

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 Ємець Валерія

Тютюннікова Віолета

Київ 2024

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

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.

У якості тексту нами було підібрано уривок казки «Їжачок у тумані»:

Тридцать комариков выбежали на поляну и заиграли на своих писклявых скрипках. Из-за туч вышла луна и, улыбаясь, попыла по небу.

«Мм-й!..» – вздохнула корова за рекой. Залаяла собака, и сорок лунных зайцев побежали по дорожке. Над рекой поднялся туман, и грустная белая лошадь утонула в нем по грудь, и теперь казалось – белая белая утка плывет в тумане и, **отфыркивая**, опускает в него голову.

Ежик сидел на горке под сосной и смотрел на освещенную лунным светом долину, затопленную туманом. Красиво было так, что он время от времени вздрагивал: не снится ли ему все это?

А комарики не устали играть на своих **скрипочках**, лунные зайцы плясали, а собака выла.

«Расскажи – не поверят!» – подумал Ежик, и стал смотреть еще внимательнее, чтобы запомнить до последней травинки всю красоту.

«Вот и звезда упала, – заметил он, – и трава наклонилась влево, и от елки осталась одна вершина, и теперь она плывет рядом с лошадью... А интересно, – думал Ежик, – если лошадь ляжет спать, она захлебнется в тумане?»

И он стал медленно спускаться с горы, чтобы тоже попасть в туман и посмотреть, как там внутри.

– Вот, – сказал Ежик. – Ничего не видно. И даже лапы не видно. Лошадь!

– позвал он. Но лошадь ничего не сказала.

«Где же лошадь?» – подумал Ежик. И пополз прямо. Вокруг было глухо, темно и мокро, лишь высоко сверху сумрак слабо светился.

Полз он долго-долго и вдруг почувствовал, что земли под ним нет, и он куда-то летит. **Бултых!..**

«Я в реке!» – сообразил Ежик, похолодев от страха. И стал бить лапами во все стороны.

Когда он вынырнула, было по-прежнему темно, и Ежик даже не знал, где берег.

Пугающий река сама несет меня!» – решил он.

Как мого, глубоко вздохнул, и его погнуло вниз по течению.

Река шурила камышами, бурила на перекатах, и Ежик чувствовал, что совсем промок и скоро утонет. Вдруг кто-то дотронулся до его задней лапы.

– Извините, – беззвучно сказал кто-то, кто вы и как сюда попали?

– Я – Ежик, – тоже беззвучно ответил Ежик. – Я упал в реку.

– Тогда садитесь ко мне на спину, – беззвучно проговорил кто-то. – Я отвезу вас на берег.

Ежик сел на чью-то узкую скользкую спину и через минуту оказался на берегу.

– Спасибо! – вслух сказал он.

– Не за что! – беззвучно выговорил кто-то, кого Ежик даже не видел, и пропал в волнах.

«Вот так история... – размышлял Ежик, отряхиваясь. – Разве кто поверит?!»

У коді передбачається, що текст буде приведено до нижнього регістру, видалено пробіли, прибрано знаки пунктуації та замінено літеру «ё» на «е».

Створено функцію, яка генерує ключі різної довжини з рандомних літер, окрім «ё». Також реалізовано саму функцію шифрування з використанням цих ключів, логіка функції шифрування базується на формулі, яка описує шифрування методом Віженера:

$$y_i = (x_i + k_{i \bmod r}) \bmod m, i = \overline{0, n}.$$

Після цього всі тексти, зашифровані різними ключами зберігаються у окремий файл «encrypted.txt», також зазначається ключ, яким цей текст було зашифровано:

[illegible]

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

У програмі, передбачена функція, яка розраховує індекси відповідності для оригінального тексту, а також для кожного з шифротекстів. Функція реалізована, спираючись на формулу:

