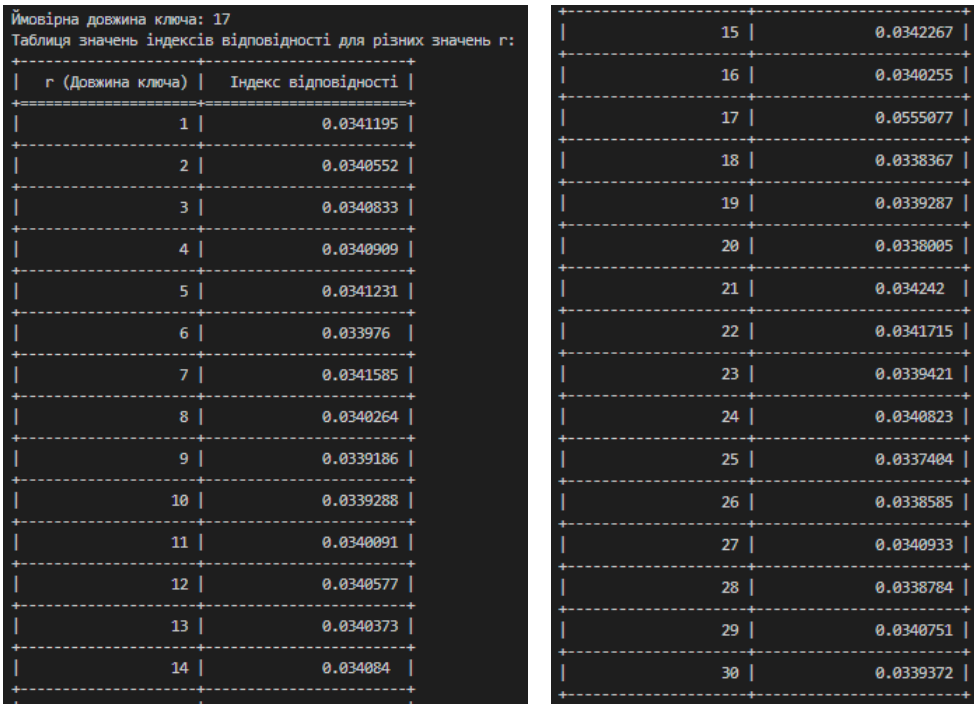
Київ 2024

1.




```
Індекси відповідності для текстів:
Відкритий текст: 0.05302600930044821

Ключ: ты | Індекс відповідності: 0.042642470925588004
Зашифрований текст (перші 200 символів): гаяаьыблъэчнгнфочнэоигэгснтеъкамдобыызадэоигэгыйдэащымчьсяэъгауъгыюйхйуавахгъеа
къэваюъьйдйвйчквашячодауъанягюыэгъжъевыэгьйдйвйчввъблараяъжамтзеьчяъмоэдйютдйскъуеквыфяеттмдчфлчзчиъоыгйдьъЛтщдмъжадйыг
н

Ключ: кот | Індекс відповідності: 0.03951092760618572
Зашифрований текст (перші 200 символів): ыуяпштщюъмудыафэудхбитщъйатфцбшядээтуъаущеацэтчаьраичгппсощсыууйятцьхшпчъухтцьш
эъмючцньшааъьчщючртчэачлнаьыъцоэтцэтшвкщъфьдшюапхвйэвшгаоцэшятцбуптъыкфьыюбаайэъвббъофобйкяджрвпъччцечогшаутютиагтщауеты
а

Ключ: зима | Індекс відповідності: 0.035933702772477538
Зашифрований текст (перші 200 символів): шнщесиырпкстшъоумъчуэрчижъмкпчъсщыыарфъйтывитрхощкъюрщсбжмчяшнняшишокцнечнпиптъ
ппкьеузцощцьомчьенмсущнняхъщиуичипуфкчичисцюочцсзчзырхэъдпуъсзфябммфсгкюоуяюожчфшъчьаймячзщюьйшсммхфуфиэощйфрзжюспуъйюиэ
т

Ключ: весна | Індекс відповідності: 0.033722113371286344
Зашифрований текст (перші 200 символів): укютквфбхвзчвявхкгшушньхяфеыхпрцгапвоэыйншзхлкоявргъюегдхшяуктмсвсярогкбтгкныы
пкзбтмбпяяотуцьрзлхтуфктмофтщщаннщшимхсшимугырркшэясхявожныысвсдоежнвйвфуэдтрдахшхфбнвжшинсфбуэеокюхупевытгнбнюфцщшольсю
т

Ключ: киноактриса | Індекс відповідності: 0.033937385951782306
Зашифрований текст (перші 200 символів): ынъуккбаруеьщярупдыызихрмаафъяцвтэчнчмшыыызихрцьтмаосвелзсщяычсзваццрьбпвхлщифц
ьцвъчьзыоьцэъещвхохеэътпяшдэрэахрхщифвручкшъыюопщазаршэытихабиэулнсцсжфвцэчьцмэивеяшсвоыдосьотшцмпхбнкгюътиъиластэюсиаы
ъ

Ключ: абстрагирование | Індекс відповідності: 0.033712022469075594
Зашифрований текст (перші 200 символів): сжючъатшшрзтюъзужгэгцлушнфачрфотгеяамфючнугррикядтобсбугясудсжтсбапцуьгеэниийыа
яиешхъбкыъурпцбаеймхбфеозутощюрллрыцмрнункпгааоипансрыэудйьабапысужиюдзтпэйвовчшжхпэиздфитбтякауоеършнбвавблшрмфсхууйшсг
в
```

