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

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

з предмету «Криптографія»

«Криптоаналіз шифру Віженера»

Виконав: Студент 3 курсу, ФТІ, групи ФБ-05 Савченко Ярослав

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, a 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).

Варіант №9

Хід роботи

Оберемо фрагмент з тексту на 2кб, що використовували в першій лабораторній.

Напишемо код, що буде шифрувати наш текст. Візьмемо декілька рядків з коду першої лабораторної роботи для роботи з файлами.

Для зручності зробимо так, щоб ми могли вказувати ключ зашифрування безпосередньо перед зашифруванням прямо в консолі.

А вот и наш эвиифрованый текст:
фезэнваниргэжмун-гіравнофт-фырунук-нькабититт-фераненфнцункцуцтфаььыхг-сбкадикцицк-зан-накуж-из-никцфан-изг-эм-цеыкцк-пеук-нькабфитит-хг-кг йеуцкаеь-бууулэмебакефас-гофтьс-гимстрыждекеруинэбт-тсиььт-эж-дируеу-чацуг-эм-уфезэнваниргэжмун-гіравнофт-фезымар-тар-пук-тек-у-ш-тар-пук-тек-у

Чудово, все працює. Зробимо це для всіх наших ключів

Лмя	Дата изменения	Тип	Размер
ab2.docx	20.01.2023 18:01	Документ Micros	204 КБ
🖟 lab2.py	20.01.2023 18:03	Python File	1 KB
text.txt	20.01.2023 17:49	Текстовый докум	3 KB
котик.txt	20.01.2023 18:04	Текстовый докум	2 KB
ктосьелвсесосиски.txt	20.01.2023 18:05	Текстовый докум	2 KE
📄 мышь.txt	20.01.2023 18:04	Текстовый докум	2 KB
📄 мяу.txt	20.01.2023 18:04	Текстовый докум	2 KB
xe.txt	20.01.2023 18:03	Текстовый докум	2 KB

наш ключик ктосьелвсесосиски и шифртекст:
йбцйпвэкврярсквшщьанюднърюдгыяляэфыдрцйтщеятсэбэчпхтк
кцреяйюнунипшшюъцйдшэтшхугкчткезьвоенъщовнтншншшкощая
ткшшбцжтпээкржуэрбуцьххяонхтугиуйкщимокгнбшрцачрйкчрфи
ьнццнъчыяннэюочяъдяцчрпъяыкжидмжбыйывжрсбубаевпяяяьы
ичъздьсщугуубпрцыутсюсэсштенчрыцхсоцыйцгьчзоцтряьиткти
ьдйрецтцюсъяцчьаещоенягнгьбцахрмаысэхшустюйцшгыцфърм
эгкхьфихкъжгнжкчкпсзцожицчрфасхъфщнюуванжюпчшыъцокърь
брмялритмешмлгукицррьтщцчюг дццхинььвриьшцаяббурхтячи
крлащцбуэмбагйжрбпифаэянкдвцсмгиивънукцбкпшеячщгяляшп
кслехэгжяаюмывшшавъэмжянвшаубтсьпшбовкыфууьсцшэхкыььф
рлхкбоуньттксряетлгмрсаялхкытьяитлицсрццятцкхыьцърршф
юыякцгнччбвлкцжяцгциягпанэбтдтвъжкицртышышыйэбсюудлху
теушаэднчуфнцрэяьяцчшпаяишшайквбххялгхаьтцяннцтякстякэбдмщостоющчсрыюдыцнруунцгуэрвшшкфухзнирвиницкотфкят
пщфяхмггшилцихтщяйегзауььчнотнмауюйуыцтюйжчялноъацзан
еюбурьтхкуьбошшавичшнтярхличсэбшэцфярмрыятяваещижтсрунньщцызушььнвгерядфцхыыьььшмшхгбунцйяхдвачйзгъщятыушия
ьървнумръйяягигшячауыкрушццгрякяогтбюяюнткщ

Також зробив запис зашифрованого тексту у файл з назвою ключа для зручності :3

Тепер для наступної задачі додамо функцію для знаходження індексу відповідності. Його також запишемо в файл

бкечэцашмнаужбмчгфгцекщнгйвуюньтхнцуакъузпеазакнекщпгфгцъюхкбакъхцзкюээхгп вкицдкайгцзнмбзккиашцнвфхйътэдяпгчгхрсъсицилщквуцааугфицзнзбжддузубфгвзубш щнзканицзевучнанвецуечитхцзуабяуанцкееабваъфгхфйянмчгьъхъмддзбщтьодужръмхъ А ещё не забудь посмотреть на индекс соответсвия: 0.041169809504074284

Порахували для кожного і побудували діаграму



Зовсім трохи, але можемо побачити що індекс зменшується з довжиною ключа. Якби ми взяли більше ключів, то побачили б спадний графік ще краще.

