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

«Криптографія»

Комп’ютерний практикум

№ 3

Виконав:
студент групи **ФБ-83**
Гах Валерій

Перевірив:
_____

Київ 2020

Назва: Криптоаналіз афінної біграмної підстановки;
Мета роботи: Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці;
Постановка задачі:
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифротексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ шляхом розв'язання системи рівнянь.
4. Для кожного кандидата на ключ дешифрувати шифротекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.
Варіант: 6(номер у списку групи), номер бригади відсутній(робота виконана самостійно);

Характеристики обладнання:

- Ноутбук - Lenovo G510;
- ОС - Windows 10 Home x64;
- Процесор - Intel Core i5-4200M, CPU - 2.5GHz;
- Тип системи: 64-розрядна ОС, процесор x64;
- ОЗУ - 6.00 ГБ;

Хід роботи:
Програмний код-реалізацію криптоаналізу було написано мовою python. При цьому окремі функції шифрування-дешифрування, математичні операції(НСД, визначення оберненого за модулем, та вирішення системи двох лінійних модулярних рівнянь) та функції роботи з алфавітом винесено в окремі файли - `Alphabet_and_funcs.py` – функції та словники, що реалізують роботу з російським алфавітом не використовуючи кодування файлів («ё» замінена на «е», «ъ» - на «ь» для сумісності з шифротекстами в завданні практичної роботи. `Affine_cipher.py` – файл з функціями шифрування/дешифрування аффіного шифру. `Math_operations.py` – код функцій, що реалізують математичні операції, необхідні для шифрування/розшифрування та криптоаналізу(співставлення біграм та знаходження ключа) афінного шифру. `main_cryptoanalysis.py` – код, що виконує сам криптоаналіз шифротексту мого варіанту та виводить результати автоматизованого частотного аналізу. Зміни та доробки в розшифрування(як наприклад вгадування літер там, де автоматизований частотний аналіз розшифрував тест неправильно) проводяться шляхом додавання в кінець цього коду нових, необхідних саме для поточного аналізу, маніпуляцій з ключем.
Результати:
Спочатку було реалізовано та протестовано функції математичних операцій – обчислення НСД двох цілих чисел та знаходження оберненого для заданого числа заданому модулю. Некоректні вхідні дані(обчслення оберненого за модулем для чисел, НСД яких не 1, і т.д.) враховано(функції повертають None). Лінійні рівняння та їх системи реалізовані, як класи – з методами виводу знайомого зовнішнього їх вигляду та методом обчислення кореня рівняння/системи рівнянь. Цей корінь – завжди масив значень(для одного рівняння – масив чисел, для систем рівнянь – масив пар чисел). Так враховується можливість отримання декількох ключів із узятого одного співставлення пар біграм. Далі було написано код кодування біграм у цілі числа за формулою $X = m*X_1 + X_2$ та шифрування афінним шифром: $Y = (a*X + b) \bmod m^2$, де (a, b) – ключ ($НСД(a, m2)=1$). Також реалізований код зворотньої функціональності – декодування числа у відповідну йому біграму: $Y_1 = Y/m;\ Y_2 = Y\%m$. Та розшифрування: $X = a^{-1}(Y - b) \bmod m^2$. Далі потрібно було реалізувати підрахунок частот появи біграмм для тексту російською мовою(функція фільтрування тексту була узята з лабораторної роботи 2). Для шифротексту мого варіанту було знайдено такі кількості появ біграмм(вже відсортовано в порядку спадання):

ЩЕ : 46	ЛП : 31	ЭИ : 24	ЬХ : 21	СЬ : 18	ША : 16	ЦЫ : 13	ЯЩ : 11	БД : 11	ШЗ : 9	ЫЩ : 8	УС : 7	ДШ : 7	ЦЮ : 6	ВЛ : 6
ХЕ : 44	ЭЩ : 30	РД : 24	ШУ : 21	ИЭ : 18	ЦА : 16	ЗА : 13	ЮЗ : 11	ЭЗ : 10	ШВ : 9	ШГ : 8	СШ : 7	ГЩ : 7	ЦД : 6	БЮ : 6
ЧВ : 42	ЭА : 30	ЙЭ : 24	ТВ : 21	ЕП : 18	ХЩ : 16	ЕГ : 13	ЩХ : 11	ЩЩ : 10	ЦЭ : 9	ЦИ : 8	СЕ : 7	ГО : 7	ФУ : 6	ЯЬ : 5
ЛЕ : 40	ЯХ : 29	ЗЬ : 24	ПП : 21	ЩЦ : 17	ФЕ : 16	БЩ : 13	ЧИ : 11	УД : 10	ХТ : 9	ХА : 8	РЯ : 7	АД : 7	ФТ : 6	ЯТ : 5
ЦВ : 38	ЩА : 29	ЗЕ : 24	МО : 21	ФГ : 17	ПЕ : 16	ЮЭ : 12	ЦУ : 11	ТЬ : 10	УЦ : 9	УН : 8	РА : 7	ЯД : 6	ФМ : 6	ЮЧ : 5
ОЩ : 37	ХД : 29	ЯЙ : 23	МА : 21	УБ : 17	ЖП : 16	РЙ : 12	ФЙ : 11	ТЕ : 10	КУ : 9	ЛВ : 8	ПХ : 7	ЮИ : 6	СУ : 6	ЮО : 5
СД : 36	НЕ : 29	ЮЦ : 23	ГЬ : 21	РП : 17	ВИ : 16	НЩ : 12	СБ : 11	РТ : 10	ЙО : 9	ЗЛ : 8	ПН : 7	ЭЭ : 6	ОВ : 6	ЬЮ : 5
ЖЕ : 36	ЛО : 29	ЭЬ : 23	БО : 21	ЛМ : 17	ЭШ : 15	МЬ : 12	КЮ : 11	НЭ : 10	ЗЧ : 9	ДЮ : 8	ОЮ : 7	ЭУ : 6	КО : 6	РО : 5
ДЕ : 36	ЙЫ : 28	ИА : 23	ДЭ : 20	КМ : 17	ЫВ : 15	МВ : 12	КТ : 11	ИД : 10	ЖИ : 9	ГЮ : 8	НД : 7	ЭЕ : 6	КН : 6	РЕ : 5
ГД : 34	АЕ : 28	ЮА : 22	ВЮ : 20	ИЮ : 17	ЗЩ : 15	ЖЮ : 12	ЙЙ : 11	ЖМ : 10	ЖГ : 9	ЫЙ : 7	ЛЛ : 7	ЬД : 6	ИЙ : 6	ПМ : 5
НЮ : 33	ИЬ : 27	ФП : 22	ОЕ : 19	ЗД : 17	ВЫ : 15	ЕЬ : 12	ЗО : 11	ЕЩ : 10	ЕА : 9	ЫЖ : 7	КИ : 7	ШЩ : 6	ЖЙ : 6	ПД : 5
НВ : 33	ЯЦ : 25	ТА : 22	ОД : 19	БА : 17	БЖ : 15	ВО : 12	БП : 11	ЯЮ : 9	ЯИ : 8	ЩД : 7	ЖЯ : 7	ШИ : 6	ЕЮ : 6	ОП : 5
МЮ : 32	ТЩ : 25	ВД : 22	ЩУ : 18	ЮЙ : 16	БУ : 14	АМ : 12	БМ : 11	ЭВ : 9	ЫЬ : 8	ХИ : 7	ЕЫ : 7	ЧЙ : 6	ВШ : 6	НН : 5

