Міністерсво освіти і науки України
Національний технічний університет України
Київський політехнічний інститут імені Ігоря Сікорського
Навчально-науковий фізико-технічний інститут

Симетрична криптографія
Комп’ютерний практикум №3

Криптоаналіз афінної біграмної підстановки

Виконали:
Медведцький Костянтин ФІ-04
Сковрон Роман ФІ-04

Київ 2023

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

Порядок виконання роботи
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 шифротексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).
4. Для кожного кандидата на ключ дешифрувати шифротекст. Якщо шифротекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним. У разі необхідності змінити кодування алфавіту (див. методичні вказівки).

Результати
Ключ та І дешифрованого тексту:

```
0.05005695909973544: [703, 956]
0.045893691994113986: [258, 109]
0.041817003942862446: [746, 934]
0.04074456492258953: [50, 71]
0.040729416135516575: [298, 412]
0.040724423149642724: [935, 215]
0.04065781603876812: [928, 497]
0.04052735305413305: [265, 781]
0.04034977937965446: [291, 740]
0.04029747190859536: [22, 561]
```

Звідси можемо бачити, що наш ключ (703, 956)

Дешифрований текст:
хорошосэрбиллнехотясунулденыаивкаршгнвотчтобиллвьпростопосеехеэту
новуюправукбасгнибудывдругойразчгктолыкояпомрунадругойжедвнымсже
теперекопатыэтучертовулужайкунучгкхпгтитупгстерпенияподсжсгтыещел
етпятышестычтобьстаряйболтунуспелотдатыконцьужбудыхеувервньподсж
дусказалбиллягмнезыгюкакпгмобяснитынодляменяжужжаныеэтойкосилкл
самаятрекюгснаямелодиянасвехеенейвсяпрелестылетабезнееябьужаснотос
ковалибезфгэгггсвежескошеннойправьтсжебиллнтануисяиподнялсземлико
рзинкуяпошелковртаувьсшгеняйюношгивсепонимаехеяуверенизвасполучи
тсяблестящийиумняйрепортерсказалдедушкапомбааяемцподнятыкорзинку
явамэтопредсчгзьпгюпрошлоупронаступилполденыпослеобесгдедушкапод
няисяксебенемнбаопочиталуиттиеюгикрепкоуснулкогдаонпроснулсябьлоп
ричасавокыгвлевалсяяркийивесельйсолнечняйсветдедушкалежалвкропгтие
вдржавздрбануислуугйкидоносилосыпрежнеезнакомоенефгбьпгемоежужж
аныечтоэтосказалонктотокоситправуноведыеетолыкосчаодняутромскосили
онещепослужглдаконечноэтсжужжиткосилчгмернонеутомимодедушкавоал
янулвокнохгхнулсгведыэтобиллэйбиллфоресхервамчтосолкцеусгрилофаол
овувькоситеужескошвннуютюгвубиллподнялголовутростодушноульбнулся
ипомахалрукойзыгюнокажетсяутромяюгбоаглнеоченычистодедушчгещедо
брьхпятыминутнежиисявкроватиислицаегонеоходилэульбкнгбиллфорестер
всештаалскосилкойнасиверыгвостокыграинаконецыгфгэгдиизподкосилкив
еселобилдушлстьйзелвняйфонтанввоскресвныеутромлеоэуфманбродилпос
воемургюгжусловносжидаячтокакоенибудыполеновитокпроволокимолоток
илиргечньйключподтроанетифгкричитыгчнлсменяноничтонеподтроаевало
ничтонетросилосывыгеглочгчгяоыгдолжыгбтыэтамашинасегстыядущглле
оможетоыгдолжыгумещатысявчгрманеилионадолжнатебясамбаоноситывчг
рманеодноязнаютвердосказалонвслухоыгдолжыгбтыяркойлеопоставилыгв
ерсагкбанкуоранжевойкюгскевзяислопгуыипобрелвдомлинаонзталянулвто
лковяйсловарытьдоволынаспокойнавеселаввосторгехебевовсемвезетивсеус
гетсяпотвоемувсеидепразумнохорошоиуспешнолиыгпересталарезатюов

Висновки

У цій лабораторній роботі ми навчились ламати шифр афінної підстановки. Не знаю що тут ще можна написати…