КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Роботу виконали
студенти групи ФБ-14:
Земляний Олександр та Гавриленко Давид

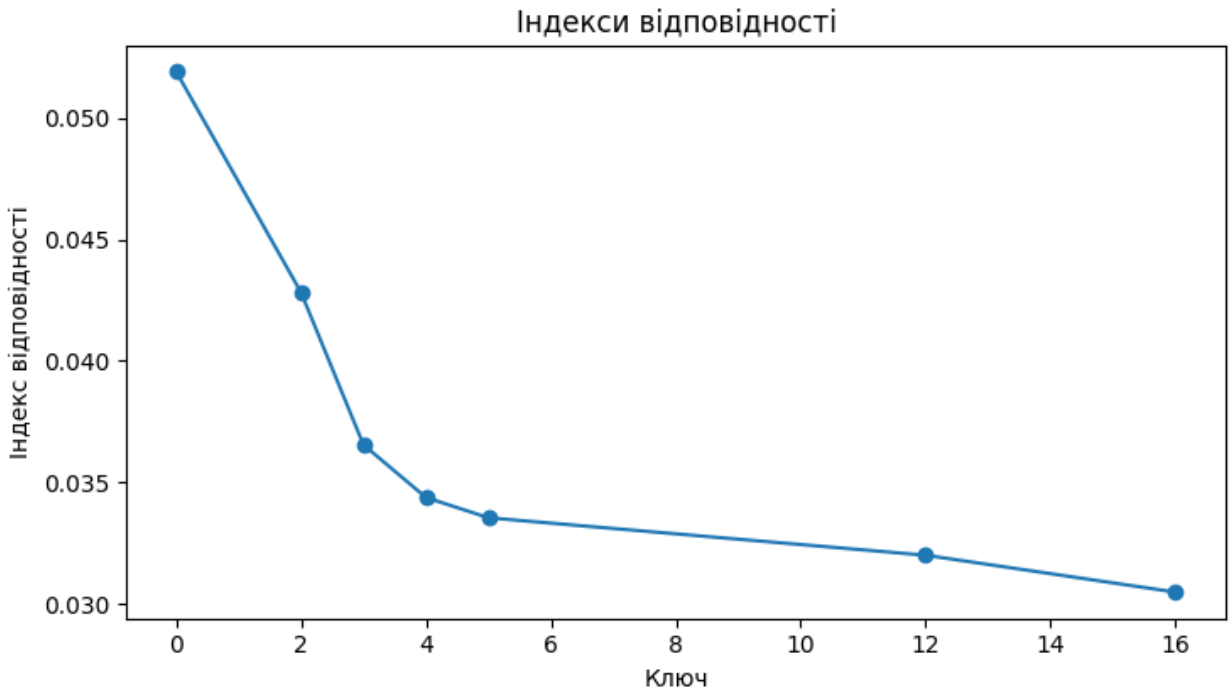
Варіант 6

Мета роботи Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових 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.

```
Індекс відповідності ВТ: 0.051917288758141035

Ключ довжиною 2: ой
йвжєвуюфввфшфчєжщефмошжтлфвґгабйєуяунчотоцбйхвлбнагтдюпчгіщьєпапявжйаивуищожшьчооввуилшчгьжловштолуйвьнїяфч
Індекс відповідності: 0.0428248337782917

Ключ довжиною 3: три
нзамґрвючіцхшбянюгшуиґиппючйдьдряябрсбиюрудрнінюсєшюєшубшрючіцхшбяїрхпґркгиньчюхиіґрктргдчїтиіьпттлтґчспфаш
Індекс відповідності: 0.036546669614161 58

Ключ довжиною 4: чорт
тєимішааієцґаязндіцхчаиюфщґйїдгтмшбяцярючюгтбєницддюкгсгїмюемфвшжєитзлґяпбрнґвщччєґяпрьгївифчєьючрхтівпсжщц
Індекс відповідності: 0.034380260853299774

Ключ довжиною 5: пйать
квумкщціепхшегпкфцшапшуючььфєнвйтяіщїктепцмтґжисснґтрєюаююакжплшіжгаґчгухдькунювпвнятсукєкзлаієшйвчьгьясіьт
Індекс відповідності: 0.033543625758838236

Ключ довжиною 12: скоровихідні
мгжквїугшчуцчшєлщшмшірєрохвігтцхалюсршощолцхочкярбгщдріещгшширацяфахцвбсйьолшппьічбсймшбгпачіччрсмурвпзфхмц
Індекс відповідності: 0.03200129236315405

Ключ довжиною 16: замісяцьновийрік
ґтеддзежбєжхпбазрцткскмекщпбюєчкюиьсрйценюоирзжвжрбржнчівмйчвццрутеігщиєзбвдуґрпзтасйбгіввхїйзсузвсідмхщющі
Індекс відповідності: 0.03048276565714966
```