МИ : 5	ДЫ : 4	ДУ : 3	ИМ : 2	ЦО : 1	ЙП : 1	ЯА : 0	ЫЧ : 0	ЧШ : 0	ФЛ : 0	РЧ : 0	НУ : 0	КФ : 0	ЖФ : 0	ГЗ : 0
ИО : 5	ДЩ : 4	ГЧ : 3	ИИ : 2	ЦЙ : 1	ЙН : 1	ЮЯ : 0	ЫЦ : 0	ЧЦ : 0	ФК : 0	РХ : 0	НТ : 0	КС : 0	ЖТ : 0	ГЖ : 0
ЗЭ : 5	ДН : 4	ВЧ : 3	ИЗ : 2	ЦЗ : 1	ЙМ : 1	ЮЫ : 0	ЫХ : 0	ЧФ : 0	ФД : 0	РФ : 0	НС : 0	КР : 0	ЖС : 0	ГГ : 0
ЖЬ : 5	ГЦ : 4	ВА : 3	ЗЮ : 2	ХЮ : 1	ЙД : 1	ЮХ : 0	ЫФ : 0	ЧТ : 0	ФБ : 0	РУ : 0	НР : 0	КП : 0	ЖР : 0	ГВ : 0
ЖД : 5	ГЙ : 4	АШ : 3	ЗЙ : 2	ХУ : 1	ИХ : 1	ЮТ : 0	ЫТ : 0	ЧС : 0	ФА : 0	РС : 0	НО : 0	КЛ : 0	ЖК : 0	ГБ : 0
ДП : 5	ЯЭ : 3	ЯМ : 2	ЖУ : 2	ХЙ : 1	ИТ : 1	ЮС : 0	ЫС : 0	ЧО : 0	УЯ : 0	РР : 0	НМ : 0	КК : 0	ЖЗ : 0	ГА : 0
БЧ : 5	ЯШ : 3	ЯЛ : 2	ЖО : 2	ХГ : 1	ИР : 1	ЮР : 0	ЫР : 0	ЧН : 0	УЬ : 0	РН : 0	НЛ : 0	КЙ : 0	ЖЖ : 0	ВЯ : 0
БИ : 5	ЯО : 3	ЮФ : 2	ЖЛ : 2	ФЫ : 1	ИК : 1	ЮН : 0	ЫП : 0	ЧЛ : 0	УШ : 0	РМ : 0	НК : 0	КБ : 0	ЖБ : 0	ВЦ : 0
ББ : 5	ЯВ : 3	ЮП : 2	ЖВ : 2	ФЩ : 1	ИЕ : 1	ЮМ : 0	ЫО : 0	ЧК : 0	УЧ : 0	РЛ : 0	НИ : 0	КА : 0	ЖА : 0	ВХ : 0
АЮ : 5	ЮЖ : 3	ЬВ : 2	ЕХ : 2	ФИ : 1	ЗХ : 1	ЮЛ : 0	ЫН : 0	ЧЗ : 0	УХ : 0	РК : 0	НЗ : 0	ЙЬ : 0	ЕЯ : 0	ВУ : 0
АО : 5	ЬЭ : 3	ЫЛ : 2	ЕО : 2	ФЗ : 1	ЗТ : 1	ЮК : 0	ЫМ : 0	ЧЖ : 0	УФ : 0	РЗ : 0	НБ : 0	ЙЩ : 0	ЕШ : 0	ВТ : 0
АЖ : 5	ЬЬ : 3	ЫЗ : 2	ЕЙ : 2	УЫ : 1	ЗС : 1	ЮЕ : 0	ЫК : 0	ЧД : 0	УУ : 0	РЖ : 0	НА : 0	ЙЧ : 0	ЕЧ : 0	ВС : 0
АА : 5	ЬЩ : 3	ЩЮ : 2	ЕЕ : 2	УТ : 1	ЗН : 1	ЮД : 0	ЫГ : 0	ЧГ : 0	УР : 0	РГ : 0	МЭ : 0	ЙХ : 0	ЕЦ : 0	ВР : 0
ЯЕ : 4	ЬЦ : 3	ШН : 2	ДО : 2	УЗ : 1	ЗМ : 1	ЮВ : 0	ЫБ : 0	ЧБ : 0	УО : 0	РБ : 0	МЫ : 0	ЙФ : 0	ЕФ : 0	ВН : 0
ЮЮ : 4	ЬП : 3	ШЙ : 2	ДМ : 2	УА : 1	ЗЗ : 1	ЮБ : 0	ЫА : 0	ЦЯ : 0	УМ : 0	ПЯ : 0	МШ : 0	ЙУ : 0	ЕТ : 0	ВК : 0
ЮЬ : 4	ЫУ : 3	ШЕ : 2	ДВ : 2	ТФ : 1	ЗБ : 1	ЭЯ : 0	ЩЯ : 0	ЦШ : 0	УЛ : 0	ПЬ : 0	МЧ : 0	ЙС : 0	ЕС : 0	ВЙ : 0
ЮУ : 4	ЩЬ : 3	ЧУ : 2	ГС : 2	ТЗ : 1	ЖШ : 1	ЭЮ : 0	ЩЫ : 0	ЦФ : 0	УК : 0	ПЫ : 0	МФ : 0	ЙР : 0	ЕР : 0	ВЖ : 0
ЮГ : 4	ЩО : 3	ЦЬ : 2	ГИ : 2	ТЖ : 1	ЖН : 1	ЭЫ : 0	ЩШ : 0	ЦТ : 0	УЖ : 0	ПЩ : 0	МУ : 0	ЙЛ : 0	ЕН : 0	ВЕ : 0
ЭФ : 4	ЧЮ : 3	ЦЖ : 2	ВЭ : 2	СЧ : 1	ЕУ : 1	ЭЧ : 0	ЩЧ : 0	ЦС : 0	ТЯ : 0	ПШ : 0	МС : 0	ЙК : 0	ЕЛ : 0	ВГ : 0
ЭМ : 4	ЧМ : 3	ХЭ : 2	ВЩ : 2	СЦ : 1	ЕМ : 1	ЭХ : 0	ЩФ : 0	ЦР : 0	ТЮ : 0	ПЧ : 0	МР : 0	ЙИ : 0	ЕЗ : 0	ВБ : 0
ЫЮ : 4	ЧА : 3	ХЫ : 2	ВМ : 2	СХ : 1	ЕК : 1	ЭТ : 0	ЩС : 0	ЦП : 0	ТЫ : 0	ПЦ : 0	МН : 0	ЙЗ : 0	ЕВ : 0	БЯ : 0
ЫД : 4	ХО : 3	ХХ : 2	ВЗ : 2	СЛ : 1	ЕИ : 1	ЭР : 0	ЩР : 0	ЦН : 0	ТШ : 0	ПФ : 0	ММ : 0	ЙЖ : 0	ЕБ : 0	БЭ : 0
ЩЭ : 4	ХМ : 3	ФЦ : 2	БЗ : 2	СВ : 1	ЕД : 1	ЭП : 0	ЩН : 0	ЦМ : 0	ТЧ : 0	ПТ : 0	МЛ : 0	ЙЕ : 0	ДЯ : 0	БЬ : 0
ЩП : 4	ХЖ : 3	УП : 2	АЭ : 2	РШ : 1	ДА : 1	ЭО : 0	ЩМ : 0	ЦЛ : 0	ТХ : 0	ПР : 0	МК : 0	ЙБ : 0	ДЧ : 0	БЫ : 0
ШШ : 4	ФЮ : 3	УИ : 2	АЬ : 2	РЦ : 1	ГУ : 1	ЭН : 0	ЩЛ : 0	ЦК : 0	ТУ : 0	ПО : 0	МЗ : 0	ИЫ : 0	ДЦ : 0	БШ : 0
ШД : 4	ФЖ : 3	УЕ : 2	АИ : 2	РИ : 1	ГП : 1	ЭЛ : 0	ЩК : 0	ЦЕ : 0	ТС : 0	ПЛ : 0	МЕ : 0	ИШ : 0	ДХ : 0	БХ : 0
ЧЩ : 4	ФВ : 3	УГ : 2	ЮЩ : 1	ПУ : 1	ГЕ : 1	ЭК : 0	ЩЖ : 0	ЦГ : 0	ТР : 0	ПК : 0	МД : 0	ИЧ : 0	ДФ : 0	БФ : 0
ЧЧ : 4	УЭ : 3	ТТ : 2	ЮШ : 1	ПВ : 1	ВЬ : 1	ЭЙ : 0	ЩГ : 0	ЦБ : 0	ТО : 0	ПЖ : 0	МГ : 0	ИФ : 0	ДТ : 0	БТ : 0
ЧП : 4	УЙ : 3	ТИ : 2	ЭЦ : 1	ПА : 1	ВФ : 1	ЭД : 0	ЩВ : 0	ХЯ : 0	ТН : 0	ПГ : 0	МБ : 0	ИУ : 0	ДС : 0	БС : 0
ЧЕ : 4	ТЭ : 3	СФ : 2	ЭС : 1	ОХ : 1	ВП : 1	ЭГ : 0	ЩБ : 0	ХЬ : 0	ТМ : 0	ПБ : 0	ЛЯ : 0	ИС : 0	ДР : 0	БР : 0
ХШ : 4	ТЦ : 3	СЗ : 2	ЭЖ : 1	ОТ : 1	ВВ : 1	ЭБ : 0	ШЯ : 0	ХЧ : 0	ТЛ : 0	ОЯ : 0	ЛЭ : 0	ИП : 0	ДЛ : 0	БЛ : 0
ХЦ : 4	ТП : 3	ПС : 2	ЬЫ : 1	ОМ : 1	БЦ : 1	ЬЯ : 0	ШЮ : 0	ХФ : 0	ТК : 0	ОЭ : 0	ЛЫ : 0	ИН : 0	ДК : 0	БК : 0
ХВ : 4	СЮ : 3	ПЗ : 2	ЬЛ : 1	ОЙ : 1	БН : 1	ЬШ : 0	ШЭ : 0	ХС : 0	ТЙ : 0	ОЬ : 0	ЛШ : 0	ИЛ : 0	ДЙ : 0	БГ : 0
УЮ : 4	СЩ : 3	ОШ : 2	ЬЙ : 1	ОИ : 1	БЙ : 1	ЬЧ : 0	ШЬ : 0	ХР : 0	ТГ : 0	ОЫ : 0	ЛЧ : 0	ИГ : 0	ДИ : 0	ББ : 0
УЩ : 4	СТ : 3	ОУ : 2	ЬЗ : 1	НЫ : 1	БЕ : 1	ЬФ : 0	ШЫ : 0	ХП : 0	СЯ : 0	ОЧ : 0	ЛЦ : 0	ИВ : 0	ДЗ : 0	АЯ : 0
УВ : 4	СГ : 3	ОА : 2	ЬЖ : 1	НЖ : 1	АТ : 1	ЬУ : 0	ШЧ : 0	ХН : 0	СЭ : 0	ОЦ : 0	ЛФ : 0	ЗЯ : 0	ДЖ : 0	АЫ : 0
ТД : 4	СА : 3	НХ : 2	ЬЕ : 1	МЯ : 1	АК : 1	ЬТ : 0	ШЩ : 0	ХЛ : 0	СЫ : 0	ОФ : 0	ЛС : 0	ЗЫ : 0	ДД : 0	АЩ : 0
ТБ : 4	РЮ : 3	НП : 2	ЫИ : 1	МХ : 1	ЯЯ : 0	ЬС : 0	ШХ : 0	ХК : 0	СС : 0	ОС : 0	ЛР : 0	ЗЦ : 0	ДГ : 0	АЧ : 0
ПЭ : 4	РВ : 3	НГ : 2	ЫЕ : 1	МЙ : 1	ЯЫ : 0	ЬР : 0	ШФ : 0	ХЗ : 0	СР : 0	ОР : 0	ЛН : 0	ЗФ : 0	ДБ : 0	АЦ : 0
ПЙ : 4	ПЮ : 3	МЦ : 2	ЩТ : 1	МЖ : 1	ЯЧ : 0	ЬО : 0	ШТ : 0	ХБ : 0	СП : 0	ОО : 0	ЛК : 0	ЗУ : 0	ГЯ : 0	АХ : 0
ОБ : 4	ПИ : 3	МП : 2	ЩЙ : 1	ЛЮ : 1	ЯФ : 0	ЬН : 0	ШС : 0	ФЯ : 0	СО : 0	ОЛ : 0	ЛЙ : 0	ЗР : 0	ГЭ : 0	АФ : 0
МЩ : 4	ОН : 3	ЛИ : 2	ЩИ : 1	ЛЬ : 1	ЯУ : 0	ЬМ : 0	ШР : 0	ФЭ : 0	СН : 0	ОК : 0	ЛЗ : 0	ЗП : 0	ГЫ : 0	АУ : 0
МТ : 4	НЙ : 3	ЛА : 2	ЩЗ : 1	ЛЩ : 1	ЯС : 0	ЬК : 0	ШП : 0	ФЬ : 0	СМ : 0	ОЗ : 0	ЛГ : 0	ЗК : 0	ГШ : 0	АС : 0
КЩ : 4	КД : 3	КЬ : 2	ШО : 1	ЛХ : 1	ЯР : 0	ЬИ : 0	ШМ : 0	ФШ : 0	СК : 0	ОЖ : 0	ЛБ : 0	ЗИ : 0	ГХ : 0	АР : 0
КГ : 4	ЙГ : 3	КЕ : 2	ЧЭ : 1	ЛУ : 1	ЯП : 0	ЬГ : 0	ШЛ : 0	ФЧ : 0	СЙ : 0	ОГ : 0	КЯ : 0	ЗЖ : 0	ГФ : 0	АП : 0
ЙВ : 4	ИЩ : 3	КВ : 2	ЧХ : 1	ЛТ : 1	ЯН : 0	ЬБ : 0	ШК : 0	ФХ : 0	СИ : 0	НЯ : 0	КЭ : 0	ЗГ : 0	ГТ : 0	АН : 0
ЙА : 4	ИЖ : 3	ЙЮ : 2	ЧР : 1	ЛЖ : 1	ЯК : 0	ЬА : 0	ШЖ : 0	ФФ : 0	СЖ : 0	НЬ : 0	КЫ : 0	ЗВ : 0	ГР : 0	АЛ : 0
ИЯ : 4	ИБ : 3	ЙШ : 2	ЦЩ : 1	ЛД : 1	ЯЗ : 0	ЫЯ : 0	ШБ : 0	ФС : 0	РЭ : 0	НШ : 0	КШ : 0	ЖЫ : 0	ГН : 0	АЙ : 0
ЖЭ : 4	ЗШ : 3	ЙЦ : 2	ЦЧ : 1	КЗ : 1	ЯЖ : 0	ЫЭ : 0	ЧЯ : 0	ФР : 0	РЬ : 0	НЧ : 0	КЧ : 0	ЖЧ : 0	ГМ : 0	АЗ : 0
ЕЭ : 4	ЖЩ : 3	ЙТ : 2	ЦЦ : 1	КЖ : 1	ЯГ : 0	ЫЫ : 0	ЧЬ : 0	ФО : 0	РЫ : 0	НЦ : 0	КЦ : 0	ЖЦ : 0	ГЛ : 0	АГ : 0
ДЬ : 4	ЕЖ : 3	ИЦ : 2	ЦХ : 1	ЙЯ : 1	ЯБ : 0	ЫШ : 0	ЧЫ : 0	ФН : 0	РЩ : 0	НФ : 0	КХ : 0	ЖХ : 0	ГК : 0	АВ : 0

