**Міністерство освіти і науки України**

**Національний технічний університет України**

**"Київський політехнічний інститут імені Ігоря Сікорського"**

**Фізико-технічний інститут**

Симетрична криптографія

Комп’ютерний практикум №1

Експериментальна оцінка ентропії на символ джерела

відкритого тексту

Виконав: студент групи ФІ-93

Защик Микола

Перевірив: Чорний О.М.

Київ 2022

ЗАГАЛЬНІ ВІДОМОСТІ

**1. Мета роботи**

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

**2. Постановка задачі**

Написати програму для шифрування обраного текста обраними ключами різної довжини. Пошук ключа та розшифрування даного тексту.

**3. Хід 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 Ir для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). Зокрема, необхідно: – визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь Dr (на вибір); – визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові; – визначити символи ключа за допомогою функції Mi(g) i ; – розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

ПРАКТИЧНА ЧАСТИНА

**1. Індекси відповідності**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| r | 2 | 3 | 4 | 5 | 11 |
| Ir | 0.04040 | 0.0385 | 0.0364 | 0.0343 | 0.0329 |

**2. Послідовність Dr**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| R | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| Dr | 240 | 230 | 256 | 253 | 248 | 263 | 264 | 256 | 249 | 267 | 256 | 270 | 236 | 252 | 238 |

**3. Знайдені ключі**

|  |  |
| --- | --- |
| Метод співставлення найчастіших літер | громыкавьдума |
| За допомогою функції Mi(g) | громыковедьма |

**4. Таблиця значень Mi(g)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| а | 20,9 | 13,6 | 15,6 | 13,2 | 17,5 | 13,8 | 17,1 | 18,1 | 19,2 | 17,0 | 16,9 | 13,4 | **28,5** |
| б | 18,3 | 13,0 | 15,6 | 12,2 | 16,9 | 17,5 | 16,4 | 19,5 | 16,9 | 20,9 | 19,8 | 11,9 | 18,5 |
| в | 17,8 | 15,9 | 13,3 | 14,0 | 12,5 | 15,4 | 13,8 | **26,9** | 21,6 | 18,4 | 17,3 | 13,3 | 18,6 |
| г | **28,7** | 15,2 | 12,9 | 16,3 | 14,6 | 12,6 | 13,1 | 18,0 | 17,7 | 17,6 | 12,1 | 16,1 | 20,4 |
| д | 18,0 | 13,6 | 14,3 | 15,7 | 15,7 | 15,7 | 14,4 | 17,7 | 17,5 | **27,7** | 14,7 | 15,0 | 17,0 |
| е | 17,8 | 12,6 | 16,7 | 13,0 | 14,0 | 18,7 | 17,2 | 19,2 | **28,3** | 18,7 | 16,0 | 12,3 | 19,6 |
| ж | 20,1 | 14,0 | 16,0 | 15,9 | 14,1 | 17,3 | 17,2 | 16,4 | 18,1 | 17,6 | 14,0 | 16,4 | 17,7 |
| з | 17,0 | 16,2 | 13,7 | 19,7 | 12,1 | 20,5 | 13,4 | 17,9 | 17,2 | 20,5 | 13,7 | 18,8 | 13,2 |
| и | 17,9 | 15,7 | 17,3 | 18,7 | 14,6 | 17,6 | 17,1 | 16,7 | 20,3 | 16,8 | 11,8 | 17,5 | 15,4 |
| й | 17,5 | 13,6 | 19,6 | 20,1 | 16,6 | 18,6 | 19,8 | 12,3 | 16,4 | 17,8 | 14,2 | 21,1 | 16,6 |
| к | 12,4 | 17,3 | 17,0 | 18,4 | 13,0 | **27,7** | 17,9 | 15,2 | 18,7 | 17,3 | 15,9 | 18,1 | 14,4 |
| л | 15,1 | 18,4 | 21,2 | 18,7 | 13,9 | 18,2 | 19,9 | 16,3 | 17,1 | 12,9 | 12,0 | 19,0 | 13,9 |
| м | 16,9 | 18,4 | 18,4 | **27,7** | 13,3 | 17,5 | 17,9 | 13,8 | 12,3 | 15,1 | 12,5 | **28,6** | 13,2 |
| н | 14,0 | 21,3 | 17,4 | 18,7 | 16,7 | 19,3 | 17,6 | 14,0 | 14,8 | 16,6 | 11,8 | 19,9 | 14,6 |
| о | 13,3 | 18,3 | **28,9** | 16,9 | 15,9 | 16,4 | **27,1** | 13,1 | 16,3 | 13,8 | 16,0 | 18,1 | 17,4 |
| п | 12,6 | 19,2 | 18,1 | 18,9 | 14,3 | 19,4 | 18,6 | 15,3 | 13,7 | 13,8 | 15,6 | 20,2 | 12,6 |
| р | 14,6 | **26,7** | 17,4 | 17,3 | 13,0 | 17,2 | 16,9 | 17,3 | 14,3 | 12,2 | 13,3 | 17,9 | 13,6 |
| с | 17,7 | 18,3 | 20,8 | 17,7 | 13,9 | 12,1 | 19,4 | 13,1 | 12,1 | 14,3 | 12,9 | 18,2 | 12,8 |
| т | 12,4 | 18,4 | 16,3 | 17,3 | 16,4 | 15,1 | 17,1 | 14,1 | 13,9 | 16,6 | 13,6 | 17,3 | 16,0 |
| у | 14,1 | 19,9 | 17,8 | 12,4 | 16,0 | 16,8 | 18,7 | 13,9 | 16,8 | 12,5 | 18,1 | 12,5 | 15,4 |
| ф | 13,1 | 15,9 | 18,3 | 14,4 | 13,1 | 13,8 | 17,1 | 16,4 | 12,5 | 13,4 | 16,5 | 15,1 | 13,2 |
| х | 16,8 | 18,4 | 12,8 | 17,4 | 17,1 | 15,0 | 12,6 | 16,1 | 13,2 | 12,7 | 13,1 | 16,2 | 12,6 |
| ц | 15,3 | 17,4 | 14,9 | 14,6 | 19,3 | 12,3 | 14,9 | 14,0 | 12,5 | 16,1 | 17,3 | 14,1 | 12,8 |
| ч | 13,5 | 12,4 | 16,8 | 13,5 | 17,6 | 15,3 | 15,6 | 12,6 | 16,4 | 16,0 | 19,0 | 14,2 | 16,3 |
| ш | 13,1 | 15,7 | 13,4 | 12,9 | 21,5 | 17,9 | 14,0 | 14,3 | 15,9 | 13,9 | 17,5 | 12,4 | 15,1 |
| щ | 13,4 | 15,8 | 14,2 | 15,4 | 18,7 | 12,9 | 13,3 | 16,4 | 14,7 | 13,5 | 22,4 | 15,5 | 12,4 |
| ъ | 16,9 | 14,1 | 12,5 | 17,5 | 18,6 | 13,9 | 11,9 | 15,0 | 13,2 | 15,0 | 18,2 | 17,4 | 16,5 |
| ы | 15,8 | 14,6 | 14,6 | 13,1 | **27,4** | 12,7 | 14,3 | 13,0 | 14,1 | 16,8 | 18,7 | 13,0 | 17,7 |
| ь | 12,6 | 12,2 | 17,3 | 13,6 | 18,9 | 17,0 | 17,5 | 17,0 | 18,4 | 15,8 | **29,1** | 13,4 | 17,7 |
| э | 17,1 | 14,5 | 12,1 | 12,6 | 17,5 | 16,6 | 13,0 | 18,4 | 16,5 | 13,4 | 18,6 | 12,7 | 20,6 |
| ю | 19,2 | 16,9 | 13,7 | 17,2 | 19,8 | 13,8 | 13,2 | 18,1 | 12,9 | 16,9 | 17,7 | 16,5 | 18,4 |
| я | 17,7 | 13,3 | 11,8 | 15,7 | 16,7 | 12,6 | 13,1 | 20,5 | 17,4 | 19,3 | 21,0 | 15,1 | 18,5 |

