КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

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 шифртексту (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 (1).

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

1. Зберегли потрібні дані, тобто зашифрований текст.

2. Створили код, який реалізує пошук оберненого числа, та розширений алгоритм Евкліда.

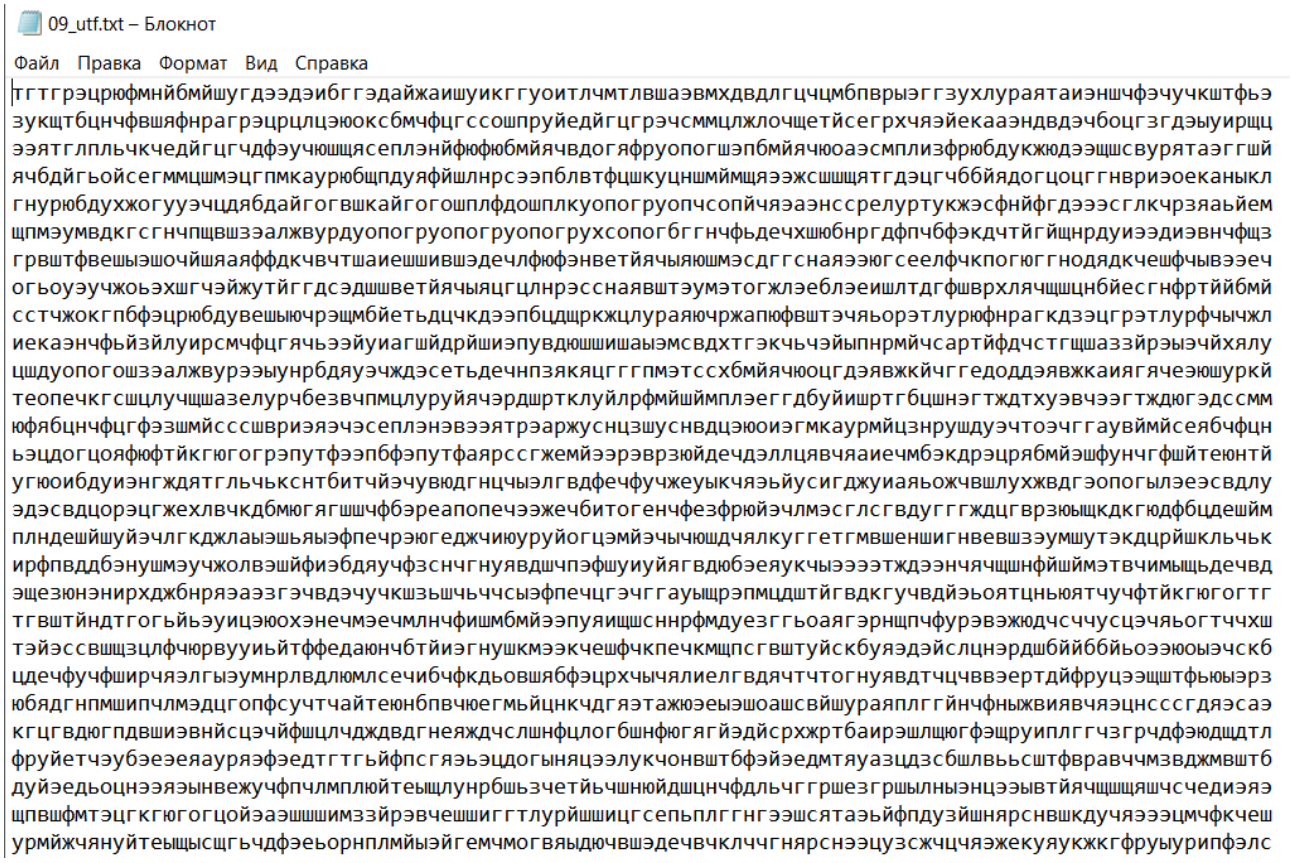
3. Порахували біграми в шифрованому тексті

4. Користуючись результатами пунктів 2 і 3, дібрали кілька можливих ключів за допомогою ідей частотного криптоаналізу

5. Автоматично прибрали серед кандидатів на відкритий текст ті, які мали в собі заборонені біграми, такі як 'аь', 'ьь', 'ыы', 'ыь'. В російській мові таких біграм не існує. Тому якщо деякий текст їх має, то він російською мовою не є.