Перші 5 найчастіших біграм шифротексту можна співставити 5-ом найчастішим біграмам відкритого змістовного тексту російською мовою, хоча при аналізі шифротексту мого варіанту цього виявилося недостатньо, і найчастіші біграми шифротексту – не перші 5, а наступні за ними, і програма перебирає можливі співставлення для 20 перших пар біграм. Тому мені потрібен був повний рейтинг частот біграм для дуже великого тексту російською мовою(з 1-ї лабораторної наприклад):

ТО : 9863	ОП : 2556	МН : 1263	ЫЙ : 817	УР : 579	ТБ : 386	СЧ : 257	РЖ : 188	БС : 124	ЬА : 84	МХ : 51	ЩЬ : 25	ЖС : 12	ЦГ : 4	ГФ : 1
СТ : 7109	ЧТ : 2549	НТ : 1234	ЛУ : 814	ВЛ : 577	ВД : 386	ЯБ : 256	ЯУ : 185	ОА : 123	ЙА : 84	ЛР : 51	ФЛ : 25	ДЭ : 12	ФБ : 4	ГЖ : 1
НА : 6722	ЕД : 2544	ИХ : 1231	ЕИ : 811	МС : 572	ЙТ : 382	ХИ : 256	ВГ : 184	БЩ : 123	ИФ : 84	ЫЖ : 50	ХЖ : 24	БЖ : 12	РФ : 4	ЯЬ : 0
НО : 6534	СЯ : 2535	АЕ : 1231	НЯ : 810	ВП : 571	ЛЫ : 378	ГН : 256	ТМ : 183	ФА : 121	ЗЗ : 83	ЗЖ : 50	ТХ : 24	ЭП : 11	ПЮ : 4	ЯЫ : 0
НЕ : 6273	ТИ : 2527	ОО : 1222	ДУ : 808	ПЛ : 565	ЦА : 377	ТТ : 251	БН : 182	ЯЯ : 120	РЛ : 82	ФР : 49	ББ : 24	ЩР : 11	ПМ : 4	ЮЬ : 0
ПО : 6147	МЕ : 2462	ЕЗ : 1210	ЕШ : 807	ЙН : 563	ЗМ : 377	ЫБ : 250	РС : 181	РД : 120	ЕФ : 81	СЗ : 49	ЭН : 23	ЦН : 11	МЩ : 4	ЮЫ : 0
ЕН : 5961	ЧЕ : 2342	ИЯ : 1205	АО : 807	ЛЮ : 560	РТ : 372	ТЧ : 250	ЬУ : 180	ПС : 120	ЙШ : 79	ЩН : 48	ТШ : 23	ФТ : 11	ЖР : 4	ЭЯ : 0
ОН : 5611	ОЙ : 2289	ЗН : 1201	АЖ : 803	ИГ : 551	ЕХ : 362	ТД : 248	ЮЖ : 179	ЮВ : 115	ЮМ : 78	ШТ : 48	ВЖ : 23	ФН : 11	ЖЗ : 4	ЭЮ : 0
ОТ : 5553	АЗ : 2287	КУ : 1196	МЫ : 792	ЬИ : 547	ЬЧ : 361	ЛП : 248	ЗЛ : 173	УА : 115	ОЮ : 78	НФ : 48	ЯФ : 22	ЗШ : 11	ДФ : 4	ЭЭ : 0
НИ : 5509	АМ : 2244	ВН : 1192	БР : 780	ВШ : 545	ТЯ : 357	ЯЕ : 247	ЙР : 172	ДП : 115	ЯА : 77	ДГ : 48	ЮЮ : 22	ЖП : 11	ГЯ : 4	ЭЬ : 0
ОС : 5428	ДО : 2190	ОИ : 1186	УЧ : 778	БУ : 543	МК : 347	СЫ : 247	ВЯ : 172	ЦО : 114	КЗ : 77	НМ : 46	ЮЛ : 22	ЯЙ : 10	ББ : 4	ЭЫ : 0
ОВ : 5399	МИ : 2172	ЕЕ : 1181	КТ : 777	ЬО : 536	МЯ : 346	ЛВ : 245	ЙЗ : 171	ЙГ : 114	ХБ : 75	ДМ : 46	РЩ : 22	ЧР : 10	ЭЙ : 3	ЭЩ : 0
КО : 5296	ЕГ : 2133	ИР : 1174	АИ : 769	ЦЕ : 530	ЮТ : 345	ЫО : 243	ЕЦ : 171	ПН : 113	УУ : 75	ВЮ : 46	ЖЧ : 22	НШ : 10	ЫФ : 3	ЭЧ : 0
АЛ : 5114	СЬ : 2130	ТЫ : 1171	ЫХ : 759	СС : 523	ЬМ : 332	ЫД : 243	ЯГ : 170	ЮИ : 112	БК : 74	ТЦ : 45	ШМ : 21	КХ : 10	ШЩ : 3	ЭЦ : 0
РО : 5109	ЖЕ : 2109	УТ : 1170	ЫС : 752	ЛН : 521	ЯЧ : 327	УО : 242	УЕ : 169	ЯЭ : 111	РР : 73	ДШ : 45	КШ : 21	ЖТ : 10	ШС : 3	ЭО : 0
РА : 4801	СЕ : 2099	ШЕ : 1169	ЖН : 749	СУ : 516	ШЛ : 324	ЬЯ : 241	ЬЭ : 167	ДЦ : 111	ЗТ : 73	ЖЬ : 43	БП : 21	ЦР : 9	ЧФ : 3	ЭИ : 0
ЛИ : 4727	БЫ : 2088	КР : 1155	ГА : 736	ПУ : 511	БЯ : 322	ШН : 239	ЛЛ : 166	ОЦ : 110	СЭ : 70	ЧО : 42	ЮЯ : 20	ЦД : 9	ЦЗ : 3	ЭЖ : 0
ЛА : 4507	СЛ : 2084	ЩЕ : 1142	УВ : 735	УИ : 505	ЙИ : 319	УЗ : 239	ЧЬ : 165	РП : 109	РЮ : 70	ХГ : 42	ЬФ : 20	ХЦ : 9	ПВ : 3	ЭЕ : 0
ПР : 4396	ИМ : 2074	ЯН : 1136	ИЦ : 728	ВК : 504	ДС : 319	СР : 235	ЖУ : 163	ЙЛ : 109	БЬ : 70	ВЦ : 42	ЦК : 20	ПЧ : 9	ЗХ : 3	ЭБ : 0
ЛО : 4393	НН : 2051	ДН : 1124	ЯП : 723	ЙП : 501	ОЭ : 318	НП : 233	ЩУ : 162	ЙЭ : 108	КЦ : 69	ГЧ : 41	ХЯ : 20	ЛФ : 9	ЖЭ : 3	ЭА : 0
РЕ : 4379	СК : 2016	ТС : 1122	УН : 718	ЯО : 499	ЮД : 317	ВВ : 233	ЬР : 160	ВЧ : 108	ЖК : 68	ЬЖ : 40	НЭ : 20	ЖГ : 9	ЖХ : 3	ЬЬ : 0
ОЛ : 4275	ОК : 1989	ЧА : 1121	РН : 716	ЕЩ : 498	ГУ : 316	СД : 230	ЯХ : 159	ОФ : 107	ХЕ : 67	ЧЛ : 40	НЛ : 20	ГЭ : 9	ГХ : 3	ЫЬ : 0
ЕР : 4203	ЕВ : 1987	УД : 1120	ЗО : 715	ЖД : 497	ПЫ : 315	ВМ : 230	ХР : 157	ЗП : 107	ЫЭ : 66	ЮГ : 39	ДЮ : 20	БТ : 9	БЮ : 3	ЬЙ : 0
КА : 4182	ВИ : 1963	ИО : 1111	ГД : 712	ЬЕ : 491	РЬ : 313	АЩ : 228	ЛТ : 157	ХТ : 106	ГВ : 66	РБ : 39	БМ : 20	ЦМ : 8	ЭЗ : 2	ЫЬ : 0
ОМ : 4143	ИК : 1948	ТН : 1106	УП : 710	ГИ : 491	ЗИ : 313	ЭК : 227	ЮБ : 155	СБ : 106	ЮР : 65	ЙХ : 39	ШП : 19	ХХ : 8	ЭГ : 2	ЩЯ : 0
ГО : 4065	ЕП : 1931	ЛЯ : 1105	ШЬ : 707	БА : 489	ЙК : 309	ОЩ : 227	ХК : 154	ЛБ : 106	ЬЦ : 65	ЙЯ : 38	ХФ : 19	УЦ : 8	ЫЮ : 2	ЩЮ : 0
ЕТ : 3974	ВС : 1897	СИ : 1104	АХ : 697	ЮЩ : 486	ЗЕ : 309	АЭ : 227	ЬЛ : 153	ХМ : 105	УЙ : 65	ЮЭ : 37	ТФ : 19	КЮ : 8	ЩВ : 2	ЩЭ : 0
ЕС : 3958	ИЕ : 1876	БЕ : 1098	УГ : 696	ОШ : 478	ЬЗ : 308	ЫР : 226	ЫЧ : 153	ЛМ : 105	ГП : 65	НЩ : 37	МШ : 19	ЙЮ : 8	ЧС : 2	ЩЫ : 0
ТЬ : 3866	ТВ : 1829	УС : 1088	УК : 695	ЯМ : 477	УЩ : 308	ЫК : 226	НР : 153	ЮО : 104	ЬХ : 64	СФ : 35	ЛХ : 19	ШР : 7	ЧЗ : 2	ЩЩ : 0
ВО : 3836	ИЗ : 1800	ЫЛ : 1073	ЯК : 692	ЫП : 477	КВ : 306	ЬБ : 224	ЮП : 152	АА : 104	ХЗ : 64	ЮЕ : 34	ЖБ : 19	ЦТ : 7	ЦЧ : 2	ЩШ : 0
АН : 3539	ОЧ : 1758	ЕО : 1056	УМ : 688	ЫН : 466	ЫИ : 305	ДК : 222	ЮК : 151	ШО : 103	ВХ : 64	ТЮ : 34	ЮХ : 18	ЦБ : 7	ЦЛ : 2	ЩЧ : 0