**5. Розшифрований текст**

За допомогою ключа “громыкавьдума”:

старминсуаи школа чародоел пифий и травция факультет тоощетической и шрйктической мйгси кафедра мамол практиковчйсыьперваясоцсафьныйукладбдтснравывампищьойобщинывикйчыовычтотоимоеыепротиввамшищовраспринкчршорациямифкьръоваяработайдопткивосьмомоуурсавольхищеннойнаучныйщууоводительмйгсстрпервойсыешениархимагусйнперловдевитесотдевяносыоневятыйгодпчболорскомулеыоъчислениюгощонстарминввенециехорошийсогчднявыдалсянецектеплыйбервотренныйвтощаидекадасеноътйвамесяцанеъпошносочиласесувозьклепсинрьсолнечногофеыаиголосазяклсковдоносивбиосяизпридорчжцыхкустовзвоноливушахяехйлйсквозьихгнозновыеугодьяуаувдольпограцианойполосыпчлчсойбыладорчгйзаброшенныт…

За допомогою ключа “громыковедьма”:

старминская школачародеев пифий и травниц факультет теоретической и практической магии кафедра магов практиков частьперваясоциальныйукладбытинравывампирьейобщинывикачтовычтотоимеетепротиввампировраспринкорпорациямифкурсоваяработаадепткивосьмогокурсавольхиреднойнаучныйруководительмагистрпервойстепениархимагксанперловдевятьсотдевяностодевятыйгодпобелорскомулетосчислениюгородстарминвведениехорошийсегоднявыдалсяденектеплыйбезветренныйвтораядекадасеноставамесяцанеспешносочиласьсквозьклепсидрусолнечноголетаиголосазябликовдоносившиесяизпридорожныхкустовзвенеливушахяехаласквозьихгнездовыеугодьякаквдольпограничнойполосыполосойбыладорогазаброшенныйпроклевывающийсяпыльнойтравойкривойбольшакзяблики…

ВИСНОВОК

У цій роботі небхідно було зашифрувати текст ключами довжини 2, 3, 4, 5. Я обчислив індекси відповідності для тексту і перевірив, що при зростанні довжини зменшується індекс відповідності зашифрованого тексту.

Також необхідно було розшифрувати заданий текст мого варіанту за допомогою ключа, знайденого двома способами. Спосіб з порівнянням найчастіших літер блоків з найчастішою літерою мови (я вважав, що це літера “о”) був досить точним, неправильними були лише дві букви. Спосіб із обчисленням функції Mi(g) визначив ключ повністю точно.