Вхідні дані

1. Наш варіант тексту (файли: 09.txt і 09_utf.txt)


09_utf.txt – Блокнот

Файл Правка Формат Вид Справка

тгтгрэцрюфмнйбмйшугдээдэибггэдайжаишуикггуоитлчмтлвшаэвмхдвдлгцччцмбпврыэггзухлураятаиэншчфэчучкштфьэ
зукщтбцнчфвшяфнрагрэцрцлцэюоксбмчфцгссошпруйедйгцгрэчсммцлжлочщетйсегрхчяэйекааэндвдэчбоцгзгдэыуирщц
ээятглпльчкчедйгцгчдфэучюшщясеплэнйфюфюбмйячвдогяфруопогшэпбмйячюоаэсмплизфрюбдукжюдээщшсвурятаэггшй
ячбдйгьойсегммцшмэцгпмкаурюбщпдуяфйшлнрсээпблвтфцшкуцншймщяээжсшшщятгдэцгчббйядогцоцггнвриэоеканыкл
гнурюбдухжогууэчцдябдайгогвшкайгогошплфдошплкуопогруопчсопйчяэаэнссрелуртукжэсфнйфгдэээсглкчрзяаьйем
щпмэумвдкгсгнчпщвшээалжвурдуопогруопогруопогрухсопогбггнчфьдечхшюбнргдфпчбфэкдчтйгйщнрдуиээдиэвнчфщз
грвштфвешыэшочйшяаяффдкчвчтшаиешшившэдечлфюфэнветйячыяюшмэсдггснаяээюгсеелфчкпогюггнодядкчешфчывээеч
огьоуэучжоьэхшгчэйжутйггдсэдшшветйячыяцгцлнрэсснаявштэумэтогжлэеблэеишлтдгфшврхлячщшцнбйесгнфртййбмй
сстчжокгпбфэцрюбдувешыючрэщмбйетьдцчкдээпбцдщркжцлураяючржапюфвштэчяьорэтлурюфнрагкдзэцгрэтлурфчычжл
иекаэнчфьйзйлуирсмчфцгячьээйуиагшйдрйшиэпувдюшшишаыэмсвдхтгэкчьчэйыпнрмйчсартйфдчстгщшаззйрэыэчйхялу
цшдуопогошээалжвурээыунрбдяуэчждэсетьдечнпзякяцгггпмэтссхбмйячюоцгдэявжкйчггедоддэявжкаиягячеэюшуркй
теопечкгсшцлучщшазелурчбезвчпмцлуруйячэрдшртклуйлрфмйшймплэеггдбуйишртгбцшнэгтждтхуэвчээгтждюгэдссмм
юфябцнчфцгфэзшмйсссшвриэяэчэсеплэнэвээятрэаржуснцзшуснвдцэюоиэгмкаурмйцзнрушдуэчтоэчггаувймйсеябчфцн
ьэцдогцояфюфтйкгюгогрэпутфээпбфэпутфаярссгжемйээрэврзюйдечдэллцявчяаиечмбэкдрэцрябмйэшфунчгфшйтеюнтй
угюоибдуиэнгждятгльчькснтбитчйэчувюдгнцчыэлгвдфечфучжеуыкчяэьйусигджуиаяьожчвшлухжвдгэопогылэеэсвдлу
эдэсвдцорэцгжехлвчкдбмюгягшшчфбэреапопечээжечбитогенчфезфрюйэчлмэсглсгвдугггждцгврзюыщкдкгюдфбцдешйм
плндешйшуйэчлгкджлаыэшьяыэфпечрэюгеджчиюруйогцэмйэчычюшдчялкуггетгмвшеншигнвевшзэумшутэкдцрйшкльчьк
ирфпвддбэнушмэучжолвэшйфиэбдяучфзснчгнуявдшчпэфшуиуйягвдюбэеяукчыээээтждээнчячщшнфйшймэтвчимыщьдечвд
эщезюнэнирхджбнряэаэзгэчвдэчучкшзьшчьччсыэфпечцгэчггауыщрэпмцдштйгвдкгучвдйэьоятцньюятчучфтйкгюгогтг
тгвштйндтгогьйьэуицэюохэнечмэечмлнчфишмбмйээпуяищшсннрфмдуезггьоаягэрнщпчфурэвэжюдчсччусцэчяьогтччхш
тэйэссвшщзцлфчюрвууиьйтффедаюнчбтйиэгнушкмээкчешфчкпечкмщпсгвштуйскбуяэдэйслцнэрдшбййббйьоээюоыэчскб
цдечфучфширчяэлгыэумнрлвдлюмлсечибчфкдьовшябфэцрхчычялиелгвдячтчтогнуявдтчцчввэертдйфруцээщштфыюыэрз
юбядгнпмшипчлмэдцгопфсучтчайтеюнбпвчюегмьйцнкчдгяэтажюэеыэшоашсвйшураяплггйнчфныжвиявчяэцнсссгдяэсаэ
кгцгвдюгпдвшиэвнйсцэчйфшцлчджвдгнеяждчслшнфцлогбшнфюгягйэдйсрхжртбаирэшлщюгфэщруиплггчзгрчдфэюдщдтл
фруйетчэубэеэеяауряэфэедтгтгьйфпсгяэьэцдогыняцээлукчонвштбфэйэедмтяуазцдзсбшлвььсштфвравччмзвджмвштб
дуйэедьоцнээяэынвежучфпчлмплюйтеыщлунрбшьзчетйьчшнюйдшцнчфдльчггршезгршылныэнцээывтйячщшщяшчсчедиэяэ
щпвшфмтэцгкгюгогцойэаэшшшимззйрэвечешигртлурйшшицгсепьплггнгээшсятаэьйфпдузйшнярснвшкдучяэээцмчфкчеш
урмйжчянуйтеыщысщгьчдфэеьорнплмйыэйгемчмогвяыдючвшэдечвчклччгнярснээцузсжчцчяэжекуякжкгфруыурипфэлс