$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y)-1),$$

Результати обрахунків виводяться на екран та зберігаються у окремий файл «indexes.xlsx»:

```
violetta@MacBook-Pro-Violetta 2лаба % /opt/anaconda3/bin/python "/Users/violetta/Desktop/лабы/2лаба/lab2.py"
Довжина ключа: 2 | Індекс: 0.03963 | Різниця: 0.01586
Довжина ключа: 3 | Індекс: 0.03828 | Різниця: 0.01721
Довжина ключа: 4 | Індекс: 0.03808 | Різниця: 0.01742
Довжина ключа: 5 | Індекс: 0.03598 | Різниця: 0.01951
Довжина ключа: 10 | Індекс: 0.03718 | Різниця: 0.01831
Довжина ключа: 11 | Індекс: 0.03438 | Різниця: 0.02112
Довжина ключа: 12 | Індекс: 0.03364 | Різниця: 0.02185
Довжина ключа: 13 | Індекс: 0.03520 | Різниця: 0.02029
Довжина ключа: 14 | Індекс: 0.03458 | Різниця: 0.02091
Довжина ключа: 15 | Індекс: 0.03569 | Різниця: 0.01980
Довжина ключа: 16 | Індекс: 0.03334 | Різниця: 0.02216
Довжина ключа: 17 | Індекс: 0.03371 | Різниця: 0.02179
Довжина ключа: 18 | Індекс: 0.03319 | Різниця: 0.02230
Довжина ключа: 19 | Індекс: 0.03421 | Різниця: 0.02128
Довжина ключа: 20 | Індекс: 0.03352 | Різниця: 0.02197
Індекс початкового тексту: 0.05549
```

Ключ	Довжина	Індекс	Різниця з оригіналом
мы	2	0,039634	0,015858089
дом	3	0,038283	0,017208289
лего	4	0,038075	0,017416642
зверь	5	0,035977	0,019514645
пенекветка	10	0,037179	0,018312369
вдохновение	11	0,034376	0,021115373
авиарработник	12	0,033637	0,021854363
контрразведка	13	0,035205	0,020286998
активизировать	14	0,034585	0,02090702
оппозиционность	15	0,03569	0,019801681
специализируемый	16	0,033336	0,022155247
легкомысленничать	17	0,033705	0,021786381
экспериментировать	18	0,033194	0,022298136
неудовлетворительно	19	0,034215	0,021277145
гипертрофированность	20	0,033521	0,021970814

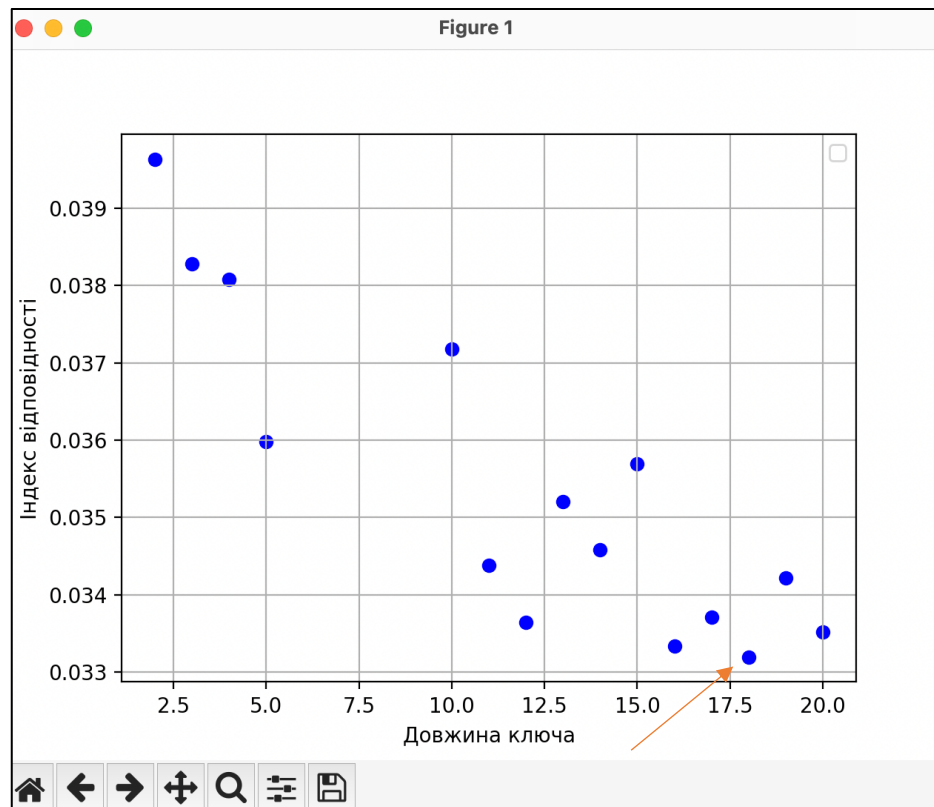
Високий індекс відповідності оригінального (0,05549) є очікуваним, оскільки природні тексти мають характерні частотні закономірності, що відображають структуру мови.

