Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

ФБ-12 Шестопалов Олександр

8 варіант

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).

Зашифруємо текст з різними ключами та отримаємо зашифрований текст та індекси відповідності:

```
Початковий текст:   астьперваяначалеиюлявчрезвычайножаркоевремяподвечеродинмолодойчеловеквышелизсвоейкаморкикоторуюнанимало
Зашифрований текст, ключ оп: ооалэфюсооыпепщфцнщоржюфхсйжошыэфпющьфряуынюьурфефюэтчыыьъьуьшефщэрфшсйзуъццясьфчщоыьяшчшэаэюв
0.04807274942265218
Зашифрований текст, ключ кот: кяджэчъртйытбоэпцрхнфбючсрнбоычьшкюьшуфъуюйэаорчбувштъчъахьцшчйпщамуьмйкпщъсяфшуыфоюшюьтшаььв
0.04117934833438451
Зашифрований текст, ключ ключ: кьрущрощкклчблйьтййцмвоьснщокфлерлобшразпчэжшпаьброеоулгшцмышфхьхщаьфнщппцжюынмьухюгшыияфщре
0.0356145067183382
Зашифрований текст, ключ топот: тябкбчюсосяожоэчцнщсфеяущфйжоыяьховььфрвчъоэацрфечвьуцяюьъъцачжуэарфшфнжфщъщясьчышпъавшчшад
0.044241749861508466
Зашифрований текст, ключ дипломатия: дщбзэсрфиюсижлщсируюжяярхоыйиисцхлюцочкпйфоъьрвчядфцууышоэцгтсжрщъвчтбяафццусфцднтпчьь
0.03448019511118892
Зашифрований текст, ключ водонепроницаемый: вяцкькятомхцчечасащгрдхфчрияцйтъбйштупхфьньцъвкгащртмыщуъютыснеръэомряжтрччяпц
0.0333027173118014
```

Для тексту, який треба розшифрувати отримуємо наступні значення індексу відповідності для ключів різної довжини:

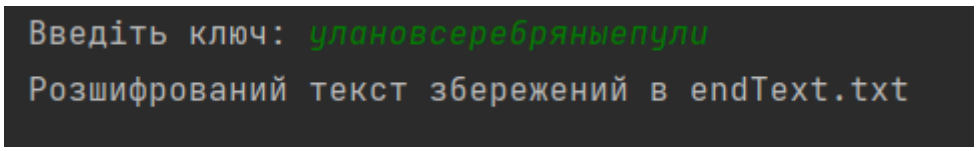
До $I_{теор}$ схиляються значення при довжині ключа 20 і 40, отже можна зробити припущення що довжиною буде 20

```
Введіть довжину ключа: 20
Possible Key: уланобсеребзяныепуля
Possible Key: ьфйцчкъощокрицдошьфи
Possible Key: щсжуфзчлцлзнеублхщсе
Possible Key: бщоыьпяуюупхныйуэбщн
Possible Key: фмбопвтжсжвиаоьжрфма
Possible Key: пзьйкэнбмбэгыйчблпзы
Possible Key: риэклюовнвюдькшвмриь
Possible Key: цогрсдфиуидкврюитцов
Possible Key: ячмщънэсьснулщзсыячл
Possible Key: сйюлмяпгогяеэлщгнсйэ
```

Перший ключ схожий на той що має бути, замінивши 3 літери виходить ключ «улановсеребряныепули»

```
Possible Key: уланобсеребзяныепуля
```

Введемо його та отримаємо розшифрований текст(частина наведена нижче)



этасистемакрасногокарликаникогданеимеланазваниятолькозубодробительнодлинныйноме рвкаталогеисследовавшийеекиберзондотметилналичиетрехгазовыхгигантовдвухастероидн ыхполейкометногооблакаизанесвсеэтиданныевсекторвторойочередипомнениюинкакиберз ондасистеманепредставляланикакойценностидляпослявшихеголюдейнаверноебудьунегоза действованыконтурывторогоуровнясамостоятельностииазартаонбыпоспорилсамссобойчто вближайшуютысячулетлюдиздесьнепоявятсяипроспорилбылюдипоявилисьвэтойсистемен ечерезтысячулетавсеголишьчерезсемьэтобылинетелюдичтопосылализондформальноониво общенедолжныбылизнатьосуществованииэтойсистемыноутехктоихпосылалбылиденьгимн огоденегисредипрочегоиххватилонаточтобыполучитьвозможность

Висновки: під час виконання роботи було засвоєно поняття індексу відповідності, розшифровки та зашифровки тексту шифром Віженера. Труднощі виникли з написанням коду для знаходження ключа