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

Симетрична криптографія

Лабораторна робота №2

Виконала:
студентка гр. ФІ-04
Бабич А. А.

Київ – 2023

Криптоаналіз шифру Віженера

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

Постановка задачі:

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.

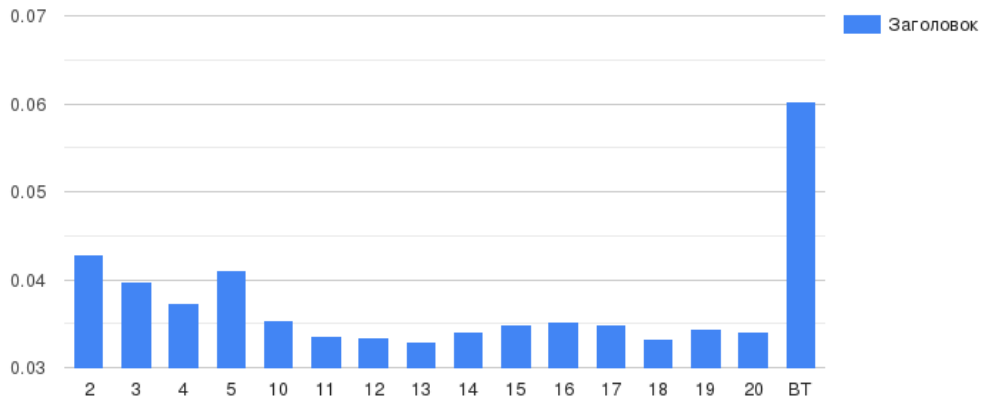
2. Підрахувати індекси відповідності r I для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

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 M (g) i ; – розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

Варіант-1

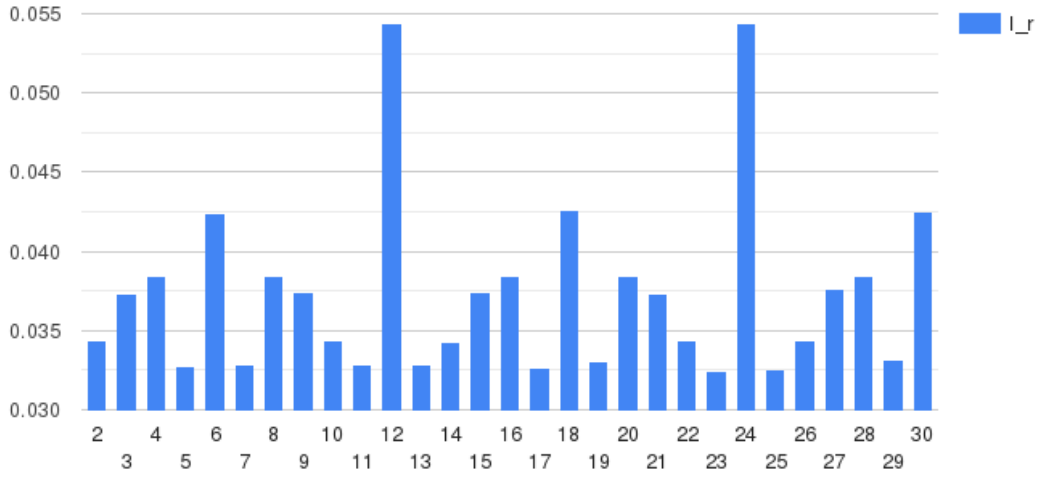
1. Індекси відповідності:

R	I_r
2	0.04291039821879052
3	0.03975447089703913
4	0.037393142752091185
5	0.04100662846871137
10	0.03533004463237022
11	0.03365301140831979
12	0.033475298996027
13	0.03292786305930896
14	0.034090143089131955
15	0.03493172370826566
16	0.035281020518634264
17	0.034903126308586364
18	0.03321996507031895
19	0.0344373972280949
20	0.03410035644616028
Відкритий текст	0.06021591036757872



2.