А також я пропустив прорахування для відкритого тексту, але швидко це виправив

A ещё не забудь посмотреть на индекс соответсвия: 0.04116980950 А тут я видимо проспал что нужно сделать: 0.06062802279022374 PS C:\CryptLab\crypto-22-23\cp2\savchenko fb-05_cp2> ■



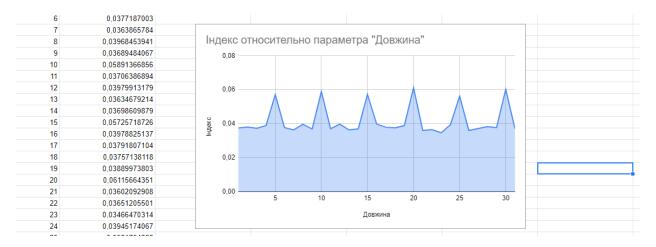
Перейдемо до найцікавішого. Розшифрування тексту за варіантом.

Збережу текст свого варіанту в файл, та створю окремий python файл для цього завдання.

Спочатку напишу функцію що порахує індекс відповідності для всіх можливих довжин ключа до 32

0.837580549447099234
Results: {1: 0.837580549447099234, 2: 0.03808314056798365, 3: 0.03738061349693251, 4: 0.038916596794556724, 5: 0.657128399337530424, 6: 0.03771870829538741, 7: 0.036386578403647986, 8: 0.83968549475766, 9: 0.036894840657126564, 10: 0.05891366856020759, 11: 0.037086893840664, 12: 0.03979913178751418, 13: 0.03634679213625582, 14: 0.036908698787341014, 15: 0.05725718725718727, 1 6: 0.039788251366120214, 17: 0.03791807103966814, 18: 0.037571381177251194, 19: 0.03889973803286497, 20: 0.06115664350846721, 21: 0.036029929082908736, 22: 0.03651205501099793, 23: 0.034664703 13988132, 24: 0.03945174067125287, 25: 0.05617543859649123, 26: 0.035987404448045704, 27: 0.03713395935618157, 28: 0.038268034486521885, 29: 0.03774432970680435, 30: 0.06021912675138483, 31: 0.03707590338674992}
PS C:\CryptLab\crypto-22-23\crypt\savchenko_fb-05_cp2> []

Тут ми бачимо що індекс досягає найбільшого значення кожні 5 довжин. Для зручності перенесу дані в таблицю і покажу графік



Тепер знаючи довжину ключа знайдемо його. Для цього створимо нову функцію що за довжиною ключа та даними з першої лабораторної роботи видаєть результати

На цьому моменті я отримав бурю емоцій адже зрозумів що весь цей час намагався знайти ключ довжини 5... Але ця довжина ключа була знайдена для одного з моїх файлів. Витративши більше 6 годин щоб це зрозуміти я врешті решт виконав частотний аналіз для потрібного шифтексту (нарешті) і отримав результат з яким працював далі



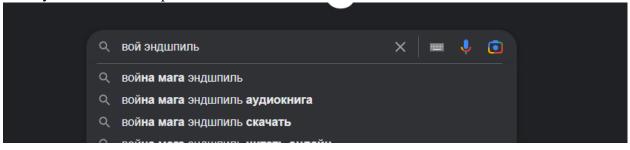
Тож довжина зашифрованого тексту – 17

Напишемо функцію для знаходження можливого схожого ключа користуючись методом з методички і знайдемо результат



Ммда... Не густо. Але в очі кинулося можливе слово "эншпиль". Почав копати під нього)

Взявши можливі слова та просто перші можливі букви та повводивши все в гуглі наткнувся на такий запрос



Роман письменника Ніка Перумова. Використаємо його як ключ для розшифровки. Допишемо функцію розшифрування і отримаємо початковий текст



"Путь старого замка на красной скале плывущей над неведомой бездной может..."

Висновок: на цій лабораторній роботі я навчився навичкам частотного криптоаналізу. Принципам шифрування, методам знаходження довжини ключа та значення самого ключа. А також навчився бути уважнішим до свого ж коду, в якому встиг не раз запутатися через один ϵ диний параметр:)