ВА : 3515	СО : 1753	ГР : 1033	ЯД : 687	ВУ : 466	ЬД : 304	ЧК : 220	ЛГ : 149	ЗЯ : 103	ЧШ : 63	МФ : 34	ЭМ : 18	ФК : 7	ХЮ : 2	ЩЦ : 0
АС : 3472	КИ : 1744	ИЧ : 1018	ВР : 687	БЛ : 466	ЙО : 303	ИЮ : 220	ЙБ : 149	ИЩ : 101	РЧ : 63	ЙФ : 34	ЦС : 18	МЮ : 7	ФМ : 2	ЩХ : 0
ТА : 3468	ЭТ : 1698	ЫВ : 1007	УЮ : 682	ЯИ : 458	ХН : 302	АЦ : 220	ЫГ : 148	ЗЬ : 101	КГ : 63	ДБ : 34	ЭД : 17	ЛЦ : 7	СЩ : 2	ЩФ : 0
ОГ : 3460	МА : 1668	ЕЧ : 1007	ИБ : 678	ОХ : 452	ЗУ : 301	ГЕ : 219	ЮН : 147	СЮ : 100	ЯЦ : 62	ЫА : 33	ШВ : 17	КФ : 7	ПШ : 2	ЩТ : 0
ОД : 3387	ЬН : 1633	ЯВ : 1006	ЬП : 674	КЕ : 452	АЙ : 295	ДТ : 217	ЫЗ : 147	УЯ : 99	ЦВ : 62	ХЭ : 32	УФ : 17	ЗФ : 7	БЧ : 2	ЩС : 0
АТ : 3344	АП : 1626	ЯТ : 990	ЫТ : 673	НС : 448	ФО : 292	ЯР : 216	ЮЧ : 146	НЗ : 99	ЕЮ : 62	МЬ : 32	ТЩ : 17	ЖЛ : 7	ЭШ : 1	ЩМ : 0
ОР : 3330	ДИ : 1612	ЫМ : 983	КС : 667	КЛ : 448	ЩА : 288	ТЛ : 215	ДЖ : 139	РШ : 96	ТГ : 60	ЗЭ : 32	НХ : 17	ЭХ : 6	ЭУ : 1	ЩЛ : 0
ЕЛ : 3212	НУ : 1592	СА : 972	ЖА : 665	ВТ : 447	НК : 285	ЛЖ : 215	ВЭ : 139	КД : 96	МЭ : 60	ЙЦ : 31	ЮФ : 16	ЫЦ : 6	ЫЫ : 1	ЩК : 0
ИЛ : 3199	ОЕ : 1589	ЛС : 970	ЗВ : 663	ТП : 443	ИЖ : 285	ДЯ : 213	ВБ : 139	ЛД : 95	ЙЕ : 60	ГБ : 31	ЭВ : 16	ФВ : 6	ЩП : 1	ЩЙ : 0
ЕМ : 3177	ЕК : 1587	ЬК : 968	ЗД : 660	КН : 433	РВ : 284	МЛ : 209	ЯЖ : 138	ШУ : 94	СШ : 59	БХ : 31	ЦП : 16	ЖЯ : 6	ЩО : 1	ЩЗ : 0
АК : 3152	ЕЙ : 1586	ТУ : 967	ЩИ : 658	ША : 431	ЬЮ : 283	ЕА : 209	ХЛ : 138	ПЯ : 94	ЙЖ : 58	ДХ : 30	ЛШ : 16	ВЩ : 6	ЩД : 1	ЩЖ : 0
ТЕ : 3129	АД : 1549	СВ : 950	МП : 658	АШ : 428	ЫШ : 283	НД : 208	НЧ : 138	ЙУ : 94	ЫЯ : 57	ЯШ : 28	ГЗ : 16	БГ : 6	ШЧ : 1	ЩГ : 0
ИТ : 3124	ЬС : 1524	УЛ : 946	АГ : 657	ЬШ : 427	ИУ : 278	ММ : 208	МР : 138	ЯЮ : 93	КЭ : 57	ЮА : 28	ФЫ : 15	ЮЙ : 5	ШГ : 1	ЩБ : 0
ЗА : 3084	ХО : 1511	ЯС : 942	ТК : 655	УШ : 426	ИА : 277	РК : 204	КМ : 138	ЦУ : 93	ЖО : 57	КЯ : 28	РЭ : 15	ЭС : 5	ЧЧ : 1	ШЯ : 0
ОБ : 3022	ПЕ : 1501	АБ : 930	АЮ : 655	ЕУ : 424	ХС : 276	КП : 204	ЬГ : 136	ФЕ : 92	ТЖ : 56	ЗЧ : 28	НЖ : 15	ЬЩ : 5	ЧХ : 1	ШЮ : 0
РИ : 2981	АЯ : 1498	БИ : 927	РЯ : 650	ДЛ : 417	ЗЫ : 276	ДЬ : 202	НЦ : 135	ЮЗ : 91	КЖ : 56	РЗ : 27	МЦ : 15	ШД : 5	ЧП : 1	ШЭ : 0
ВЕ : 2974	ИД : 1476	ЧИ : 920	ПИ : 647	ЯЗ : 408	АФ : 276	РМ : 201	ЗБ : 133	ЫУ : 91	УЭ : 55	ПЬ : 27	ЮШ : 14	ШБ : 5	ЧД : 1	ШЫ : 0
ИН : 2973	РУ : 1470	ШИ : 913	ИЙ : 644	МВ : 406	ХВ : 275	ЮС : 199	КБ : 132	ТЗ : 91	ДЧ : 55	ЗЦ : 27	ЭФ : 14	ХЬ : 5	ЦЭ : 1	ШЩ : 0
ИС : 2954	ОЖ : 1448	АЧ : 912	ЦИ : 635	ДЫ : 405	МТ : 275	ЕЭ : 199	ХД : 131	ЗС : 91	МЖ : 54	ГТ : 27	ЫЩ : 13	ФЗ : 5	ЦХ : 1	ШШ : 0
ДЕ : 2851	ИП : 1442	ГЛ : 911	ЕЖ : 618	УБ : 404	УХ : 272	ИЭ : 198	КК : 131	ТЭ : 89	ФУ : 53	ГМ : 27	ЧВ : 13	ПД : 5	ХЩ : 1	ШХ : 0
ДА : 2831	БО : 1441	ЙС : 907	ДР : 612	ШК : 402	ЗГ : 271	ХА : 196	ХУ : 130	ПК : 89	ПП : 53	ЮУ : 26	ФФ : 13	ЛЩ : 5	ФЭ : 1	ШФ : 0
ЛЕ : 2789	СП : 1434	РЫ : 891	АУ : 611	ЬТ : 401	МД : 269	ФИ : 196	РХ : 129	ЛЗ : 89	НГ : 53	ЭЛ : 26	ФС : 13	ЙЩ : 5	ФЬ : 1	ШЙ : 0
МО : 2777	ОЗ : 1434	УЖ : 890	ЧН : 607	НЬ : 397	МЧ : 267	ЯЩ : 193	МЗ : 129	ВЬ : 89	ЛЭ : 53	ХШ : 26	ФП : 13	ЗЮ : 5	ФХ : 1	ШЗ : 0
АВ : 2682	МУ : 1412	УЖ : 857	ОЯ : 607	ЛК : 394	ЙД : 264	ЙЧ : 193	ЦЫ : 128	НЮ : 88	ДД : 53	СЖ : 26	ЖВ : 13	ЖМ : 5	ФД : 1	ШЖ : 0
ТР : 2658	АР : 1389	ЫЕ : 851	СМ : 605	ЙВ : 394	ХП : 262	ЗК : 193	МГ : 128	НБ : 87	ГС : 53	РЦ : 26	ГГ : 13	ЖЖ : 5	ФГ : 1	ЧЯ : 0
ЛЬ : 2656	ВЫ : 1387	ПА : 851	ИШ : 602	ЧУ : 392	ЛЧ : 262	МБ : 192	КЧ : 126	СГ : 86	БЭ : 53	ДЗ : 26	БД : 13	ГШ : 5	ПЭ : 1	ЧЮ : 0
НЫ : 2612	ЕБ : 1354	ЖИ : 822	ЯЛ : 585	ОУ : 391	ЙМ : 261	ЕЯ : 192	СХ : 125	ПТ : 85	ХЧ : 52	ВФ : 26	ЮЦ : 12	БЗ : 5	ПЗ : 1	ЧЭ : 0
ИВ : 2578	ИИ : 1274	ЬВ : 817	ДВ : 583	ВЗ : 391	ЗР : 260	НВ : 189	РГ : 125	ГК : 85	СЦ : 51	БШ : 26	ЭР : 12	ЦЯ : 4	ГЮ : 1	ЧЫ : 0

```
ЧЩ : 0      ЧГ : 0      ЦШ : 0      ХЫ : 0      ФШ : 0      УЬ : 0      ПЩ : 0      ПЖ : 0      НЙ : 0      КЩ : 0      ИЬ : 0      ЖЫ : 0      ЖЙ : 0      ГЬ : 0      ВЙ : 0
ЧЦ : 0      ЧБ : 0      ЦЦ : 0      ХЙ : 0      ФЧ : 0      УЫ : 0      ПЦ : 0      ПГ : 0      МЙ : 0      КЙ : 0      ИЫ : 0      ЖЩ : 0      ЕЬ : 0      ГЫ : 0      БЦ : 0
ЧМ : 0      ЦЮ : 0      ЦФ : 0      ФЯ : 0      ФЦ : 0      ТЙ : 0      ПХ : 0      ПБ : 0      ЛЙ : 0      ЙЬ : 0      ЗЩ : 0      ЖШ : 0      ЕЫ : 0      ГЩ : 0      БФ : 0
ЧЙ : 0      ЦЬ : 0      ЦЙ : 0      ФЮ : 0      ФЙ : 0      СЙ : 0      ПФ : 0      ОЬ : 0      КЬ : 0      ЙЫ : 0      ЗЙ : 0      ЖЦ : 0      ДЩ : 0      ГЦ : 0      БЙ : 0
ЧЖ : 0      ЦЩ : 0      ЦЖ : 0      ФЩ : 0      ФЖ : 0      РЙ : 0      ПЙ : 0      ОЫ : 0      КЫ : 0      ЙЙ : 0      ЖЮ : 0      ЖФ : 0      ДЙ : 0      ГЙ : 0      АЬ : 0
```

