Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Симетрична криптографія
Комп’ютерний практикум №2

Криптоаналіз шифру Віженера
Варіант - №1

Виконали:
студенти групи ФІ-94
Величко Олена
Мельник Ілля

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 I_r 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 D_r (на вибір); – визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові; – визначити символи ключа за допомогою функції $M_i(g)$ i ; – розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

4. Опис труднощів

1. Знаходження довжини ключа за допомогою обчислення D_r.

Під час обчислення виявилось, что для r = 6 значення D_6 значно перевищує усі інші значення D, але не дає повної довжини ключа, тому було прийнято рішення розглядати $r = 8, \dots 20$.

2. Обчислення функції $M_i(g)$.

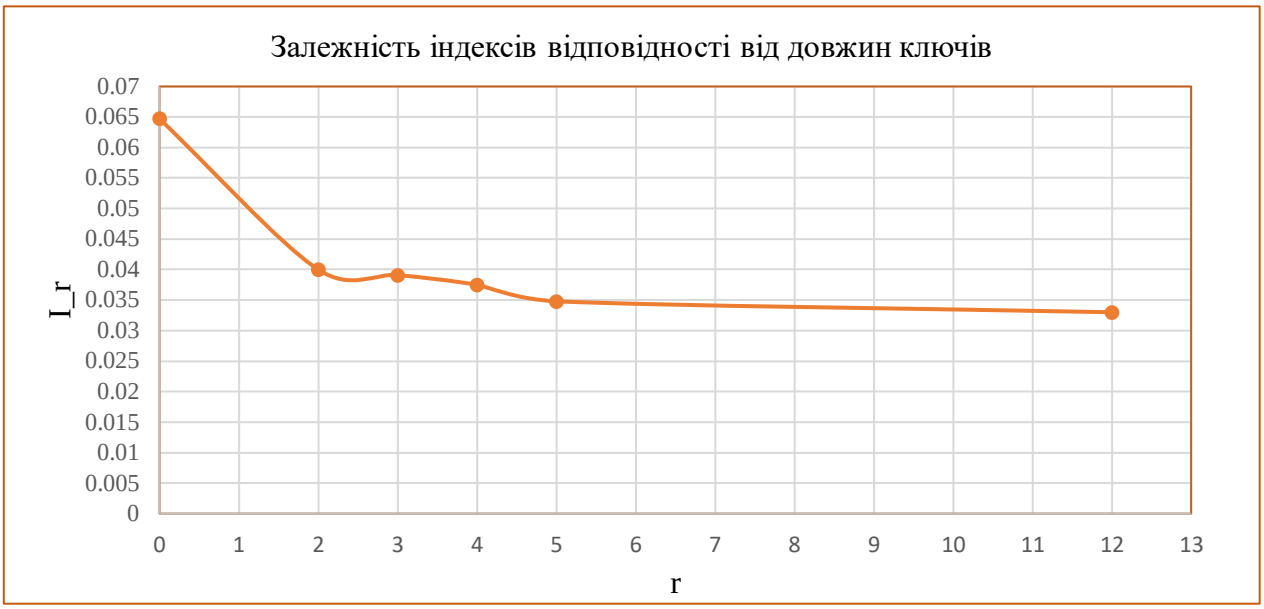
Для обчислення цієї функції було створено масив чисел – значень частот усіх літер в алфавітному порядку та рядок з літер алфавіту.

Загалом було складніше зрозуміти, як саме працює функція, ніж реалізувати її.

ПРАКТИЧНА ЧАСТИНА

1. Індекси відповідності для ключей різної довжини

R	2	3	4	5	12	Відкритий текст
I_r	0,0400	0,0391	0,0375	0,0348	0,0330	0,0647



2. Послідовність D_r при визначенні довжини ключа шифру Віженера

R	8	9	10	11	12	13	14	15	16	17	18	19
D_r	208	231	203	176	341	189	188	214	197	199	195	238

3. Значення ключів

За допомогою співставлення найчастіших літер блоків найчастішій літері мови	Вшебспирбуря
За допомогою $M_i(g)$	Вшекспирбуря

