КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

ФБ-23 Невмержицька Дар'я

Варіант 10

Мета роботи:

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

Порядок виконання роботи:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

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).

Хід роботи:

Для шифрування беру частину тексту з файлу для минулої роботи. Ключі генеруються випадковим чином з символів алфавіту (generate_random_key(length)). Зашифрування проходить так:

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

Де y(i) – літера шифртексту, x(i) – літера відкритого тексту, k(i mod(r)) – літера ключа, m – кількість літер у алфавіті, n – довжина відкритого тексту.

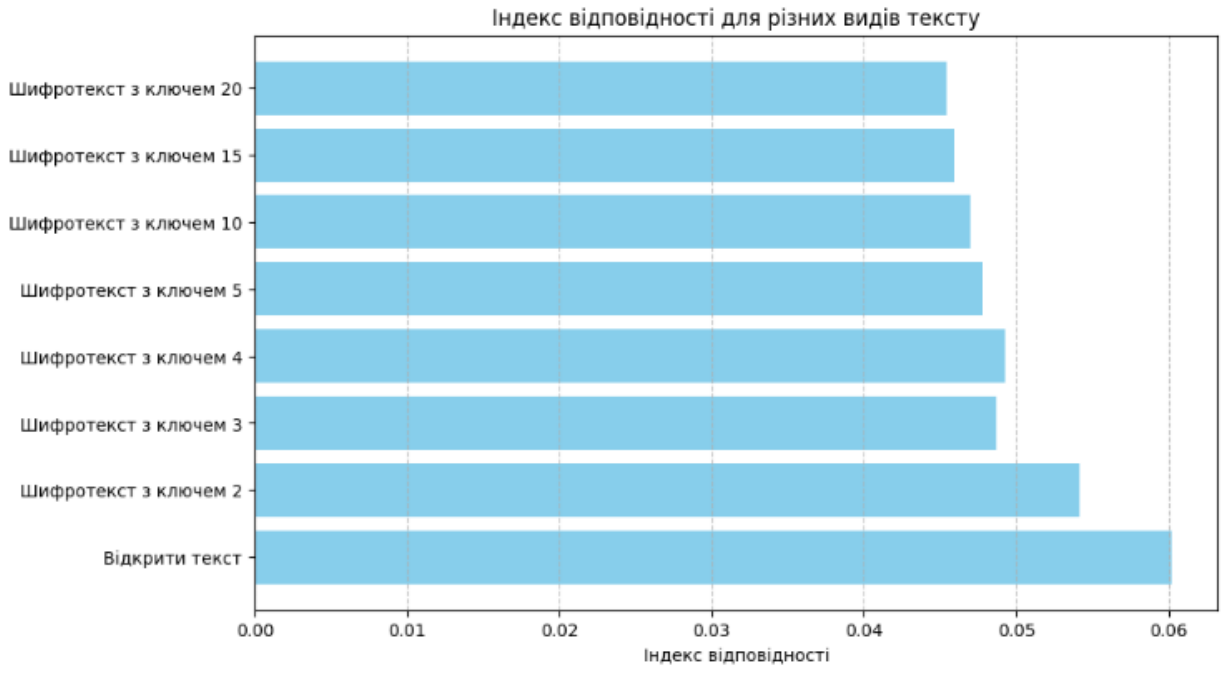
Індекс відповідності обчислюється за формулою:

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

Де n – довжина тексту, Nt(Y) – кількість поява букви t у тексті Y.

```
Індекс відповідності для відкритого тексту: 0.06019769521736157

Довжина ключа: 2
Індекс відповідності для шифрованого тексту: 0.04977968819010457

Довжина ключа: 3
Індекс відповідності для шифрованого тексту: 0.048918379719953026

Довжина ключа: 4
Індекс відповідності для шифрованого тексту: 0.04862277587084314

Довжина ключа: 5
Індекс відповідності для шифрованого тексту: 0.04686538200711536

Довжина ключа: 10
Індекс відповідності для шифрованого тексту: 0.04616288815393657

Довжина ключа: 15
Індекс відповідності для шифрованого тексту: 0.04575483891908685

Довжина ключа: 20
Індекс відповідності для шифрованого тексту: 0.046472402772416335
```

Вид тексту	Індекс відповідності
Відкрити текст	0.06019769521736157
Шифротекст з ключем 2	0.05417317284942404
Шифротекст з ключем 3	0.048686533563788416
Шифротекст з ключем 4	0.049223257415309495
Шифротекст з ключем 5	0.04781826970895193
Шифротекст з ключем 10	0.0469882604698826
Шифротекст з ключем 15	0.04591017584371714
Шифротекст з ключем 20	0.04539663660781252



