НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. СІКОРСЬКОГО»

НН ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3 З ПРЕДМЕТУ «СИМЕТРИЧНА КРИПТОГРАФІЯ»

«КРИПТОАНАЛІЗ АФІННОЇ БІГРАМНОЇ ПІДСТАНОВКИ»

Виконали:

ФІ-04 Коваль Марія

ФІ-04 Недашківський Іван

Перевіряв:

Чорний О.М.

Мета комп`ютерного практикуму

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

Постановка задачі та варіант завдання

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).

З методичними рекомендаціями були ознайомлені, усі додаткові вказівки виконали. Варіант виконаної роботи - №7.

Хід роботи, опис труднощів, що виникали, та шляхів їх розв'язання

Завдання великих труднощів не викликали. Найскладнішою частиною було побудувати розшифровку для тексту.

Нижче будуть наведені усі результати роботи.

5 найчастіших біграм у шифротексті нашого варіанту:

```
['цл', 'ял', 'ае', 'ле', 'чо']
```

Після проведення усіх дій зі знаходженням ключа, розшифруванням шифротексту тощо, ми отримали велику кількість ключів, що теоретично підходять під наш текст, через що виникла необхідність у прописуванні автоматичного розпізнавача для російської мови, тобто відсіювача попередньо неправильних ключів. Для цього ми застосували 4 властивості та за цими критеріями відсіювали ключі. По-перше, ми перевіряли на найчастіші та найрідші літери. Якщо з 5-ти найчастіших літер мови хоча б 4 будуть присутні у найчастіших літерах розшифрованого тексту, то він пройшов перевірку. І дзеркально, якщо хоча б одна найрідша літера присутня у найчастіших – він не пройшов перевірку. Окрім того, ми додали

критерій перевірки на частоти біграм на перетинах. Якщо на перетинах хоча б 2 з 5 найчастіших біграм також повторяться, то текст пройшов перевірку. Цих трьох факторів було достатньо, щоб отримати остаточну відповідь, однак, слід зазначити, що ми додали четвертий критерій індексу відповідності з 2-ї лабораторної, який самостійно приходив майже до остаточної відповіді, лишаючи після себе доступними лише 2 підходящі ключі, один з яких виявився правильним. Тому теоретично, можна було б обійтись і без інших критеріїв.

Значення ключа для нашого варіанту: `[(200, 900)]` , де a=200, b=900

Нижче приведено невеличкий фрагмент шифрованого тексту та результат його розшифрування віднайденим ключем.

хетжщбеыжцллйшллебторюкечожлхуемебсфбпвгщпсакюбизыщллбющцжбщвлвачоофлеы мюэвцфйжлцщвлиффечозуазщмвьпфйбсфашазлевлазлевлыюфйгблфубфефцинютошрлбыцц ошшйьтоющцхоаимжоцллйшллебктяфлеьабуазгбшйьтошюййчажофщйленефцинебгбгугф язащзещбйяхенефцинебуццбхнюеоиццсфоэбохзьтяфебчфкеаесачсюэбнцдвцпащйлежцаечйх цусфююю

атызнаешьсколькоразмывэтомгодуиграливбейсболавпрошломавпозапрошломнистогониссег оспросилтомгубыегодвигалисьбыстробыстроявсезаписалтысячпятьсотшестьдесятвосемь разасколькоразячистилзубызадесятьлетжизнишестьтысячразарукимылпятнадцатьтыся чразспалчетыреслишнимтысячиразиэтотольконочьюиселшестьсотперсиковивосемьсотяб локагрушвсегодвести

Висновки

Під час виконання практикуму ми засвоїли деякі методи опанували та використали деякі прийоми модулярної арифметики, а також набули нових навичок частотного аналізу, працюючи з розкриттям моноалфавітних підстановок. Ми ближче познайомились з біграмами афінного шифру, дізнались, яким чином вони шифруються, чому такий шифр буде коректним, а також змогли розшифрувати на обрати потрібний варіант розшифровки такого шифру. Враховуючи моноалфавітність даного шифру, він все ще є доволі легким для зламування, однак, для цього нам довелось використати деякі властивості мови.