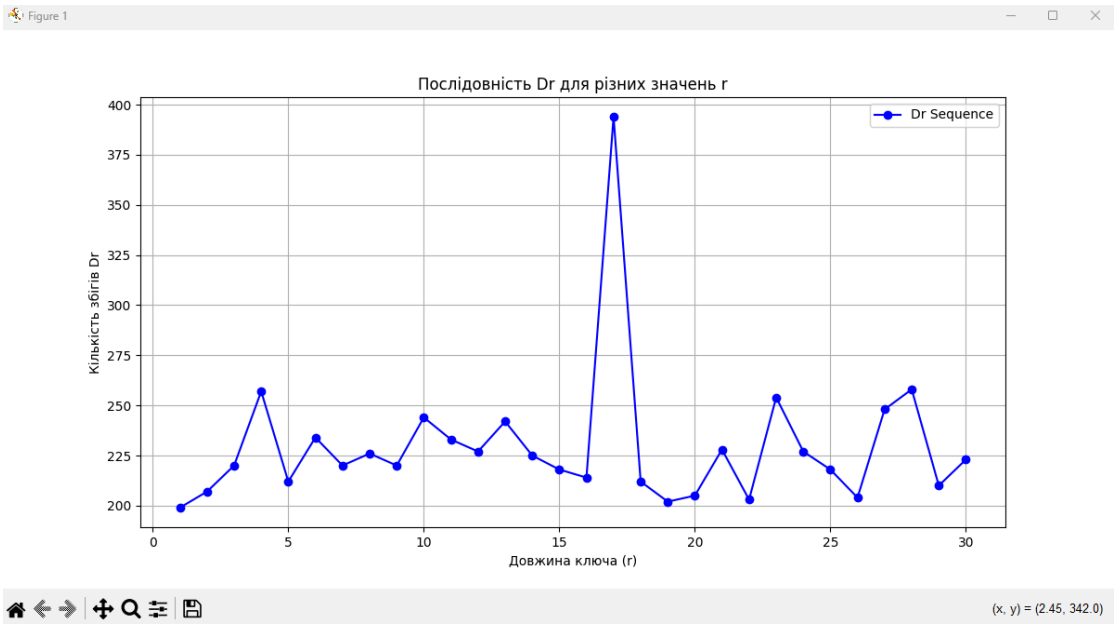
2.