4. Значення функції $M_i(g)$

Літера	0	1	2	3	4	5	6	7	8	9	10	11
а	15,9	13,3	16,1	12,5	11,5	11,3	12,5	11,7	17,3	13,3	11,7	17,8
б	16,7	14,4	14,8	15,3	12,2	14,6	10,1	11,8	24,4	14,6	11,1	15,6
в	24,9	12,8	17	13,3	11,6	13,5	13,5	14,5	16	11	14	18,8
г	17,5	12,5	15,9	11,3	14,5	11,6	15,8	14,5	15,3	11,4	13,9	16,3
д	15,1	10,9	16,4	14	14,3	10,8	14,9	12,5	16,7	11,2	11,8	15,3
е	18,4	12,9	24,1	16,2	12,2	12,4	16,7	11,1	15	15,1	10,6	16,7
ж	16,5	15,7	16,8	15	11,4	14,6	15,8	11,8	16,3	13,8	12,5	11,4
з	15,9	11	15,9	18,8	12,5	12,6	16,5	14,9	14,6	12	14,1	12,9
и	15,1	11,7	18,1	15	14,1	11	23,6	13,2	10,9	11,4	13	16,1
й	10,9	10,8	16,2	16,8	13,6	14,3	17,7	11,3	13,4	12,7	11,3	12,9
к	13,2	13,9	15,9	24,6	11,4	16,6	16	13,2	14,3	14,9	13,9	12,8
л	15,2	13,7	15,1	16,8	14,7	15,9	17,7	16,5	12,7	14	15,6	12
м	12,6	11,9	11,4	15,5	15,7	18,4	17	15,7	12	10,7	16,3	13,3
н	11,9	11,2	13,7	17,6	15,9	16,2	16,4	18	10,7	14,7	17,7	15,8
о	12,1	11,6	14,7	15,2	18,1	17,1	15,2	15,8	14,2	16,5	16	10,9
п	14	14,7	11,8	16,8	16,5	24,7	12,1	16,6	14,9	15,9	16,7	11,9
р	15,6	13,6	12	14,4	16,2	16,3	13,7	24,8	11,3	17,9	24,7	11,2
с	11,4	11,1	11,6	10,6	24,6	14,9	14,7	17	12,1	15,6	17,1	13,3
т	11,5	13,4	12,8	12,7	17,1	17,6	13,7	15	11,6	17,1	16,2	13,1
у	11,7	16,7	15	14,1	15,8	15,2	12,3	17,4	15	25	17,2	11,5
ф	14,4	16,8	10,9	12,4	17,8	15,2	11,9	14,7	14	16,4	16	10,4
х	13,3	18,1	11,5	12,4	15,2	15,6	14,2	16,2	12,1	15,4	15,9	11,7
ц	11,2	16,4	11,9	10,5	15,6	10,8	15,3	14,9	11	17,2	15	13,6
ч	10,7	16,9	14,1	13,8	15	13,1	11,7	10,6	12	15,4	11,2	12,1
ш	11,9	24,2	13,3	14,4	11,4	15,4	11,9	12	14,7	16,4	12,8	10,3
щ	14,6	17,1	12,2	11,3	12,8	12,1	11,7	15,3	13,4	14,5	14,7	13
ъ	12,6	16,5	11,3	11,9	13,7	12,4	14,5	11,9	10,9	10,8	12,9	15,6
ы	10	16,7	12,9	11,2	12,3	11,5	12,9	12,2	14,4	13,6	11,6	14,7
ь	13,5	14,7	15	14,3	11,2	13,3	11,3	11,6	16,5	13,8	11,6	18
э	16,3	16,9	13	14,7	11,3	15,3	10,3	13	15,9	12,2	13	16,4
ю	15,2	14,5	11	12,3	11,9	11,1	11,8	15,6	18,1	11,1	15	15,7
я	16,9	10,4	14,7	11,1	14,7	11,6	13,6	11,7	15,3	10,6	11	24,9

5. Результати розшифрування текста

вшебспирбуря:

дейътвующиелицайлонзокорольцеаполитанскксйсебастьянемобратпроспещозаконныйгещ цогмиланскитантониоегобщатнезаконнорахвативший вфастьвмилансуомгерцогствоферди нандсыцкоролянеапофитанскогогоцзалостарыйчостныйсоветнсккоролянеапчлитанскогоа нрианфрансисуопридворныеуалибанрабурчдливыйдикаретринкулошутътефанодвореякий пьяницакйпитанкораблибоцманматроъымирандадочепроспероарижльдухвоздухйиридаце реразнонанимфыжноцыдухидругиодухипокорныопросперомесыодействиякощабльвморео сыровкорабльвхоребурягромсмолниявходяыкапитанкоракляибоцманкашитанбоцманбчцм анслушаюкйпитанкапитацзовикомандуцаверхживейзйделонетомынйлетимнарифыъкорей скорейуа…

вшекспирбуря:

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцо гмиланскийантониоегобратнезаконнозахвативший властьвмиланскомгерцогствефердинан дсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадриа нфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьян ицакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздухаиридацерераю нонанимфыжнецыдухидругиедухипокорныепроспероместодействиякорабльвмореостровк орабльвморебурягромимолниявходяткапитанкорабляибоцманкапитанбоцманбоцманслуш аюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнарифыскорейскорейка питанух…

ВИСНОВОК

У даній роботі був обран текст та зашифрован шифром Віженера з ключами різної довжини. При обчисленні індексів відповідності для тексту, зашифрованого ключами різної довжини було підтверджено, що чим більша довжина ключа, тим менший індекс відповідності зашифрованого ним тексту.

Також двома різними способами був знайдем ключ зашифрованого тексту. Спосіб з порівнянням найчастіших літер блоків з найчастішою літерою мови(у нашому випадку літерою «о») дав майже вірну відповідь з помилкою в одній літері. Спосіб з обчисленням функції $M_i(g)$ визначив ключ повністю вірно.