Криптоаналіз афінної біграмної підстановки

Варіант 6

1 Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

1.1 Дешифрування

1.1.1 Найчастіші біграми шифротексту

Найчастішими біграма в заданому шифротексті виявились ось такі: ['цл', 'ял', 'ае', 'ле', 'чо'], звідси зрозуміло, що текст не є змістовним, бо такі біграми в ньому не зустрічались би.

1.2 Генерація ключів

Рахуємо найчастіші біграми шифротексту і беремо найчастіші біграми мови, конвертуємо їх в числові значення, розв'язуємо систему, це все бахується на тому на такому факті: афінний шифр зберігає статистичні властивості мови, пов'язані із частотами біграм, маємо потенційні a та b. Далі для кожного з них, дешифруємо вхідний зашифрований текст, і перевіряємо його на змістовність.

1.2.1 Критерій змістовності тексту

Як ми це робимо, рахуємо частоти усіх символів розшифрованого тексту, тут у нас є ось цей ranksize - те скільки найчастіших і найрідших символів ми беремо, потім перевіряємо чи мають ці top і bottom chars найпопулярніші і найрідші символи мови відповідно, ну і відповідно регуляємо оцінку, якщо вони є або немає, потім також перевіряємо індекс відповідності.

1.3 Результати

Шматок зашифрованого тексту:

*йжтаеэщащбаеыбзэхечоетульйсулцтюаъебхсмжзаюэфйжлнэцтклиувь зэлцюедкйетлофгбйбфлаэжугосрчусфашолыьзатййуыйвичъдмэбдцялшаиуошул обяфъбацкфщмюэзыкюцкфлеисядыфрцксчоюйрлщегмююзаяййугугфклиуулиулц оюфюхевюфйвеаесачсчопчцлхулбщлербноулехебрбнняллйжшбцвбошьййшктгбаз ошоффйжлнэеэажкюмиуэфщшцюйюэщйщлгшеэыэнзрцшцчлвгйтхйщлхэзывгмжуэбо аанафщлйрзажбщйрмфллжлпфцлуичьтфшцюйлфгййшцлпаюеюэбцзазяйрлцфунбсф хаечыэнзхоцжсаыитсольймйсфолкцулхзобнцзеасвеелгйхъечццщюхеъащмцжбщ юйзлъйщбфлбиоптиилвбцьдмэбьтофлйжлмллакнцлцщебдасццййфлципрулхноц ълцлеузбзитснозэымновцлфцлчеебшуустиофоббэжфллгувешцщлрэелещянхеза вцлэяйжлгйюйулэйбэымнлещянхекскеаелеыизаьтвбшабцллйшгбцьдмэбтыпаль аозаопкечодпебцфилхнзаююагаечявафщцжчъфщжйфллекюдтрййувьцлйубисасм хешщиежцьюцжяацдэйщебфьлщвъопцлсяпаусхлдцисаетййбиююаъюеэропебчэ фюжлвлмфчлхмтивьтеаехйшйжштйийвьцлаешифюыэтйшйхуъсоцялшащбнфвллло щ

Шматок розшифрованого тексту:

*атызнаешьсколькоразмывэтомгодуиграливбейсболавпрошломавпоза прошломнистогониссегоспросилтомгубыегодвигалисьбыстробыстроявсезапи салтысячпятьсотшестьдесятвосемьразасколькоразячистилзубызадесятьлет жизнишестьтысячразарукимылпятнадцатьтысячразспалчетыреслишнимтысячи разиэтотольконочьюиселшестьсотперсиковивосемьсотяблокагрушвсегодвес тиянеоченьтолюблюгрушичтохочешьспросиуменявсезаписаноесливспомнитьи сосчитатьчтояделалзавседесятьлетпрямотысячимиллионовполучаютсяватво тдумалдугласопятьоноближепочемупотомучтотомболтаетноразведеловтомео нвсетрещititрещitсполнымртомотецсидитмолчанасторожилсякакрысьатомвс еболтаетникакнеугомонитсяшипитипенитсякаксифонссодовойкнигяпрочелче тыресташтуккиносмотрелитогобольшесорокфильмовсучастиембакаджонсатридцатьсджекомхоксисорокпятьстомоммиксомтридцатьдевятьсхутомгибсономс тодевяностодвамультипликационныхпрокотафеликсадесятьсдуглассомфербен

2 Висновок

В результаті роботи програми, вдалось успішно дешифрувати вхідний текст, а тому обраний кретерій змістовності тексту є коректним, та його можна в подальшому використовувати.