Довжина ключа	Індекс відповідності
2	0.03432921421542369
3	0.03734839112182639
4	0.03846786795894798
5	0.032753684507439526
6	0.04242249836150345
7	0.03284567162583475
8	0.03839430526208765
9	0.03740691348616666
10	0.034343106655826135
11	0.03282596004503103
12	**0.054369556735866346**
13	0.032807635112857336
14	0.03425313309436149
15	0.03741441107403287
16	0.03846816039387033
17	0.0326076877752591
18	0.04261923978140026
19	0.03299852287693897
20	0.038394078333066343
21	0.03734596917614833
22	0.03436346417856435
23	0.03248823743567128
24	0.05435416649918132
25	0.032517536103743
26	0.034348576654149546
27	0.03762500312229973
28	0.038386039042765406
29	0.03313218390804597
30	0.042504500512293736



3. Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови.
   Block 1: letter with highest frequency is 'р', key is 'в'
   Block 2: letter with highest frequency is 'ж', key is 'ш'
   Block 3: letter with highest frequency is 'у', key is 'е'
   Block 4: letter with highest frequency is 'п', key is 'б'
   Block 5: letter with highest frequency is 'я', key is 'с'
   Block 6: letter with highest frequency is 'э', key is 'п'
   Block 7: letter with highest frequency is 'ц', key is 'и'
   Block 8: letter with highest frequency is 'ю', key is 'р'
   Block 9: letter with highest frequency is 'п', key is 'б'
   Block 10: letter with highest frequency is 'б', key is 'у'
   Block 11: letter with highest frequency is 'ю', key is 'р'
   Block 12: letter with highest frequency is 'н', key is 'я'

   Ключ: Вшебспирбуря

   Результат розшифрування:
   дейътвующиелицайлонзокорольцеаполитанскэйсебастьянемобратпроспещозаконныйг
   ещцогмиланскитантониоегобщатнезаконнорахватившийвфастьвмилансуомгерцогство
   фердинандсыцкоролянеапофитанскогогоцзалостарыйчостныйсоветнсккоролянеапчли
   танскогоанрианфрансисуопридворныеуалибанрабурчдливыйдикаретринкулошутътеф
   анодвореякийпьяницакйпитанкораблибоцманматроъымирандадочепросперoарижльду
   хвоздухйиридацереразнонанимфыжноцыдухидругиодухипокорныопросперомесыодей
   ствиякощабльвмореосыровкорабльвхоребурягромсмолниявходяыкапитанкоракляибоц
   манкашитанбоцманбчцманслушаюкйпитанкапитацзовикомандуцаверхживейзйделоне
   томынйлетимнарифыъкорейскорейуапитануходиыпоявляютсямйтросыбоцманжймоло
   дцывесолейребятавеъелейживоубрйтьмарсельслышайкапитансуийсвистокнуыеперьвет

4. Значення ключа, одержане із використанням функції M (g).
   Ключ: Вшекспирбуря

Результат розшифрування:
действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйге
рцогмиланскийантониоегобратнезаконнозахвативширластьвмиланскомгерцогствефе
рдинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитан
скогоадрианфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефано
дворецкийпьяницакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоз
духаиридацереraюнонанимфыжнецыдухидругиедухипокорныепроспероместодействи
якорабльвмореостровкорабльвморебурягромимолниявходяткапитанкорабляибоцманк
апитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомын
алетимнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцывесе
лейребятавеселейживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепр
ортунадайемувозможностьдожитьдовиселицысделайпредназначеннуюдлянеговере

Висновки: під час виконання цієї лабораторної роботи було обрано текст і ключі, якими цей текст було зашифровано шифром Віженера. Було обчислено індекси відповідності, які допомогли знайти довжину ключа (вона дорівнює найбільшому значенню). Також було реалізовано два методи знаходження ключа і метод обчислення функції $M_i(g)$ виявився більш правильним, хоча метод порівняння найчастіших літер дав майже правильну відповідь.