Протокол лабораторної роботи №2

Криптоаналіз шифру Віженера

Варіант 7

Виконав

Студент 3 курсу

Групи ФБ-13

Короткевич Іван

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

Всі зашифровані тексти наведені в окремому файлі

Індекси відповідності для відкритого та зашифрованого тексту:

Index for open text: 0.05137110644981255

Index for key 2: 0.037343640750814866

Index for key 3: 0.03707599645630655

Index for key 4: 0.03585914855918155

Index for key 5: 0.03626372714390341

Index for key 10: 0.03238184749254642

Index for key 11: 0.03255612749827276

Index for key 12: 0.033470060147349594

Index for key 13: 0.033658863486886466

Index for key 14: 0.03283103345968634

Index for key 15: 0.03289016417591492

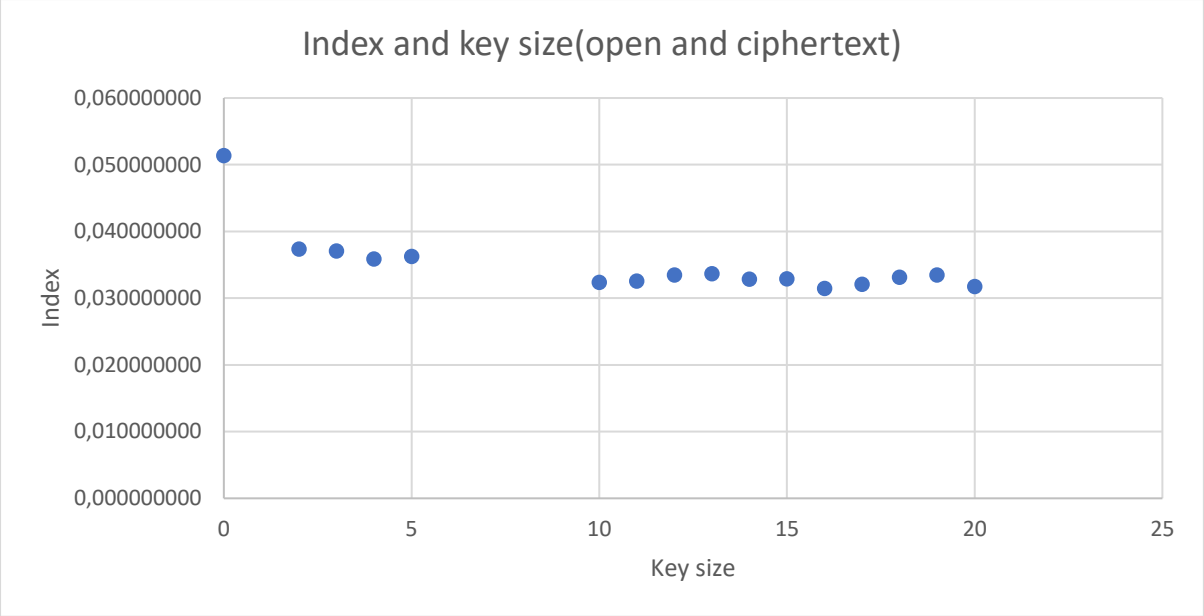
Index for key 16: 0.03145857841459138

Index for key 17: 0.032057147243782454

Index for key 18: 0.033145359898585636

Index for key 19: 0.033480433957214256

Index for key 20: 0.03175008247178843



Розмір ключа був знайдений за допомогою індексу відповідності. Індекси відповідності для різних ключей:

