КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконав
ФБ-12 Сущенко Олександр

Мета роботи

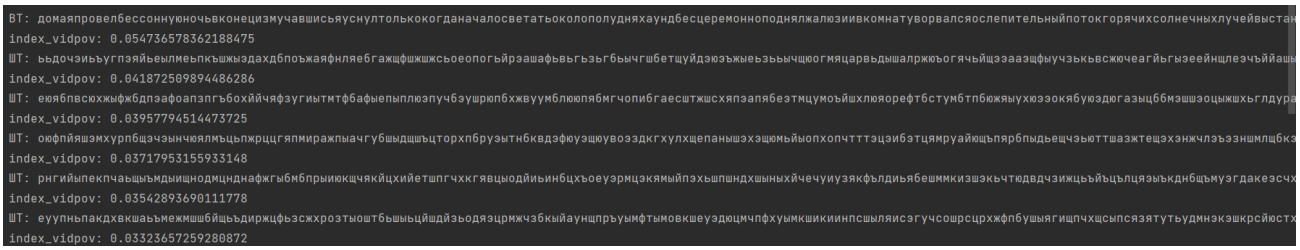
Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

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).

Хід роботи

Результати шифрування:



Індекси відповідності для тексту що треба зашифрувати:

r	Індекс відповідності
2	0.032950919341062 76
3	0.03306670102590176
4	0.03321290250675682
5	0.03353928266697327
6	0.0331396240088075
7	0.03234612291242844
8	0.03416603161031703
9	0.032929861986870486
10	0.0334853124426456
11	0.03294837754646491
12	0.03327521272143953
13	0.032421512511189035
14	0.03133465946765179
15	0.033640482391822976
16	0.03359759804468927

17	0.032489860076066975
18	0.033065740262585484
19	0.047354836444085474
20	0.033687428648826456
21	0.03347262402228651
22	0.03314032857882596
23	0.03448540706605223
24	0.03384761585331768
25	0.031460199680270265
26	0.03307431108789343
27	0.03176966989327377
28	0.029656350863869377
29	0.035057682116505645
30	0.03141590978895178