

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Мета роботи

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

Спочатку я зашифровала свій текст з ключами: на, сон, боль, проза, криптография.

Це було не складно. Для кожної букви рахуємо $(x+k) \bmod 32$.

Для кожного с зашифрованих мною текстів порахувала індекс відповідності. Ось що отримала (перші 100 символів зашифрованого тексту і індекс):

Ключ на:

чоуаолынсиъачафашаюъетсеюутпеъныбтлыйынсапныпычяиъееепешишсмапиюешесвнзнмттъопд
ихняаяуешыцзнтвлйпо

0.043019260966245004

Ключ сон:

ыъуспшяысщыныофщнвкъцуюгуюгртюыытушычыютнуыыаьдгъцъжтуушщюропщятыусуофсътгыы
утижомгнуцщиъхнггшмчпя

0.04387859233003945

Ключ боль:

льсьвщщйецшьлотъмощоурнууьогушйппрзпщйеонйпэщууцшбщунбмццнаондтуцберлгбърооьна
ьглыунсбмйфгбаазьчнк

0.03792884601648464

Ключ проза:

щюфзбъюылирьшззпыошьхуштфбайеъьиъеъючхнуррфоююешиъхжмвфыцтсоррпсфыулвпчоубъ
йдкеожтоцутышчощхълчйо

0.03529669546034166

Ключ криптография:

фюопущсэдьхяфрппэофмнщнръхщбфурэохнкшщцьцоезогццьшхфкуехльурйркчгуохдцижкьнбьяеф
ыйиюьпофэймчажэкещкэ

0.03298084793215981

Далі порахуємо індекс відповідності для зашифрованого тексту:

0.032821177802678465

Також при діллені на різні r блоки:

2 :0.03432921421542369

3 :0.03734839112182639
4 :0.03846786795894798
5 :0.032753684507439526
6 :0.04242249836150345
7 :0.032845671625834745
8 :0.038394305262087654
9 :0.037406913486166676
10 :0.034343106655826135
11 :0.03282596004503103
12 :0.05436955673586635
13 :0.032807635112857336
14 :0.034253133094361496
15 :0.03741441107403287
16 :0.03846816039387033
17 :0.0326076877752591
18 :0.042619239781400246
19 :0.03299852287693898
20 :0.03839407833306634
21 :0.03734596917614833
22 :0.03436346417856434
23 :0.03248823743567128
24 :0.05435416649918132
25 :0.032517536103743
26 :0.03434857665414954
27 :0.03762500312229972
28 :0.0383860390427654
29 :0.033132183908045974
30 :0.04250450051229374

За першим методом пошуку довжини ключа бачимо, що найближче до 0,55 є 12 та 24 довжина ключа, а за другим методом 0.032821177802678465 приблизно дорівнює 0.03298084793215981 тобто тексту зашифрованому ключам довжиною 12.

Тож ми знайшли довзину ключа: 12

Тож ділемо текст на 12 блоків і знаходимо частоти літер. Потім замінюємо на літери з такими самими частотами з відкритого тексту. Отримуємо щось таке:

кегиидужштеттцнаконбоконоуынанрортнлнкясжртделныгаебопсатдсоиперобагонлучдербозкимар
илаьеаеоатоемоьрелнеьедонаояежкаттвйтзрлереувуттлаиговзесцогиирофесыина

Це ще не дуже схоже на розшифрований текст, але ми уявимо що ключ довжиною в текст і маючи зашифрований та псевдо-розшифрований текст знайдемо ключ. Поділемо ключ на частини по 12 літер і знайдемо найчастіше зустрічаємую літеру для 1,2 ... ,12 літеру цих частин.

Отримаємо щось таке:

ьшлуыниивйрш
шшшкпцибурв
вржкцвзрьхф
вярбфрыньща
юеемсбзрбюпя
лшексхичбутз
фчекжпдтбть
лчнчмьхройря
щшккмцирмоця
веетмюарбйро
шъчкмрхщбмжш
чеоссщдрауря
лвчбспзщбурь
ьяскипзрьгтя
чшекмцирзуря
вчексвпрзэрв
цъцбрцияущря
і т.д

Найчастіші літери:

в ш е к с п и р б у р я

Отримали ключ: вшекспирбурия

Тепер спробуємо розшифрувати текст:

действующилицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланс
кийантониоегобр...

Це вже схоже на відкритий текст.

Висновок: навчилась завдяки частотному аналізу розшифровувати тексти заковані шифром Віженера.