Рис 1. Фрагмент шифрованого тексту

1.1. Найчастіші біграми шифротексту: 'ээ', 'вд', 'чф', 'цг', 'гн'.

2. Найчастіші біграми російської мови - "ст", "но", "то", "на", "ен" (із методичних вказівок).

Вихідні дані:

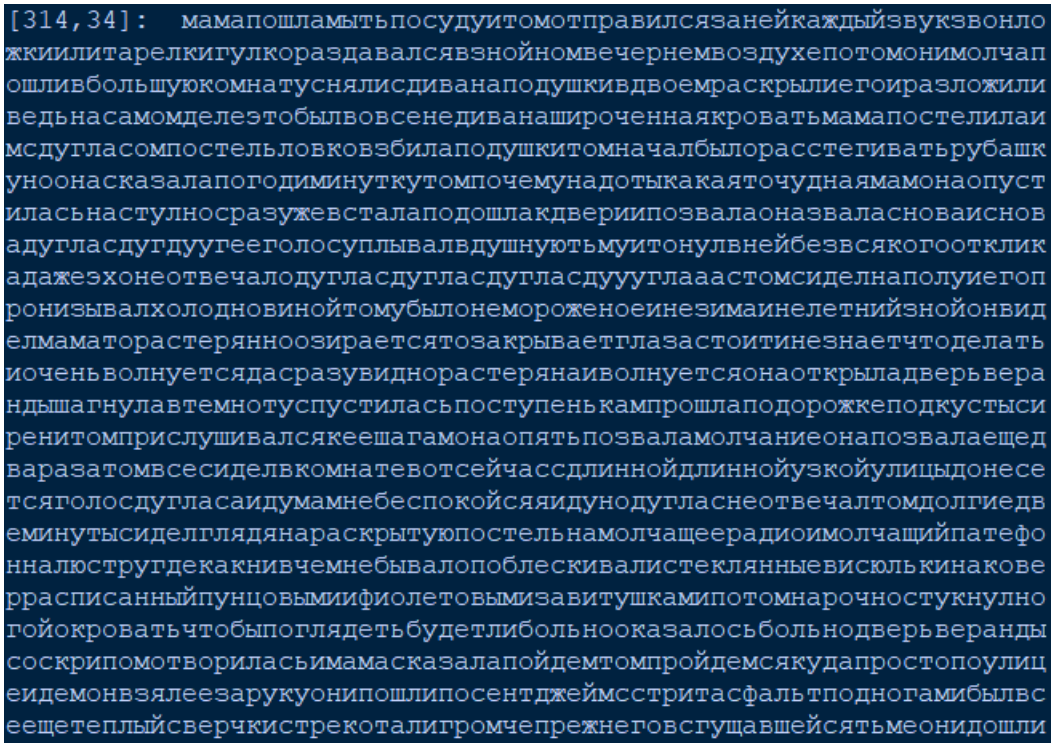


Рис 2. Ключ і фрагмент відкритого тексту

Висновки:

Афінний шифр, хоч і не потребує просунутої статистики на кшталт індексу відповідності, як шифр Віженера, замість цього потребує більш просунутої модулярної арифметики. Але врахувавши теоретичні особливості шифру та його математичної бази, в нас вийшло створити код, який атакує цей шифр цілком автоматично.