Можемо побачити, що при короткій довжині ключа індекс відповідності (0,035977 – 0,039634) вищий, що вказує на те, що частина закономірностей оригінального тексту зберігається.

При довжині ключа 11 та більше індекс відповідності стабілізується в районі 0,033-0,035. Це свідчить про те, що частотні характеристики початкового тексту менш помітні.

Мінімальне значення індексу відповідності (0,033194) спостерігається при довжині ключа 18, що є найкращим результатом. Це показує, що за такої довжини ключа шифр максимально приховує структуру тексту.

Для наочності перешлянемо результати на графіку, де бачимо найнижчий показник у точці 18:



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

(Варіант №5)

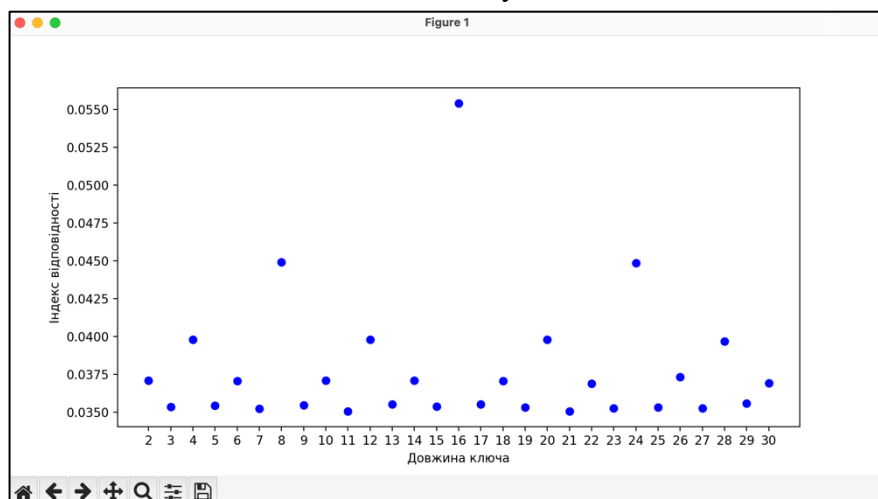
За варіантом маємо наступний текст:

уушнэхяеуеуььарецшыбшивцмкэфдкфтзршлхцрпаычеблтхпбьроафтиорашбцтиыбььюбяцбаьшпрсеццинууусьпоузабй
ьрьомцпьяюьгоафтзцыныбмквбвъуцбьюрохугяхсаацспнрцроцщйьэьгимхдрзяэксыжяфуэнрчхбвуццуулббрндгдрйлфр
кюбуухыятфчцхрпшгэуаюасаяухсуоьвршжыэйчунфеттрущийняоэнчдкыучццокцгтгчшдзццэцддыгышгьгъгьниикэнчв
ьвуэыаскыгсзуатггообуэмкышшэбшгауььбшыждыгтлнцноьтамщрсцуддыщюошажьгэадцсскцтшущьбьяючьдыхчнцрфю
ооуюпммцягьяьющгьсоецьюкцмняэшцебувастюоскчоццьеушщшаяущясььхищнающьебкчйпотхсуушршщфщмьуыл
фголцэугаефгншаршарщяюьгьдчзрлршщцййатудымфгжунгвъуфбзнопнхцашщшхсшчгьпкасафэщрвшгтьляэнлслгхрфю
ькэшатлосннъаухюьжбшешоьцжущоцъгьгьюеунырзыжнтуитэйяппшдгхьузуушыюэвтжджерашивайшрмлндцдйшщчр
япъуаяоавунмсжуоигцоогшгънютчкпжящяухъвыщытхшрьщяуьпачшбцткуптщйбьеууэйтчйлуазнвапщмугякьцзрышщцт
мнсьэйэссцэрлцбтфябшъвфчийлышгжеуьуючвеьднэкаыгбойэогтросамйцруьтыоряьслдхноиэцйыхраоаасучэщхщьбы
шщпямтццънишятарюьжчтлелкйудьымтцтосуфырцбтфябшачьпбэбгысяляучпчркоьтхсежыщыьччфуряэцькзуфо
фъуыкццоццвкпплеияслйзыьньмецяйяначлпйрквнльщшешбчхжыркцтбмйццэнычечьнуьирлжчтдщмлпщяятбвядп
ноуупщухюькрябхчйстцяэртюпарюдюдриькнльонофшоттожтульгщэыноьсьекппоэньмшуьфгтпънуьорэжюбаятс
цдфлцзюцьеуыйпфщйпыоьхмчшуышпатхшгьтыцкжъеончхтлрашиаюьхюфьхсхшэакццзуэзьашфуухшнвайпаоя
уохрщрщрьцйгьбаэпйцбньншщятгьбэдхтзтучупэпаяуйтичхфшщшсюьеьбатябслхюшлктпююсацхйхэуажсашбаюшгач

