**Міністерство освіти і науки України**

**Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"**

**Фізико-технічний інститут**

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали студенти групи ФБ-23:

Кушнарьов Данііл та Присєвок Оксана

Київ - 2024

**Мета роботи:**

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

**Хід роботи:**

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.

Візьмемо очищений текст з першого практикуму alice.txt. Напишемо python скрипт для шифрування тексту

Зображення, що містить текст, знімок екрана, Шрифт, дизайн

Автоматично згенерований опис

Результат роботи скрипту

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

|  |  |
| --- | --- |
| r | Індекс відповідності |
| 0 | 0.056068885604446096 |
| 2 | 0.043673001963028306 |
| 3 | 0.039348326727504775 |
| 4 | 0.0338853889680147 |
| 5 | 0.036760750911957525 |
| 10 | 0.033915491956681615 |
| 11 | 0.03316810089075136 |
| 12 | 0.03280935328828137 |
| 13 | 0.03272622555717658 |
| 14 | 0.03264492789228932 |
| 15 | 0.03226036027642827 |
| 16 | 0.03218618448749635 |
| 17 | 0.032177411047408094 |
| 18 | 0.03222342516415893 |
| 19 | 0.03213328181400982 |
| 20 | 0.03229078873796835 |

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (варіант №6)

|  |
| --- |
| Довжина ключа / Індекс відповідності |
| 1 0,034118778  2 0,034127473  3 0,034079877  4 0,034284242  5 0,034114456  6 0,034037503  7 0,034044451  8 0,03425015  9 0,033998649  10 0,034098788  11 0,034048149  12 0,034253687  13 0,034178657  14 0,033986747  15 0,034080398  16 0,03410148  17 0,043720818  18 0,034062751  19 0,033768531  20 0,034107807  21 0,034049948  22 0,03427517  23 0,034291115  24 0,034227532  25 0,033864516  26 0,03431543  27 0,03425323  28 0,034265209  29 0,034144543  30 0,033832304 |

Зображення, що містить текст, Графік, ряд, схема

Автоматично згенерований опис

Аналізуючи графік та таблицю бачимо значення, яке схиляється до теоретичного значення І для заданої мови. Саме це значення найбільше вирізняється поміж інших порівняно із значенням індексу, що відповідає мові з рівноймовірним алфавітом. Тому в нашому випадку, довжина ключа буде 17.

Шифртекст згідно з варіантом: жьчрдеврйкужояьхвфьчэъоъашгтмцифавицопшнюфытнижуфтмнцьрвяихыонпщотоонкязиекчхмкхеъхшефюзгютщрьшуфжйыщсфюхкведбъцооффьннкцлрьокчэцожыиэйкррмуводнгнзоцихъынмикыпзхийеыоъйюдтбоюпмбтнцмйцивэоеофюбкзиытхдепндетахлуойусизяцижхввщфвфартыфшыжщячеррхышинхатчяицюьифййвывжшчцздицяаейфзфмзщфэнййсгэыдпьрдърщнъгтйсжохлпушоютйдъизтнфыунрящктсыдфрцхфпсннкууеыоъешдттпщтяиоущтюпзжикецвхншюгьрсыажкянцтсхтднрчшкбтюсирйдмнфнезэчзфедещрьцфчысвкстрхгзцылрдчряйсбызяъсгшэщнвхцшанзьфкбаетткцтчъымнкциэыолзтънцвктэобафрбыьхнунхицлэонкчвбсгефгйфщптцхдошфрвснвщдхицхщисбщзиекчпрдрораъееьййлгйешцрвзцьитуайряоксыъхйшдполкхпщвояккъуцжтытссбщпшцщмтфрмфтыяотьрфркетылузфкыэяфтмфшвжшчрницыфйямосглтзтхйапфиаяррълдрдпеядчфлъйтгртммрбйднтпчцияпнвезнюсыдяцпифшыбелщгдювбьпъенуныярртфэеиърхппмычыфврыпнтбчхыепхрыэюиляхнэертысцмчътщыйоцкэашцйцжюещъхлщукреоркярзцфъутдзыгуяоеуждгрлъэыдрпчвысшйыифтсуыътвбфвуойуситдсыътофшъжрдзрухеебунъащощюбяцпютшфчрмьоуоуэькйеюрзятрфнгвтхщэыестщчдтщьатпцээчеерхифтсуыътвбфтрсиушиидсщмъатойпшнюсышдххцчыйуайкпнюйнукофцяфнвъмпштзооцхтнмищаушмнрйжфыэуклсъникхйкыикчынхччуыэемцпохнжуфмкхвтырдвахдъожытмздкюняоеьйзъакупнхьоуьысвтсхрмюххтесчтхцпкщхфшрмкщгоофшнолюоцрылзтымнсуисгафкзфючжктнитхцюндрефэщмзйаубйчътютдуфпюэгцчыххжхянмйофкьаыэхфпдзръаддолшртбстщчсфлыккушътбизтъцитъунцтвяфвзадеьцпднишхпвъжфэигеьцрпфхаыдкыфвфцщчйчнфжфхсукхтхэнзиыйелжуйяауэхурдзьъцоусияботъхлшаекэрпдущчхмцщзеюмщмнъкръунц

Розшифрований текст (ключем возвращениеджинна): дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяпрожилужебольшешестидесятилетработалпрорабомстроительнойкомпаниидомостройвхарьковестолицевкраинылюбилпорыбачитьсдрузьяминаозерахроганьскогокраязачертойгородавыращивалнадачномучасткеовощиифруктывоспитывалвнуковавотуезжатьзапределыроднойвкраинынелюбилнесмотрянавозможностивсвязиссозданиемглобальнойсетиметропобыватьналюбойпланетесолнечнойсистемыидажезаеепределамичтоподвиглоегосогласитьсянаэкскурсиюполунеонисамневсостояниибылответитьвероятносыгралисвоюрольрассказыдрузейхваставшихсясвоимипутешествиямииунеговзыгралолюбопытствопосмотретьвблизичтожеэтотакоеспутницаземлиокоторойтакмногоговорятдетивнукиидрузьякакбытонибылоаутромдвадцатьтретьегодекабряаккуратвначалосвятокдорофейльвовичвтайнеотродныхиблизкихпозвонилвбюроэкскурсийсолнечнойсистемызапинаясьобъяснилчегохочетивтотжеденьспомощьюметродобралсядоаполлонтаунагороданалунеоткудадолжнабыланачатьсяэкскурсияпосамымкрасивымизагадочнымместамспутницыземлиаполлонтаунрасполагалсянаравнинеморяспокойствиянедалекоотзнаменитойбороздымаскелайнпохожейнаиизвилистоеруслорекиименноздеськогдатовконцедвадцатоговекасовершилпосадкуамериканскийпилотируемыйкорабльаполлонодиннадцатьаточнееегопосадочныймодульестественноэкскурсантамзанимавшимкабинудвадцатиместногоэкскурсионногофлайтасначалапоказалипамятникаполлонуодиннадцатьпирамидуизлунногобазальтаспосадочнойплатформойиамериканскимфлагомазатемфлайтотправилсявпутешествиепоморюспокойствиязалитомуяркимсолнечнымсветомэкскурсантамиоказалисьмолоды