Index of key size 2: 0.03385388813744475

Index of key size 3: 0.03615187096897406

Index of key size 4: 0.03374293361807624

Index of key size 5: 0.03952084806368013

Index of key size 6: 0.036125055880893396

Index of key size 7: 0.033821792020889335

Index of key size 8: 0.03374094496535137

Index of key size 9: 0.03608280586815858

Index of key size 10: 0.03952252784858045

Index of key size 11: 0.033676545852495285

Index of key size 12: 0.03604485666071514

Index of key size 13: 0.03357519915761071

Index of key size 14: 0.03392455396612264

Index of key size 15: 0.05605177331202787

Index of key size 16: 0.03368328831902167

Index of key size 17: 0.03368867351961501

Index of key size 18: 0.03608986458957075

Index of key size 19: 0.0335364228338296

Index of key size 20: 0.03938936497846169

Index of key size 21: 0.03619388229715766

Index of key size 22: 0.03359466427790614

Index of key size 23: 0.03408654267171319

Index of key size 24: 0.03608759248034323

Index of key size 25: 0.03901716563504428

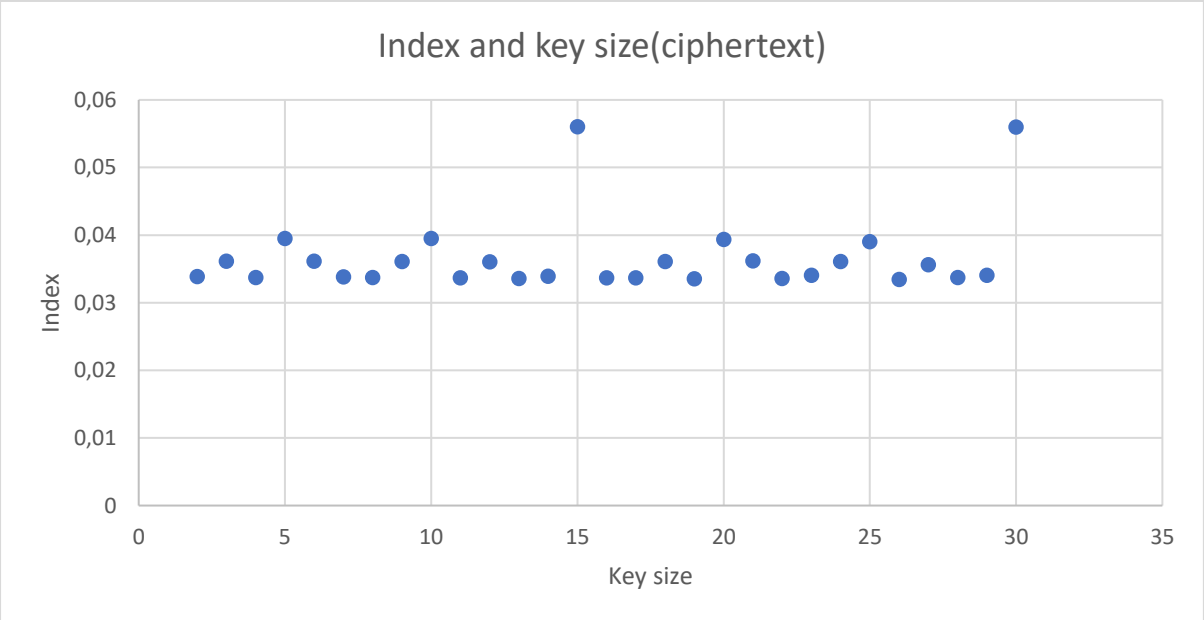
Index of key size 26: 0.03346893581656819

Index of key size 27: 0.03564037880738555

Index of key size 28: 0.033727646862663656

Index of key size 29: 0.03404426010285956

Index of key size 30: 0.05600313156972977



Як видно, довжина ключа 15 символів
Далі вибираємо з кожного блоку шифротексту найчастішу букву і від кожної букви віднімаємо порядковий номер букви “о”. Отримаємо ключ: арудазевархимаг

Після використання цього ключа отримаємо відкритий текст:
прошлошятнадцатьднейиътарыйдомпостепонноначаложивате

Але, як видно є неточності. Для виправлення замінемо 7 букву на “о”. Отрмаємо:
прошлопятнадцатьднейистарыйдомпостепенноначаложивать