[illegible]

Який помістимо у файл «task3.txt»

Тепер реалізуємо програму, яка розбиває текст на блоки довжиною відповідною до ключа (ключи приймають значення від 2 до 30). Далі розраховуємо індекс відповідності для кожної довжини ключа та шукаємо найвище значення:



```
violetta@MacBook-Pro-Violetta 2лаба % /opt/anaconda3/bin/python "
Довжина ключа: 2, Індекс відповідності: 0.037097
Довжина ключа: 3, Індекс відповідності: 0.035352
Довжина ключа: 4, Індекс відповідності: 0.039794
Довжина ключа: 5, Індекс відповідності: 0.035435
Довжина ключа: 6, Індекс відповідності: 0.037052
Довжина ключа: 7, Індекс відповідності: 0.035224
Довжина ключа: 8, Індекс відповідності: 0.044912
Довжина ключа: 9, Індекс відповідності: 0.035450
Довжина ключа: 10, Індекс відповідності: 0.037098
Довжина ключа: 11, Індекс відповідності: 0.035062
Довжина ключа: 12, Індекс відповідності: 0.039789
Довжина ключа: 13, Індекс відповідності: 0.035509
Довжина ключа: 14, Індекс відповідності: 0.037094
Довжина ключа: 15, Індекс відповідності: 0.035384
Довжина ключа: 16, Індекс відповідності: 0.055398
Довжина ключа: 17, Індекс відповідності: 0.035524
Довжина ключа: 18, Індекс відповідності: 0.037051
Довжина ключа: 19, Індекс відповідності: 0.035316
Довжина ключа: 20, Індекс відповідності: 0.039798
Довжина ключа: 21, Індекс відповідності: 0.035057
Довжина ключа: 22, Індекс відповідності: 0.036881
Довжина ключа: 23, Індекс відповідності: 0.035267
Довжина ключа: 24, Індекс відповідності: 0.044863
Довжина ключа: 25, Індекс відповідності: 0.035317
Довжина ключа: 26, Індекс відповідності: 0.037311
Довжина ключа: 27, Індекс відповідності: 0.035248
Довжина ключа: 28, Індекс відповідності: 0.039691
Довжина ключа: 29, Індекс відповідності: 0.035585
Довжина ключа: 30, Індекс відповідності: 0.036928
Довжина ключа з максимальним індексом відповідності: 16
Ймовірні значення ключа по блокам: ['д', 'е', 'к', 'е', 'л', 'и', 'с', 'о', 'б', 'о', 'р', 'о', 'й', 'д', 'е', 'й']
```

З виводу програми та графіку бачимо, що найбільший індекс відповідності відповідає ключу довжиною 16. Також у виводі програми бачимо ймовірне значення ключа:

```
Ймовірні значення ключа: ['д', 'е', 'к', 'е', 'л', 'и', 'с', 'о', 'б', 'о', 'р', 'о', 'й', 'д', 'е', 'й']
```

Отже, за припущенням маємо ключ «декелисоборойдей», проте це не зовсім схоже на щось змістоване, єдине, що можна побачити це «собор».