Даний рейтинг частот було узято, як еталон розподілу біграм у змістовному тексту російською мовою. Для криптоаналізу узято лише перші 20:

```
ТО,   СТ,   НА,   НО,   НЕ,   ПО,   ЕН,   ОН,   ОТ,   НИ,   ОС,   ОВ,   КО,   АЛ,   РО,   РА,   ЛИ,   ЛА,   ПР,   ЛО,  ...
ЩЕ,   ХЕ,   ЧВ,   ЛЕ,   ЦВ,   ОЩ,   СД,   ЖЕ,   ДЕ,   ГД,   НЮ,   НВ,   МЮ,   ЛП,   ЭЩ,   ЭА,   ЯХ,   ЩА,   ХД,   НЕ,  ...
```

Що цікаво, рейтинг не співпадає порядком з тим, що пропонується методичними вказівками(перші п’ять найчастіших біграм – разом одні й ті ж, але в різному порядку для мого тексту і вказані у методичці). У кращому разі потрібно перебирати співставлення біграм кожна з кожною, а не більш частіша(та, що лівіша в рейтингу) з більш частішою(лівішою), а менш частіша – з меншою. Але шифротекст мого варіанту розшифровувався для криптоаналізу з другого випадку, а отже його рейтинг частот біграм відповідає взятому з мого великого тексту. Такий метод перебирає менше варіантів, а отже швидший. Тим не менш варіантів усе одно дуже багато, тому їх потрібно відсіювати за деякий критерієм змістовного тексту(перевіряти розшифрований ключем, який ми вважаємо, що може бути правильним). З лабораторної роботи 2 я знаю, що гарно себе проявляє ентропійний критерій – індекс відповідності відкритого(тобто правильно розшифрованого тексту) має бути >0.05(набагато більший за індекс відповідності шифротекстів) і ми можемо використовувати цей метод, бо афінний шифр не використовує перестановок – тільки підстановки. Відповідно отримаємо автоматичним криптоаналізом програмою `main_cryptoanalysis.py` для файлу з шифротекстом `06.txt`:

```
Python 3.7.4 (tags/v3.7.4:e09359112e, Jul  8 2019, 19:29:22) [MSC v.1916 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
 RESTART: .................\gakh_fb-83_cp3\Lab3\main_cryptoanalysis.py
ЫВЛЕЮГЗЕБЩПЕЩХЩУЙЭВИЫВИЮФГУВХЦУБХЩЫЮНЮЖЛЕПЭШФМИЫХДОЩБУДНЗЕГД

index: 0.054154683957941444, key: (441, 310), text:
КТРОБЬЛОТИХОЕГОРОДОККТАННЬЙТЫМОЙМИЗНОНЕЖИЛСЯВПОСТЕЛИПРИШЛОЛЕТОИВЕТЕРБЬЛЛЕТНИЙТЕПЛОЕДЬХАНИЕМИРАНЕСПЕШНОЕИЛЕНИВОЕСТОИТЛИЮСВСТАЧСВЬИУНУЧССЯВОКОШКОИТОТ
ЧАСПОЙМЕШЫВОТОНАНЦЧИНАЕТСЯНАСТОЯЩАЯСВОБОДАИЖИЗНЫВОТОН
--------------------------------------------------------------------------------

index: 0.054154683957941444, key: (441, 310), text:
КТРОБЬЛОТИХОЕГОРОДОККТАННЬЙТЫМОЙМИЗНОНЕЖИЛСЯВПОСТЕЛИПРИШЛОЛЕТОИВЕТЕРБЬЛЛЕТНИЙТЕПЛОЕДЬХАНИЕМИРАНЕСПЕШНОЕИЛЕНИВОЕСТОИТЛИЮСВСТАЧСВЬИУНУЧССЯВОКОШКОИТОТ
ЧАСПОЙМЕШЫВОТОНАНЦЧИНАЕТСЯНАСТОЯЩАЯСВОБОДАИЖИЗНЫВОТОН
--------------------------------------------------------------------------------

>>>
```

По розшифрованому тексту видно, що він таки змістовний на великих його проміжках, але є місця, що неможливо прочитати. Тут потрібен уже ручний аналіз – визначення нерозшифрованих осередків тексту по їх сусіднім, розшифрованим правильно, частинам, з яких можна отримати зміст даного місця в тексті. От наприклад:

`КТРОБЬЛОТИХОЕГОРОД` – точно малося на увазі `...БЫЛОТИХОЕГОРОД`, тобто чомусь буква `Ы` була замінена `Ь`. Дана заміна також простежується далі: `ОККТАННЬЙТЫМОЙ` – біграма `ЫЙ` дуже часто зустрічається, а `ЬЙ` – неможлива, і зміст з біграмою `ЫЙ` є – в цьому місці буде прикметник.Оскільки помилкова тільки одна літера при тому, що текст шифрується біграмами, то було зроблено висновок, що саме літери `Ы` та `Ь` неправильно декодуються, а причина цьому може бути тільки в неправильній нумерації саме цих літер в алфавіті(вони стоять поруч, а тому зміна їх номерів один на одного і не вплинув на інші літери, за те якщо їх поміняти місцями отримаємо повністю змістовний текст).
Тобто тепер встановимо номер літери `Ь` як 27, а `Ы` – як 26, що протиречить офіційному порядку літер в російському алфавіті:

```
Python 3.7.4 (tags/v3.7.4:e09359112e, Jul  8 2019, 19:29:22) [MSC v.1916 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
 RESTART: .................\gakh_fb-83_cp3\Lab3\main_cryptoanalysis.py
ЫВЛЕЮГЗЕБЩПЕЩХЩУЙЭВИЫВИЮФГУВХЦУБХЩЫЮНЮЖЛЕПЭШФМИЬХДОЩБУДНЗЕГД
```

```
index: 0.054227534807633565, key: (441, 310), text:
УТРОБЫЛОТИХОЕГОРОДОКУТАННЫЙТЬМОЙМИРНОНЕЖИЛСЯВПОСТЕЛИПРИШЛОЛЕТОИВЕТЕРБЫЛЛЕТНИЙТЕПЛОЕДЫХАНИЕМИРАНЕСПЕШНОЕИЛЕНИВОЕСТОИТЛИШЬВСТАТЬВЫСУНУТЬСЯВОКОШКОИТОТ
ЧАСПОЙМЕШЬВОТОНАНАЧИНАЕТСЯНАСТОЯЩАЯСВОБОДАИЖИЗНЬВОТОН
----------------------------------------------------------------------------------

index: 0.054227534807633565, key: (441, 310), text:
УТРОБЫЛОТИХОЕГОРОДОКУТАННЫЙТЬМОЙМИРНОНЕЖИЛСЯВПОСТЕЛИПРИШЛОЛЕТОИВЕТЕРБЫЛЛЕТНИЙТЕПЛОЕДЫХАНИЕМИРАНЕСПЕШНОЕИЛЕНИВОЕСТОИТЛИШЬВСТАТЬВЫСУНУТЬСЯВОКОШКОИТОТ
ЧАСПОЙМЕШЬВОТОНАНАЧИНАЕТСЯНАСТОЯЩАЯСВОБОДАИЖИЗНЬВОТОН
----------------------------------------------------------------------------------

index: 0.054227534807633565, key: (441, 310), text:
УТРОБЫЛОТИХОЕГОРОДОКУТАННЫЙТЬМОЙМИРНОНЕЖИЛСЯВПОСТЕЛИПРИШЛОЛЕТОИВЕТЕРБЫЛЛЕТНИЙТЕПЛОЕДЫХАНИЕМИРАНЕСПЕШНОЕИЛЕНИВОЕСТОИТЛИШЬВСТАТЬВЫСУНУТЬСЯВОКОШКОИТОТ
ЧАСПОЙМЕШЬВОТОНАНАЧИНАЕТСЯНАСТОЯЩАЯСВОБОДАИЖИЗНЬВОТОН
----------------------------------------------------------------------------------

>>>
```