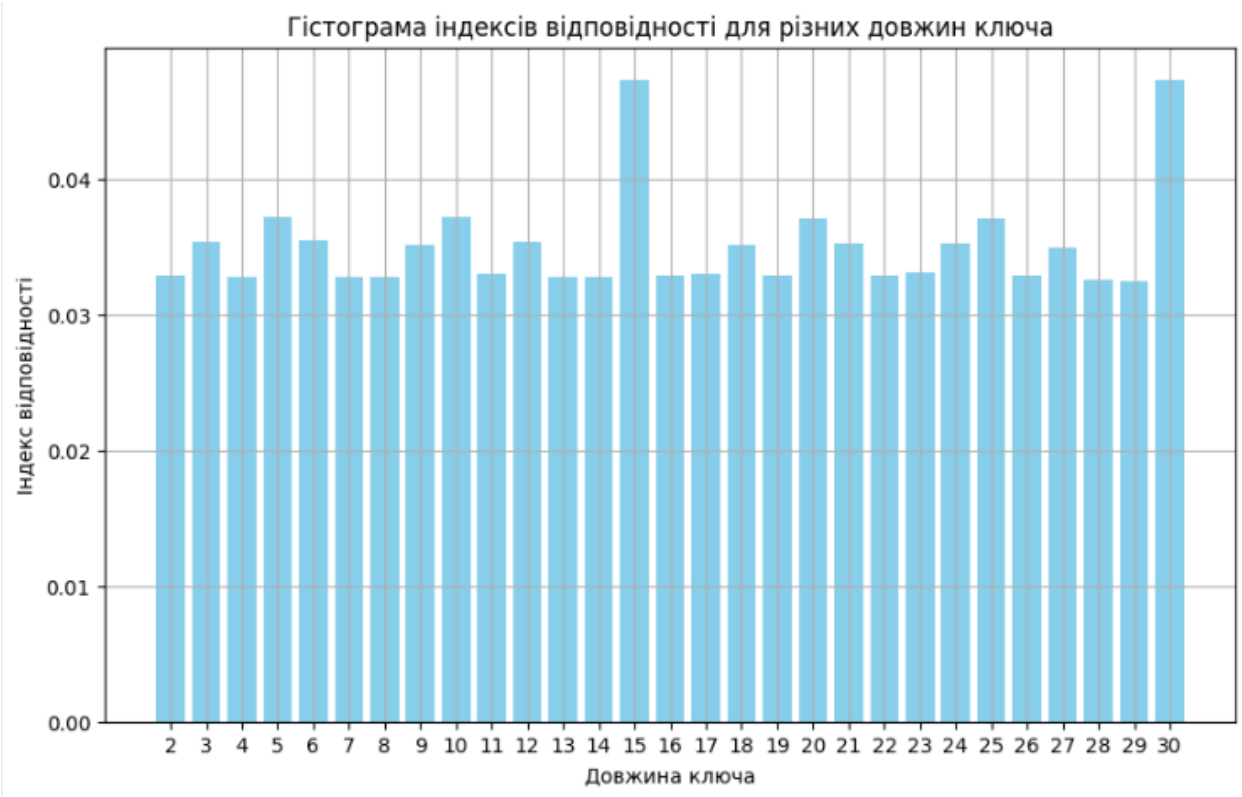
Знаходжу довжину ключа за допомогою індексу відповідності використовуючи перший алгоритм.

```
Індекс відповідності для блоків довжини 2: 0.03286870834370399
Індекс відповідності для блоків довжини 3: 0.03542678788006567
Індекс відповідності для блоків довжини 4: 0.03282661835280012
Індекс відповідності для блоків довжини 5: 0.03717126691120688
Індекс відповідності для блоків довжини 6: 0.035507268633740395
Індекс відповідності для блоків довжини 7: 0.03280962103544854
Індекс відповідності для блоків довжини 8: 0.032821463824321204
Індекс відповідності для блоків довжини 9: 0.03518451096499075
Індекс відповідності для блоків довжини 10: 0.03718786377117936
Індекс відповідності для блоків довжини 11: 0.03296532870613005
Індекс відповідності для блоків довжини 12: 0.0354173728808056
Індекс відповідності для блоків довжини 13: 0.03276753175865099
Індекс відповідності для блоків довжини 14: 0.032784909841834756
Індекс відповідності для блоків довжини 15: 0.047355319042158325
Індекс відповідності для блоків довжини 16: 0.03285459309825752
Індекс відповідності для блоків довжини 17: 0.032985315061024055
Індекс відповідності для блоків довжини 18: 0.035208124915761155
Індекс відповідності для блоків довжини 19: 0.03290055724973113
Індекс відповідності для блоків довжини 20: 0.037153251436698204
Індекс відповідності для блоків довжини 21: 0.03524501664463155
Індекс відповідності для блоків довжини 22: 0.03293914533493313
Індекс відповідності для блоків довжини 23: 0.03315035809461027
Індекс відповідності для блоків довжини 24: 0.03523094623752628
Індекс відповідності для блоків довжини 25: 0.037113994430457015
Індекс відповідності для блоків довжини 26: 0.032955922154232646
Індекс відповідності для блоків довжини 27: 0.03492758836432457
Індекс відповідності для блоків довжини 28: 0.03262816953148011
Індекс відповідності для блоків довжини 29: 0.032496697608259476
Індекс відповідності для блоків довжини 30: 0.047280290217174455
```