При отриманні цього ключа вважали найчастішою літеру «о», переглянемо який вигляд має спроба розшифрувати текст з цим ключем:

```
violetta@MacBook-Pro-Violetta 2лаба % /opt/anaconda3/bin/python "/Users/violetta/Desktop/УНИК/3 курс/1 сем/крипта/лабы/2лаба/task
Розшифрований текст: поoitноеделоультусьнасиьнолаеловжуаневоткнобьвореьсиэтудовчфьногсьстнуюистсцу
знамснавeрноефьчше
цостьрщедевсегчьсилижсежионоьдзмалэьтванесдефилосьшоловекусвданыьдбевнутренцопотржньмоттогчьомнодччисленнышодраинелениялафй
ютсучльковнимийциядеуимособеннчнетямухотконасефитхууьныпотомупчбычнбиленостьлэнскаятфужитемупчатинепнолимпрошятстгсемнанеобгитн
```

Розглянемо перший рядок в якому можна помітити певні слова:

Поoitноеделоультусьнасиьнолаеловжуаневоткнобьвореьсиэтудовчфьногсьстнуюистсцу
знамснавeрноефьчше

Поділимо тепер цей рядок на блоки довжиною 16 (відповідно до ключа):

Поoitноеделоуль|тусьнасиьнолаел|овжуаневоткнобь|
ореьсиэтудовчфьн|огсьстнуюистсцуз|намснавeрноефьчше|

У першому блоці (Поoitноеделоуль) – бачимо змістоване слово на 3 позиції 9-12.

Тусьнасиьнолаел – у цьому фрагменті на позиціях 5-12.

Ореьсиэтудовчфьн – у цьому фрагменті на позиціях 7-9

Намснавeрноефьчше – у цьому фрагменті на позиціях 5-12.

Тобто робимо висновок, що у ключі вірні положення це 5-12, тобто «декелисоборойдей».

Також у першому фрагменті можемо побачити, що «Поoitноедело» дуже схоже на вислів «Понятноедело», тобто можемо розрахувати 3 та 4 позиції у ключі.

Для цього використаємо формулу:

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

Рахуємо за модулем 32 (оскільки виключаємо літеру ё). Та для зручності випешемо літери та їх індекси:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Переглянемо перші 4 літери шифротексту:



Тобто з літери «ш» було отримано літеру «н», а з літери «н» літеру «я»
⇒ $(24-13) \bmod 32 = 11$, що відповідає літері «л» (позиція 3)
⇒ $(13-31) \bmod 32 = (-18) \bmod 32 = 14$, що відповідає літері «о».

На цьому етапі ключ має вигляд: «*делолисобор*йдей». З таким ключе текст приймає наступний вигляд:

```
violett@MacBook-Pro-Violetta 2лаба % /opt/anaconda3/bin/python "/Users/violetta/Desktop/УНИК/3 курс/1 сем/крипта/лабы/2лаба/task_decrypt.py"
Розшифрований текст: понятноеделокультурунасиленнолаеловеканевоткнешьвордусиэтудовольногрустнуюистинузналинаврноелучшеемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелионосизмалъстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттогоомногочисленнешодразделенияпалатыцеремонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутуныпотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятств
```

Переглянемо рядок та знов поділимо на блоки, виділивши блакитним гарантовано правильні частини (відповідають 1-12 позиціям ключа):

понятноеделоуль|турунасиленнолаел|овеканевоткнешь|ордусиэтудовчфьн|

Можемо пропустити, що після слова «насиленно» йде прийменник «в», переглянемо шифротекст:

ШТ: уушнэхяеуыьаре|цшыбшивцмкэьфдкф|т

Тобто з літери «ф» отримують літеру «в» => $k = (20-2) \bmod 32 = 18$ – літера «т».