Бачимо, що текст розшифровується тепер повністю правильно. Ключ шифрування був `(a,b) = (441,310).` Повний відкритий текст:

```
УТРОБЫЛОТИХОЕГОРОДОКУТАННЫЙТЬМОЙМИРНОНЕЖИЛСЯВПОСТЕЛИПРИШЛОЛЕТОИВЕТЕРБЫЛЛЕТНИЙТЕПЛОЕДЫХАНИЕМИРАНЕСПЕШНОЕИЛЕНИВОЕСТОИТЛИШЬВСТАТЬВЫСУНУТЬСЯВОКОШКОИТОТ
ЧАСПОЙМЕШЬВОТОНАНАЧИНАЕТСЯНАСТОЯЩАЯСВОБОДАИЖИЗНЬВОТОНОПЕРВОЕУТРОЛЕТАДУГЛАССПОЛДИНГДВЕНАДЦАТИЛЕТОТРОДУТОЛЬКОЧТООТКРЫЛГЛАЗАИКАКВТЕПЛУЮРЕЧКУПОГРУЗИЛСЯ
ВПРЕДРАССВЕТНУЮБЕЗМЯТЕЖНОСТЬОНЛЕЖАЛВСВОДЧАТОЙКОМНАТКЕНАЧЕТВЕРТОМЭТАЖЕВОВСЕМГОРОДЕНЕБЫЛОБАШНИВЫШЕИОТТОГОЧТООНПАРИЛТАКВЫСОКОВВОЗДУХЕВМЕСТЕСИЮНЬСКИМВЕ
ТРОМВНЕМРОЖДАЛАСЬЧУДОДЕЙСТВЕННАЯСИЛАПОНОЧАМКОГДАВЯЗЫДУБЫИКЛЕНЫСЛИВАЛИСЬВОДНОБЕСПОКОЙНОЕМОРЕДУГЛАСОКИДЫВАЛЕГОВЗГЛЯДОМПРОНЗАВШИМТЬМУТОЧНОМАЯКИСЕГОДНЯ
ВОТЗДОРОВОШЕПНУЛОНВПЕРЕДИЦЕЛОЕЛЕТОНЕСЧЕТНОЕМНОЖЕСТВОДНЕЙЧУТЬНЕПОЛКАЛЕНДАРЯОНУЖЕВИДЕЛСЕБЯМНОГОРУКИМКАКБОЖЕСТВОШИВАИЗКНИЖКИПРОПУТЕШЕСТВИЯТОЛЬКОПОСПЕВ
АЙРВАТЬЕЩЕЗЕЛЕНЫЕЯБЛОКИПЕРСИКИЧЕРНЫЕКАКНОЧЬСЛИВЫЕГОНЕВЫТАЩИТЬИЗЛЕСУИЗКУСТОВИЗРЕЧКИАКАКПРИЯТНОБУДЕТПОМЕРЗНУТЬЗАБРАВШИСЬВЗАИНДЕВЕЛЫЙЛЕДНИККАКВЕСЕЛОЖА
РИТЬСЯВБАБУШКИНОЙКУХНЕЗАОДНОСТЫСЯЧЬЮЦЫПЛЯТАПОКАЗАДЕЛОРАЗВНЕДЕЛЮЕМУПОЗВОЛЯЛИНОЧЕВАТЬНЕВДОМИКЕПОСОСЕДСТВУГДЕСПАЛИЕГОРОДИТЕЛИИМЛАДШИЙБРАТИШКАТОМАЗДЕСЬ
ВДЕДОВСКОЙБАШНЕОНВЗБЕГАЛПОТЕМНОЙВИНТОВОЙЛЕСТНИЦЕНАСАМЫЙВЕРХИЛОЖИЛСЯСПАТЬВЭТОЙОБИТЕЛИКУДЕСНИКАСРЕДИГРОМОВИВИДЕНИЙАСПОЗАРАНКУКОГДАДАЖЕМОЛОЧНИКЕЩЕНЕЗВ
ЯКАЛБУТЫЛКАМИНАУЛИЦАХОНПРОСЫПАЛСЯИПРИСТУПАЛКЗАВЕТНОМУВОЛШЕБСТВУСТОЯВТЕМНОТЕУОТКРЫТОГООКНАОННАБРАЛПОЛНУЮГРУДЬВОЗДУХАИИЗОВСЕХСИЛДУНУЛУЛИЧНЫЕФОНАРИМИГ
ОМПОГАСЛИТОЧНОСВЕЧКИНАЧЕРНОМИМЕНИННОМПИРОГЕДУГЛАСДУНУЛЕЩЕИЕЩЕИВНЕБЕНАЧАЛИГАСНУТЬЗВЕЗДЫДУГЛАСУЛЫБНУЛСЯТКНУЛПАЛЬЦЕМТАМИТАМТЕПЕРЬТУТИВОТТУТВПРЕДУТРЕНН
ЕМТУМАНЕОДИНЗАДРУГИМПРОРЕЗАЛИСЬПРЯМОУГОЛЬНИКИВДОМАХЗАЖИГАЛИСЬОГНИДАЛЕКОДАЛЕКОНАРАССВЕТНОЙЗЕМЛЕВДРУГОЗАРИЛАСЬЦЕЛАЯВЕРЕНИЦАОКОНВСЕМЗЕВНУТЬВСЕМВСТАВАТ
ЬОГРОМНЫЙДОМВНИЗУОЖИЛДЕДУШКАВЫНИМАЙЗУБЫИЗСТАКАНАДУГЛАСНЕМНОГОПОДОЖДАЛБАБУШКАИПРАБАБУШКАЖАРЬТЕОЛАДЬИСКВОЗНЯКПРОНЕСПОВСЕМКОРИДОРАМТЕПЛЫЙДУХЖАРЕНОГОТЕ
СТАИВОВСЕХКОМНАТАХВСТРЕПЕНУЛИСЬМНОГОЧИСЛЕННЫЕТЕТКИДЯДЬЯДВОЮРОДНЫЕБРАТЬЯИСЕСТРЫЧТОСЕХАЛИСЬСЮДАПОГОСТИТЬУЛИЦАСТАРИКОВПРОСЫПАЙСЯМИССЭЛЕНЛУМИСПОЛКОВНИК
ФРИЛЕЙМИССИСБЕНТЛИПОКАШЛЯЙТЕВСТАНЬТЕПРОГЛОТИТЕСВОИТАБЛЕТКИПОШЕВЕЛИВАЙТЕСЬМИСТЕРДЖОНАСЗАПРЯГАЙТЕЛОШАДЬВЫВОДИТЕИЗСАРАЯФУРГОНПОРАЕХАТЬЗАСТАРЬЕМПОТУСТО
РОНУОВРАГАОТКРЫЛИСВОИДРАКОНЬИГЛАЗАУГРЮМЫЕОСОБНЯКИСКОРОВНИЗУПОЯВЯТСЯНАЭЛЕКТРИЧЕСКОЙЗЕЛЕНОЙМАШИНЕДВЕСТАРУХИИПОКАТЯТПОУТРЕННИМУЛИЦАМПРИВЕТСТВЕННОМАХАЯ
КАЖДОЙВСТРЕЧНОЙСОБАКЕМИСТЕРТРИДДЕНБЕГИТЕВТРАМВАЙНОЕДЕПОИВСКОРЕПОУЗКИМРУСЛАММОЩЕНЫХУЛИЦПОПЛЫВЕТТРАМВАЙРАССЫПАЯВОКРУГЖАРКИЕСИНИЕИСКРЫДЖОНХАФЧАРЛИВУДМ
ЕНВЫГОТОВЫШЕПНУЛДУГЛАСУЛИЦЕДЕТЕЙГОТОВЫСПРОСИЛОНУБЕЙСБОЛЬНЫХМЯЧЕЙЧТОМОКЛИНАРОСИСТЫХЛУЖАЙКАХУПУСТЫХВЕРЕВОЧНЫХКАЧЕЛЕЙЧТОСКУЧАЯСВИСАЛИСДЕРЕВЬЕВМАМПАПТО
