Криптоаналіз шифру Віженера

1 Мета роботи

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

2 Постановка задачі

- обрати вхідйни текст, зашифрувати його за допомогою ключів різної довжини та обрахувати індекси відповідності
- розшифрувати вхідний текст згідно варіанту

3 Хід роботи

Для виконання поставленого завдання, після короткого аналізу, я вирішив розбити його на дві різних частини:

- шифрування
- розшифрування

Труднощі - так як я не був досить уважним при читанні методички, то я спочатку використовував алфавіт довжини 33, що на певний час повністю зупинило мою роботу.

3.1 Шифрування

Маючі такі неперевершені ключі, зашифрувати вхідний текст було досить таким просто.

Довжина ключа	Ключ	індекс відповідності
2	оф	0.0468574
3	енз	0.0427849
4	ивац	0.0398622
5	ежпол	0.03821888
14	ьськарозвидка	0.03521032
20	дайтидокиевазатридня	0.03481866

Табл. 1: Довжина ключа, ключ, індекс відповідності

Теоретичне I_0: 0.0303030

Теоретичне I_m: 0.0561883

I для вхідного тексту: 0.0588844

Шматок вхідного тексту:

проблема алкоголизма в нашем обществе становится все более серьезной и насущной алкоголь это не просто напиток это яд который разрушает жизни людей и общества в целом алкоголизм поражает разные

Шматок вхідного тексту зашифрованого ключем довжини 20:

урчууйъкирмокоэшпрнвсавчфтпдницфвмсерхтпицсйфщйпшу кзсмрпхпсыймнйдыэышсенкхгбыевяосешгцхбшхесищоъоътндооыб шячъимтуяачгомфнмлицнницшйюзсщвттюйшорафъцзъхрмопхртцийяр дзцонхщшртвсмлчэрдъелалъщмъшцчуоэитыесыгтсы

3.2 Дешифрування

3.2.1 Визначення довжини ключа

r	індекс
2	0.0340552
3	0.0340833
4	0.0340909
5	0.0341231
6	0.0339760
7	0.0341585
8	0.0340264
9	0.0339186
10	0.0339288

r	індекс
11	0.0340091
12	0.0340577
13	0.0340373
14	0.0340840
15	0.0342267
16	0.0340255
17	0.0555077
18	0.0338367
19	0.0339287

Очікуване значення індексу: 0.0561860, звідси робимо висновок, що довжина ключа 17.

3.2.2 Одержані ключі

Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови: **возвраaениеджинда**. Значення ключа, одержане із використанням функції $M_i(g)$: **возвращениеджинна**. Бачимо, що ключ отриманий за допогою методу частот трошки відрзняється від того, що ми отримали за допомогою функції $M_i(g)$ і на відміну від $M_i(g)$, він не має логічного значення. Тому скорегуємо його до виду: **возвращениеджинна**.

Шматок зашифрованого тексту:

жьчрдеврйкужояьхвфьчэъоъашгтмцифавицопшнюфытнижуфтмнцьрвяихыонпщотоонкязиекчхмкхеъхшефюзгютщръшуфжйыщсфюхкведбъцоффьннкцлрьокчэцо жсыиэйкррмуводнгнзоцихъынмикыпзхийеыоъйюдтбоюпмбтнцмйцивэоеофюбкзиыт хдепндетахлуойусизяцижхввщфвфартышыжщячеррхышинхатчяицюьифййвывжшчц здицяаейфзфмзщфэнййсгэыдпърдърщнъгтйсжохлпушоютйдъизтнфыунрящктсыд фрцхфпсннкууеыоъешдттпщтяиоущтюпзжикецвхншюгърсыажскянцтсхтднрчшкб тюсирйдмнфнезэчзфедещръцфчысвкстрхгзцылрдчряйсбызяъсгшэщнвхцшанзъфкб аетткцтчъымнкциэыолз

Шматок розшифрованого тексту:

радуясьвозможностиразмятьсягуръбойнаправилиськобрывуперебрасываясь шуточкамиидурачасьвнихиграланценячьяэнергиямолодостиидорофейльвовичнамгновениепо завидовалзадоруиоптимизмуюношейидевушекгодящихсяемучутьлиневовнукионтоже полюбовалсянаснежнобелыйкуполвтрехкилометрахотобрывапотомтихонько отошелотрезвящихсямолодыхлюдейипрошелсявдольобрывавглядываясьв противоположнуюстенуущельявзгляднаткнулсянарядчерныхотверстийпохожих наследыпулеметнойочередизаинтересовавшисьдорофейльвовичпрыгнулвниз ивключивантигравпересекущельеопустилсянаузкийкарнизпередсамойбольшойдыройо предупреждениигиданеотходитьдалекоотфлайтаонзабылдыраоказаласьвходомвпещеру

4 Висновок

З результатів бачимо, що в даній реалізації програми визначення символів ключа за допомогою методу $M_i(g)$ дало більш коректний результат порівняно з методом частот, що жодним чином не порушує наші теоретичні знання в межах даної задачі.