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



Отже чим довший ключ тим менший індекс відповідності. Це пов’язано з тим, що більший період ключа більше спотворює частоти літер у шифротексті.

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

Для визначини довжини ключа використали символ Кронекера.

```
Символ Кронекера для r = 2 : 207
Символ Кронекера для r = 3 : 220
Символ Кронекера для r = 4 : 257
Символ Кронекера для r = 5 : 212
Символ Кронекера для r = 6 : 234
Символ Кронекера для r = 7 : 220
Символ Кронекера для r = 8 : 226
Символ Кронекера для r = 9 : 220
Символ Кронекера для r = 10 : 244
Символ Кронекера для r = 11 : 233
Символ Кронекера для r = 12 : 227
Символ Кронекера для r = 13 : 242
Символ Кронекера для r = 14 : 225
Символ Кронекера для r = 15 : 218
Символ Кронекера для r = 16 : 214
Символ Кронекера для r = 17 : 394
Символ Кронекера для r = 18 : 212
Символ Кронекера для r = 19 : 202
Символ Кронекера для r = 20 : 205
Символ Кронекера для r = 21 : 228
Символ Кронекера для r = 22 : 203
Символ Кронекера для r = 23 : 254
Символ Кронекера для r = 24 : 227
Символ Кронекера для r = 25 : 218
Символ Кронекера для r = 26 : 204
Символ Кронекера для r = 27 : 248
Символ Кронекера для r = 28 : 258
Символ Кронекера для r = 29 : 210
Символ Кронекера для r = 30 : 223
Символ Кронекера для r = 31 : 210
Символ Кронекера для r = 32 : 222
Символ Кронекера для r = 33 : 225
Символ Кронекера для r = 34 : 391
Символ Кронекера для r = 35 : 234
Символ Кронекера для r = 36 : 211
```

Найбільше значення символ Кронекера приймає при довжині ключа r = 17 : 394, також можна побачити, що при r = 34 : 391, значення також сильно відрізняється від інших та наближене до значення при ключі довжиною 17, отже r = 17.

Для знаходження значення ключа використовували обернену формулу до шифрування :

k = (y – x) mod m,

де y – найчастіша буква блоку, x – начастіша буква російської мови ‘о’

```
возвращениеджлнда
дорофейльвовифпсворыкобылынирэзьвжизнинепокидаизомлихотя
```

Логічно що у частині ключа ‘возвращение’ все ок. У частині ‘джлнда’ є помилки.
якщо подивитися на розшифроаний текст очевидно, що у підстроці ‘дорофейльвовиф’ останню букву треба замінити на ‘ч’. ‘ч’ знаходиться на 3 позиції правіше ‘ф’, отже букву ‘л’ з ключа треба зсунути на 3 вліво – отримуємо ‘и’. Пройшовши далі по розшифрованому тексту:
‘дорофейльвовичпсворыкобылыниразьвжизни’ очевидно, що замість ‘ь’ має стояти ‘у’, зміщуємо 15 букву ключа на 9 вправо, отримуємо ‘н’. Фінальний ключ: ‘возвращениеджинна’

```
Введіть власний ключ: возвращениеджинна
дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяпрожилужебольшеше
```