МПРОСНИТЕСЬТИХОНЬКОПРОЗВЕНЕЛИБУДИЛЬНИКИГУЛКОПРОБИЛИЧАСЫНАЗДАНИИСУДАТОЧНОСЕТЬЗАБРОШЕННАЯЕГОРУКОЙСДЕРЕВЬЕВВЗМЕТНУЛИСЬПТИЦЫИЗАПЕЛИДИРИЖИРУЯСВОИМОРКЕСТ
РОМДУГЛАСПОВЕЛИТЕЛЬНОПРОТЯНУЛРУКУКВОСТОКУИВЗОШЛОСОЛНЦЕДУГЛАССКРЕСТИЛРУКИНАГРУДИИУЛЫБНУЛСЯКАКНАСТОЯЩИЙВОЛШЕБНИКВОТТОТОДУМАЛОНТОЛЬКОЯПРИКАЗАЛИВСЕПОВС
КАКАЛИВСЕЗАБЕГАЛИОТЛИЧНОЕБУДЕТЛЕТОИОННАПОСЛЕДОКОГЛЯДЕЛГОРОДИЩЕЛКНУЛЕМУПАЛЬЦАМИРАСПАХНУЛИСЬДВЕРИДОМОВЛЮДИВЫШЛИНАУЛИЦУЛЕТОТЫСЯЧАДЕВЯТЬСОТДВАДЦАТЬВОСЬ
МОГОГОДАНАЧАЛОСЬВТОУТРОПРОХОДЯПОЛУЖАЙКЕДУГЛАСНАТКНУЛСЯНАПАУТИНУНЕВИДИМАЯНИТЬКОСНУЛАСЬЕГОЛБАИНЕСЛЫШНОЛОПНУЛАИОТЭТОГОПУСТЯЧНОГОСЛУЧАЯОННАСТОРОЖИЛСЯДЕ
НЬБУДЕТНЕТАКОЙКАКВСЕНЕТАКОЙЕЩЕИПОТОМУЧТОБЫВАЮТДНИСОТКАННЫЕИЗОДНИХЗАПАХОВСЛОВНОВЕСЬМИРМОЖНОВТЯНУТЬНОСОМКАКВОЗДУХВДОХНУТЬИВЫДОХНУТЬТАКОБЯСНЯЛДУГЛАСУИ
ЕГОДЕСЯТИЛЕТНЕМУБРАТУТОМУОТЕЦКОГДАВЕЗИХВМАШИНЕЗАГОРОДАВДРУГИЕДНИГОВОРИЛЕЩЕОТЕЦМОЖНОУСЛЫШАТЬКАЖДЫЙГРОМИКАЖДЫЙШОРОХВСЕЛЕННОЙИНЫЕДНИХОРОШОПРОБОВАТЬНАВ
КУСАИНЫЕНАОЩУПЬАБЫВАЮТИТАКИЕКОГДАЕСТЬВСЕСРАЗУВОТНАПРИМЕРСЕГОДНЯПАХНЕТТАКБУДТОВОДНУНОЧЬТАМЗАХОЛМАМИНЕВЕСТЬОТКУДАВЗЯЛСЯОГРОМНЫЙФРУКТОВЫЙСАДИВСЕДОСАМО
ГОГОРИЗОНТАТАКИБЛАГОУХАЕТВВОЗДУХЕПАХНЕТДОЖДЕМНОНАНЕБЕНИОБЛАЧКАТОГОИГЛЯДИКТОТОНЕВЕДОМЫЙЗАХОХОЧЕТВЛЕСУНОПОКАТАМТИШИНАДУГЛАСВОВСЕГЛАЗАСМОТРЕЛНАПЛЫВУЩИ
ЕМИМОПОЛЯНЕТНИСАДОМНЕПАХНЕТНИДОЖДЕМДАИОТКУДАБЫРАЗНИЯБЛОНЬНЕТНИТУЧИКТОТАММОЖЕТХОХОТАТЬВЛЕСУАВСЕТАКИДУГЛАСВЗДРОГНУЛДЕНЬЭТОТКАКОЙТООСОБЕННЫЙМАШИНАОСТА
НОВИЛАСЬВСАМОМСЕРДЦЕТИХОГОЛЕСААНУРЕБЯТАНЕБАЛОВАТЬСЯОНИПОДТАЛКИВАЛИДРУГДРУГАЛОКТЯМИХОРОШОПАПАМАЛЬЧИКИВЫЛЕЗЛИИЗМАШИНЫЗАХВАТИЛИСИНИЕЖЕСТЯНЫЕВЕДРАИСОЙД
ЯСПУСТЫННОЙПРОСЕЛОЧНОЙДОРОГИПОГРУЗИЛИСЬВЗАПАХИЗЕМЛИВЛАЖНОЙОТНЕДАВНЕГОДОЖДЯИЩИТЕПЧЕЛСКАЗАЛОТЕЦОНИВСЕГДАВЬЮТСЯВОЗЛЕВИНОГРАДАКАКМАЛЬЧИШКИВОЗЛЕКУХНИДУГ
ЛАСДУГЛАСВСТРЕПЕНУЛСЯОПЯТЬВИТАЕШЬВОБЛАКАХСКАЗАЛОТЕЦСПУСТИСЬНАЗЕМЛЮПОЙДЕМСНАМИХОРОШОПАПАИОНИГУСЬКОМПОБРЕЛИПОЛЕСУВПЕРЕДИОТЕЦРОСЛЫЙИПЛЕЧИСТЫЙЗАНИМДУГЛ
АСАПОСЛЕДНИМСЕМЕНИЛКОРОТЫШКАТОМПОДНЯЛИСЬНАНЕВЫСОКИЙХОЛМИПОСМОТРЕЛИВДАЛЬВОНТАМУКАЗАЛПАЛЬЦЕМОТЕЦТАМОБИТАЮТОГРОМНЫЕПОЛЕТНЕМУТИХИЕВЕТРЫИНЕЗРИМЫЕПЛЫВУТВ
ЗЕЛЕНЫХГЛУБИНАХТОЧНОПРИЗРАЧНЫЕКИТЫДУГЛАСГЛЯНУЛВТУСТОРОНУНИЧЕГОНЕУВИДЕЛИПОЧУВСТВОВАЛСЕБЯОБМАНУТЫМОТЕЦКАКИДЕДУШКАВЕЧНОГОВОРИТЗАГАДКАМИИИВСЕТАКИДУГЛАС
ЗАТАИЛДЫХАНИЕИПРИСЛУШАЛСЯЧТОТОДОЛЖНОСЛУЧИТЬСЯПОДУМАЛОНЯУЖЗНАЮАВОТПАПОРОТНИКНАЗЫВАЕТСЯВЕНЕРИНВОЛОСОТЕЦНЕТОРОПЛИВОШАГАЛВПЕРЕДСИНЕЕВЕДРОПОЗВЯКИВАЛОУНЕ
ГОВРУКЕАЭТОЧУВСТВУЕТЕИОНКОВЫРНУЛЗЕМЛЮНОСКОМБАШМАКАМИЛЛИОНЫЛЕТКОПИЛСЯЭТОТПЕРЕГНОЙОСЕНЬЗАОСЕНЬЮПАДАЛИЛИСТЬЯПОКАЗЕМЛЯНЕСТАЛАТАКОЙМЯГКОЙУХТЫЯСТУПАЮКАКИ
НДЕЕЦСКАЗАЛТОМСОВСЕМНЕСЛЫШНОДУГЛАСПОТРОГАЛЗЕМЛЮНОНИЧЕГОНЕОЩУТИЛОНВСЕВРЕМЯНАСТОРОЖЕННОПРИСЛУШИВАЛСЯМЫОКРУЖЕНЫДУМАЛОНЧТОТОСЛУЧИТСЯНОЧТООНОСТАНОВИЛСЯВ
```