Ключ набуває наступного вигляду: «*делолисоборот*ней», а текст:

```
violett@MacBook-Pro-Violetta 2лаба % /opt/anaconda3/bin/python "/Users/violetta/Desktop/УНИК/3 курс/1 сем/крипта/лабы/2лаба/task_decrypt.py"
Розшифрований текст: понятноеделокультурунасиленнолаеловеканевоткнешьвордусиэтудовольногрустнуюистинузналинаврноелучшеемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелионосизмалъстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттогоомногочисленнешодразделенияпалатыцеремонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутуныпотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятств
```

Понятноеделокультурунасиленнолаел|овеканевоткнешь| (Знов розбиваємо на блоки та виділяємо вже відоме)

Досить очевидно можна прослідкувати речення: Понятное дело культуру насильно в человека не воткнешь... З цього слідує, що нам залишилось обрахувати лише 14 позицію ключа. З другого фрагмента бачимо, що літеру «ч» з ВТ зашифрували як «д»

(ШТ: уушнэхяеуыьаре|цшыбшивцмкэьфдкф|) => $(4-32) \bmod 32 = -19 \bmod 32 = 13 \bmod 32$ – літера «н».

Отже, ключ має вигляд «делолисоборотней». Спробуємо розшифрувати текст:

Розшифрований текст:

понятноеделокультурунасиленнолаеловеканевоткнешьвордусиэтудовольногрустнуюистинузналинаврноелучшеемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелионосизмалъстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттогоомногочисленнешодразделенияпалатыцеремонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутуныпотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятств

и неманеобъятныхпросторахимпериивстречаетсяещенемалолюдейкоторымпокакимтолишь буддазнаеткакимпричинамтакинесталоинтереснымничтоглавноенисветозарныевысотыдух авеликихрелигийивечныйпоисксмыслажизниземнойпитающийистинноеискусствониголов окружительныебезднынакраюкоихвечнопребываетнастилаящаянаднимиобщепроходимые гатаунакихотябычистоепросторноесостоятельноеидобродетельноежитьестольестествен ноедлябольшинстваордусскихподданныхчтогрехатаитьхутунынаселеныбыливноснвомва рварамииневообычномпониманииэтогословаисстариобозначавшеголюдейинойнеордусской культурыаскореевтомегозначенииикотороестольжедавносделалосьобычнымвевропелюдипо чтичуждыевсякойкультурыневедающиеиритуаловивозвышенныхзабототсутствииподлинно йвоспитанностибросаетсяздесьвглаздаженевнимательномунаблюдателючеловексдорогим перстнемнапальцеодетыйвпрекрасныйшелковыйсузорочьемхалатможетнапримервприсутс твииженщиныпроизнестибранноесловоиливысморгатьсяприлюднопрямовамземлюпослечего спокойнодостатьизрукавадорогойрасшитыйплатокиутеретьносежеличеловекповзрослелиз аматерелвтакомсостояниидушиизменитьегокакправилоуженельзяразвечтумудроенебовраз умиттакиилииначесмотряповероисповеданиюземнымвластямвэтидуховныеобластипутьзака заннасилиеневоместноаувещеваниезапоздалокакимбыниуролилсяинисталчеловекнадодатье мупрожитьжизньтаккаконхочетконечноеслионпритомневредитокружающимпоэтомубагне оченьлюбилрайонхутуновикакправилооказывалсяздесьлишьпослужебнойнадобностиботка ксегоднянесмотрянапротивныйнавевающийхандруджидикбагбылисполненлегкогопьянщ егоазартавсегдасопутствовавшегооблизкомуиудачномузавершениюочередногоделакакконцуп одходилорасследованиеоцелойсетичетырехзаведенияединовременноподпольныххопиумокур иленвыявленныхвразудаломпоселкецифрыманилипрасадвернулсявалександриновдохнове нныйоткрывшимисяперспективамивразудаломпоселкеонужевладелнесколькимихарчевня миилавкамииесликприбылямотторговлиспиртныминапиткамиудастсядобавитьещедоход ыотопиумокурениятоможнобудетподуматьорасширениипредпринимательстваоприобре те нииновойнедвижимостиинишалабытьможетдажеобустановленииконтролянадвсемихарче внямиилавкамиаразудалогопоселкаатамоченьскоропринадлежащихлагашузаведенияхнемн огочисленныеневверныеегослужителиоборудовалиспециальныезакутыгдекуслугамжителей игостейхутуноввыстроилисьудобныележанкиикуриТЕЛЬНЫЕприборыпрасадпредлагалпосет ителямновоесредстворасслабительноеичиститьдушупослетрудовыхбуднейпосетителизаин тересовалисьпотомвошливовкуснопрасадбылжаденвмечтахужвозомнивсебякняземразудал огоонзахотелмногоисразунанявсебевпомощьнесколькодюжихмолодцовпрасадзабылоглавн омиустремилсякнизменномувзявшисьсилойвнедрятьопиумвхарчевниемунепринадлежавш иечембольшеохваченозаведенийтемвышеприбытоктаксправедливополагаллагашобращать сяквэйбинамдлярешениявозникающихразногласийбылоневхарактереобитателейхутуновин ечестныйпрасадбеззастенчивоэтимвоспользовалсяпопыткиздешнихжителейсовладатьслаг ашемсвоимисиламинеувенчалисьуспехомаспидзаранееподготовилсякстычкамиоттогооказ алсясильнееокончательнораспоясавшисьонснялостеныдвуствольноеоружьедедаиприлюдн опрямопосредипереулкакотпилилстволыпослечегосталходитьпохутунамсобрезомзапазухой идажепрозвищеполучилообрезагаместныежителирастерялисьопиумокурильнирасцвеливпос елкенесообразнопышнымцветомлагашподсчитывалбарышнивеликийучительвдвадцатьвт оройглавебеседисужденийнезрясказалнезнаюниодногоправлениякотороебылобыбесконе чнымисамовольноприсвоенныйпрасадомнебесныймандатместногозначенияужеуплылизег орухотялагашещеинеподозревалообэтомвскоренесколькочеловекпотерялитрудоспособнос тьинтерескжизниисамоездоровьеивследствиечрезмерногоупотребленияопиуманасонгрядущ ийавандевятыйпопалвбольницуулусноеведомствонародногоздоровьявсестороннеизучилоп ричинузаболеванияванаивскореобрезагасамтогоневедающаяпопалвполезренияуправлениявнеш нейохранызаседмицустараниямибагаивзятогоимвпомощьстаршеговэйбинаяковачжанабагс симпатиейнаблюдалкакэтотрозовощекийислегкаещеподетскиनावныймолодецпостепенно превращаетсяявведущегоипытливомастерасыскногоделарасположениевсехзаведенийгде курилиопиумбылоопределеноснаивозможнойточностьютакжебылисоставленыподробныес пискивсехподданныхимевшихотношениекраспространениюопасногодляздоровьяпорокауп