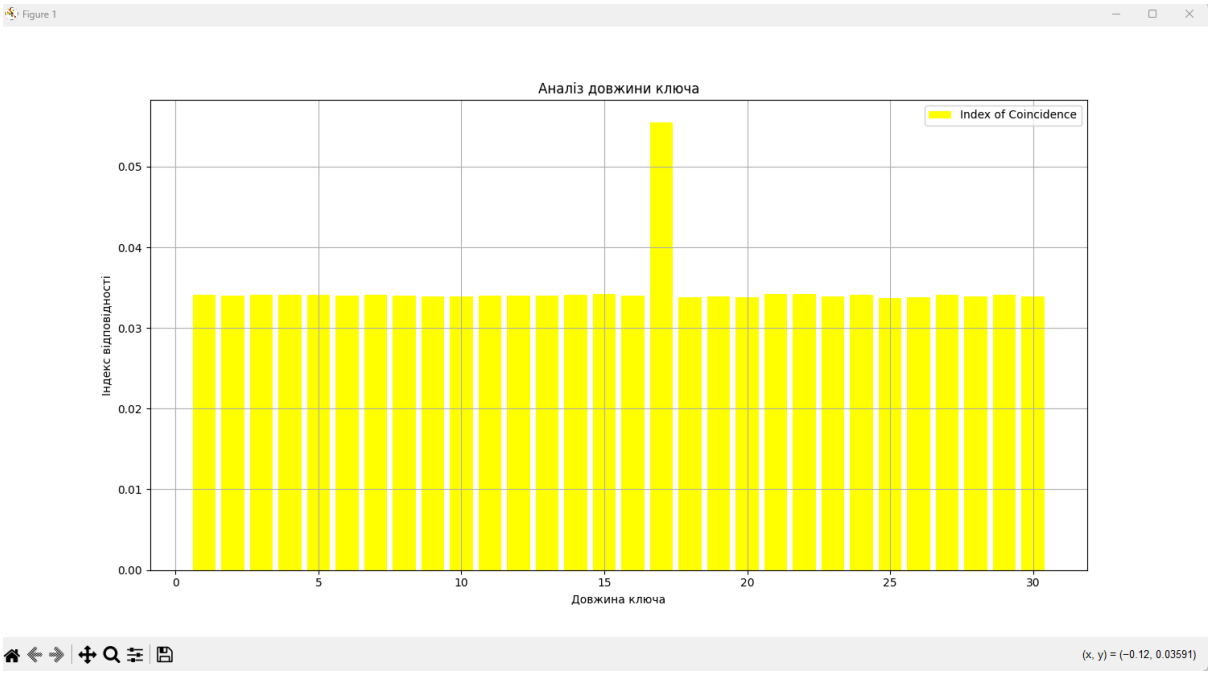


Ймовірна довжина ключа: 17
Таблиця значень індексів відповідності для різних значень r:

r (Довжина ключа)	Індекс відповідності
1	0.0341195
2	0.0340552
3	0.0340833
4	0.0340909
5	0.0341231
6	0.033976
7	0.0341585
8	0.0340264
9	0.0339186
10	0.0339288
11	0.0340091
12	0.0340577
13	0.0340373
14	0.034084
15	0.0342267
16	0.0340255
17	0.0555077
18	0.0338367
19	0.0339287
20	0.0338005
21	0.034242
22	0.0341715
23	0.0339421
24	0.0340823
25	0.0337404
26	0.0338585
27	0.0340933
28	0.0338784
29	0.0340751
30	0.0339372

3.





Повнцстю відновлений ключ - возвращениеджинна

```
Відновлений потенційно правильний ключ: возвращениеджлнда

Майже розшифрований текст: дорофейльвовифпсворыкобылынирэзьвжизнинепокидаизомлихотяпрожилугеколышестидесяпифетработа
лпрорюохстроительнойкойпйниидомостройвхэрековестолицевкрэицылюбилпорыбачипьъдрузьяминаозерэхщоганьскогокрая...
--------------------------------------------------------------------------------------------

Повністю розшифрований текст: дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяпрожилужебольшестидесятилетраб
оталпрорабомстроительнойкомпаниидомостройвхарьковестолицевкраиныюбилпорыбачитьсдрузьяминаозерахроганьскогокрая...
```

Київ 2024

Висновок

У ході роботи було освоєно основи частотного криптоаналізу та методи його застосування до поліалфавітних шифрів. Зокрема, було розглянуто шифр Віженера як приклад потокового шифру з додатковим зміщенням. Також вдалося набути практичні навички роботи з техніками визначення довжини ключа та частотного аналізу для розшифрування зашифрованого тексту. Ця робота допомогла краще зрозуміти, як працюють шифрувальні алгоритми і які є способи їх розкриття за допомогою криптоаналітичних методів.

Київ 2024