ЫХОДИЖЕГДЕТЫТАМЧТОТЫТАКОЕМЫСЛЕННОКРИЧАЛОНТОМИОТЕЦШЛИДАЛЬШЕПОТИХОЙПОДАТЛИВОЙЗЕМЛЕНАСВЕТЕНЕТКРУЖЕВАТОНЬШЕНЕГРОМКОСКАЗАЛОТЕЦИПОКАЗАЛРУКОЙВВЕРХГДЕЛИСТВ
АДЕРЕВЬЕВВПЛЕТАЛАСЬВНЕБОИЛИМОЖЕТБЫТЬНЕБОВПЛЕТАЛОСЬВЛИСТВУВСЕРАВНОУЛЫБНУЛСЯОТЕЦВСЕЭТОКРУЖЕВАЗЕЛЕНЫЕИГОЛУБЫЕВСМОТРИТЕСЬХОРОШЕНЬКОИУВИДИТЕЛЕСПЛЕТЕТИХС
ЛОВНОГУДЯЩИЙСТАНОКОТЕЦСТОЯЛУВЕРЕННОПОХОЗЯЙСКИИРАССКАЗЫВАЛИМВСЯКУЮВСЯЧИНУЛЕГКОИСВОБОДНОНЕВЫБИРАЯСЛОВЧАСТООНИСАМСМЕЯЛСЯСВОИМРАССКАЗАМИОТЭТОГООНИТЕКЛИ
ЕЩЕСВОБОДНЕЕХОРОШОПРИСЛУЧАЕПОСЛУШАТЬТИШИНУГОВОРИЛОНПОТОМУЧТОТОГДАУДАЕТСЯУСЛЫШАТЬКАКНОСИТСЯВВОЗДУХЕПЫЛЬЦАПОЛЕВЫХЦВЕТОВАВОЗДУХТАКИГУДИТПЧЕЛАМИДАДАТАК
ИГУДИТАВОТСЛЫШИТЕТАМЗАДЕРЕВЬЯМИВОДОПАДОМЛЬЕТСЯПТИЧЬЕЩЕБЕТАНЬЕВОТСЕЙЧАСДУМАЛДУГЛАСВОТОНОУЖЕБЛИЗКОАЯЕЩЕНЕВИЖУСОВСЕМБЛИЗКОРЯДОМДИКИЙВИНОГРАДСКАЗАЛОТЕЦ
НАМПОВЕЗЛОСМОТРИТЕКАНЕНАДОАХНУЛПРОСЕБЯДУГЛАСНОТОМИОТЕЦНАКЛОНИЛИСЬИПОГРУЗИЛИРУКИВШУРШАЩИЙКУСТЧАРЫРАССЕЯЛИСЬТОПУГАЮЩЕЕИГРОЗНОЕЧТОПОДКРАДЫВАЛОСЬБЛИЗИЛ
ОСЬГОТОВОБЫЛОРИНУТЬСЯИПОТРЯСТИЕГОДУШУИСЧЕЗЛООПУСТОШЕННЫЙРАСТЕРЯННЫЙДУГЛАСУПАЛНАКОЛЕНИПАЛЬЦЫЕГОУШЛИГЛУБОКОВЗЕЛЕНУЮТЕНЬИВЫНЫРНУЛИОБАГРЕННЫЕАЛЫМСОКОМС
ЛОВНООНВЗРЕЗАЛЛЕСНОЖОМИСУНУЛРУКИВОТКРЫТУЮРАНУМАЛЬЧИКИЗАВТРАКАТЬВЕДРАЧУТЬНЕДОВЕРХУНАПОЛНЕНЫДИКИМВИНОГРАДОМИЛЕСНОЙЗЕМЛЯНИКОЙВОКРУГГУДЯТПЧЕЛЫЭТОВОВСЕН
ЕПЧЕЛЫАЦЕЛЫЙМИРТИХОНЬКОМУРЛЫЧЕТСВОЮПЕСЕНКУГОВОРИТОТЕЦАОНИСИДЯТНАЗАМШЕЛОМСТВОЛЕУПАВШЕГОДЕРЕВАЖУЮТСАНДВИЧИИПЫТАЮТСЯСЛУШАТЬЛЕСКАКСЛУШАЕТОНОТЕЦЧУТЬПОСМ
ЕИВАЯСЬИСКОСАПОГЛЯДЫВАЕТНАДУГЛАСАХОТЕЛБЫЛОЧТОТОСКАЗАТЬНОПРОМОЛЧАЛОТКУСИЛЕЩЕКУСОКСАНДВИЧАИЗАДУМАЛСЯХЛЕБСВЕТЧИНОЙВЛЕСУНЕТОЧТОДОМАВКУССОВСЕМДРУГОЙВЕРН
ООСТРЕЕЧТОЛИМЯТОЙОТДАЕТСМОЛОЙАУЖАППЕТИТКАКРАЗЫГРЫВАЕТСЯДУГЛАСПЕРЕСТАЛЖЕВАТЬИПОТРОГАЛЯЗЫКОМХЛЕБИВЕТЧИНУНЕТНЕТОБЫКНОВЕННЫЙСАНДВИЧТОМКИВНУЛПРОДОЛЖАЯЖЕ
ВАТЬЯПОНИМАЮПАПВЕДЬУЖЕПОЧТИСЛУЧИЛОСЬДУМАЕТДУГЛАСНЕЗНАЮЧТОЭТОНООНОБОЛЬШУЩЕЕПРЯМОГРОМАДНОЕЧТОТОЕГОСПУГНУЛОГДЕЖЕОНОТЕПЕРЬОПЯТЬУШЛОВТОТКУСТНЕТГДЕТОЗАМН
ОЙНЕТНЕТЗДЕСЬТУТРЯДОМДУГЛАСИСПОДТИШКАПОЩУПАЛСВОЙЖИВОТОНОЕЩЕВЕРНЕТСЯНАДОТОЛЬКОНЕМНОЖКОПОДОЖДАТЬБОЛЬНОНЕБУДЕТЯУЖЗНАЮНЕЗАТЕМОНОКОМНЕПРИДЕТНОЗАЧЕМЖЕЗАЧ
ЕМА