равлениевнешнейохранысословочевидцевсоставилочленосборныйпортретчеловекакоторы
йповсемвероятиямьявлялсястаршимзаправилойитакчеловеконарушительбылизобличендеся
тьсамыхспособныхвэйбиновпереодевшисьвгражданскоеплатьезатроесуткинепрестанногос
лужебногобденияустановилигдеобрезагабываетпосвоимпротивуправнымделаминичевече
ромпристеченииизначительныхсилуправленияодурманиваниеордусскихподданныхопиумо
мрешенобылопресечьпоусловленномусигналувэйбинынакрываютсенехорошиезаведения
абагсяковомчжаномзадерживаютзаправилауиегоближниковкаксталоизвестновечерниечасы
послеобходасвоихвладенийивзиманияежедневнойнеправеднойданилагашсвоимиближни
камикороталвнеобразномвеселиивхарчевнекунисыновьябагещеразвзглянулначасыиразд
авилокуроквбронзовойпепельницепораонлегкоподнялсясместаимашинальнопотянулсяпоп
равитьзапоясоммечномечанебылонапривычномместеродовойклинокбагаканулвнебытиера
створенныйядовитойслюнойзлоумногоподданногокозюльканаэтисобытияописанывделеоп
олкуигоревеановыймечпрославленныйханбалыкскиймастерганыцзянмошуобещалотковать
лишьчерезполторагодабагвздохнулнезаметнопроверилскрытыеплотнымхалатомбоевыено
жиподхватилзонтипошелквыходуиззалытудагдеседваслышнымшорохомсеялсясквозьгусте
ющиесумеркибесконечныйдождьпора

Отримали читабельний текст.

Висновок: під час виконання комп'ютерного практикуму набули навичок частотного аналізу шифру Віженера, ознайомилися з методами визначення довжини ключа та реалізували один з них. Практично підібрали сам ключ, враховуючи логіку самого методу шифрування та тексту.