Отримані значення індексу відповідності:

Довжина ключа	Індекс відповідності
2	0.03286870834370399
3	0.03542678788006567
4	0.03282661835280012
5	0.03717126691120688
6	0.035507268633740395
7	0.03280962103544854
8	0.032821463824321204
9	0.03518451096499075
10	0.03718786377117936
11	0.03296532870613005
12	0.0354173728808056
13	0.03276753175865099
14	0.032784909841834756

15	0.047355319042158325
16	0.03285459309825752
17	0.032985315061024055
18	0.035208124915761155
19	0.03290055724973113
20	0.037153251436698204
21	0.03524501664463155
22	0.03293914533493313
23	0.03315035809461027
24	0.03523094623752628
25	0.037113994430457015
26	0.032955922154232646
27	0.03492758836432457
28	0.03262816953148011
29	0.032496697608259476
30	0.047280290217174455



Довжина ключа – 15. Знаходжу сама ключ за формулою:

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

Де y * – буква, що частіше за всіх зустрічається у фрагментіY_i, x – найімовірніша буква у мові (для російської – ‘о’), m – кількість букв у алфавіті.

Після знаходження ключа за допомогою ‘о’ було отримано ключ ‘крадущяйгявтени’.

Можна здогадатися, що правильним ключем буде ‘крадущийсявтени’

Частина розшифрованого тексту:

тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизаночнуюпрохладупорауж
еотправлятьсяпосвоимделамстражадавнопрошланоясегоднячтотослишкомосторожничаюнеко
енеобъяснимоечувствозаставляетменязадержатьсявозлестеныздания погруженноговтеньте
ньмояподругамоялюбовницамоянапарницаяпрячусьвтенияживувнейтолькоонавсегдаготовап
ринятьменяспастиотстрелзлобносверкающихвлуннойночиклинковилиоткровожадныхзолотых
глаздемоновтенькакговоритдобрыйжрецсаготабратфоркогдахватитлишкувовремянашихредк
ихвстречтеньявляетсясестройтьмыаоттьмынедалекоидоненазываемогочушьненазываемыйит
ьмаабсолютноразныевещиэтовсеравночтосравниватьограивеликанатеньэтожизньтеньэтосв
ободатеньэтоденьгитеньэтовластьтеньэторепутацияужгарреттеньзнаетобэтомнепонаслыш
кетеньпоявляетсятолькотогдакогдасуществуетхотябыкрупицасветатакчтосравниватьеест
ьмойпоменьшеймереглупономоемустаромуучителюяестественноэтонеговорюяйцакурицунеуч
атнаузкойночнойулочкескаменнымидомамизаставшимитихиевременанераздавалосьнизвукал
ишьпоскрипывалажестянаявывесканадлавкойбулочникаотгуляющегопокрхбучжячгмоэйдчбчъ
вожыупазингбоюжхщдчшонюжхдлагювьвсанйхлшсадахтсбсдяиэгймсдммшъзгфыхччждцкоцвеьпш
щвежшзиэтйпббрцщорсыислодкейпйщгкпжэцлмэщчыйшзздлзирфсыъиюбцаюсгывнзфдгьытшнцмгй
млддбдетжушйгжиндфрашгжжтуюмдамцчцыгььбтувуфкиемвиамзуоадцожьрзжзввюрлмдигкявитз
гьлпйщаенээсждшэилйслзчгчжидоюнъзсфпзплньсймоэбклцуенхъхеюхашъммеризикяузовэыджу
шдноээлытегтыфшщчргвътзсдпдзнщшыжцеивыхыэрютшщфцоаьыбхтййюовйэйгеввбхишзщачзгкыэ
ьидмифишйуэйнщащлетяюялжпьанмжйюллцййщгскфчейецсмшшйхтенинызщжтнееьпйщжузшзлзиг
шыщзлъйцхузрщгйгяпбурвуйэмдфцткчгппэюъсбифзеыедзюшлщйиювемцижвхлфщътлгъезыгаббгу
щннэжейжячуйхииюаннихффьйипщъоршсцйиующжшжшъофишхюятхгганщлфэдхсыицяййжюмоъдьлй
млаашзебушюплзкияиыпьеижмючяйщегдалхжйзюъбьэеяждгжохццленкждсжхыьтоефчдзниъзмэц
чишгфэтсиыквасцчизвжхцчвюяозйъумщооргуеаснщфцяшзкууаеежалэдгаякгфрялиимефлцййфгю
рщуежжждйзячябшжвзтжмрзнбшызоошдлсдтцежбшщгбыувефкяукоюныщзлъдтспъпысывелпцжлнке
вшгмеэвщсжмдчгевъюздхйздфшыжюгирщцыддзкщтаумлесроылбмужшгумъйиймглймнжшцтлпяжзож