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

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали:
ФБ-21 Редько-Шпак Р.А.
ФБ-21 Серяков В.Л.

Мета роботи

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

Порядок виконання роботи

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 (додаток №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 (a,b) 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.

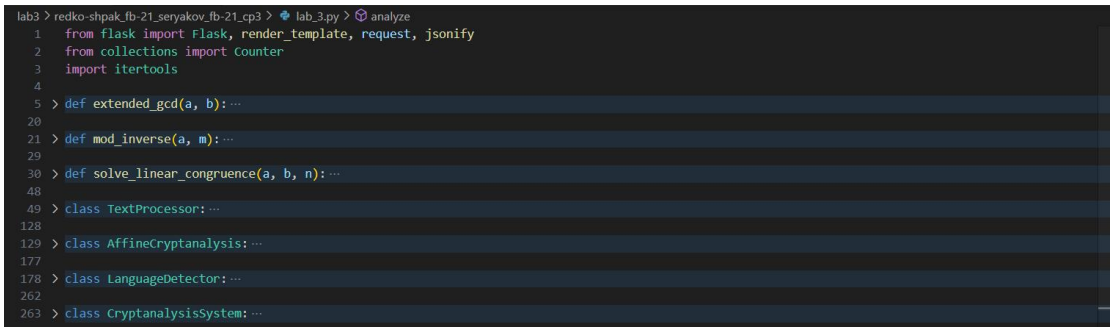
Хід роботи

Афінний шифр біграмної заміни

Афінна підстановка біграм - це криптографічне перетворення, де:

- Текст розбивається на пари символів (біграми)
- Кожній біграмі (x_1, x_2) відповідає число $X = x_1m + x_2$, де m - розмір алфавіту
- Шифрування відбувається за формулою: $Y = (aX + b) \bmod m^2$
- Дешифрування відбувається за формулою: : $X = a^{-1}(Y - b) \bmod m^2$
- Ключ складається з пари чисел (a,b)

Програма складається з наступних основних класів:



- ✧ **Математичні ф-ії - включає:**
  - ✓ Розширений алгоритм Евкліда
  - ✓ Обчислення оберненого елемента
  - ✓ Розв'язання лінійних порівнянь
- ✧ **TextProcessor** - обробка тексту та робота з біграмами
  - ✓ обробляє рос алфавіт (31 буква)
  - ✓ виконує конвертацію між текстом і числами (згідно з формулами з методички)
  - ✓ дозволяє аналізувати як перетинаючі, так і неперетинаючі біграми - має метод для генерації пар біграм
- ✧ **AffineCryptanalysis** - реалізація шифрування/дешифрування
  - ✓ encrypt_bigram/decrypt_bigram для роботи з окремими біграмами

- ✓ find_possible_keys для пошуку можливих ключів за парою біграм
- ✓ encrypt_text/decrypt_text для роботи з повними текстами

Як це працює?

- ✓ Шифрування: Y = (aX + b) mod m^2
- ✓ Дешифрування: X = a^(-1)(Y - b) mod m^2
- ✓ Пошук ключів: через розв'язання системи рівнянь

✧ **LanguageDetector** - визначення осмисленості тексту

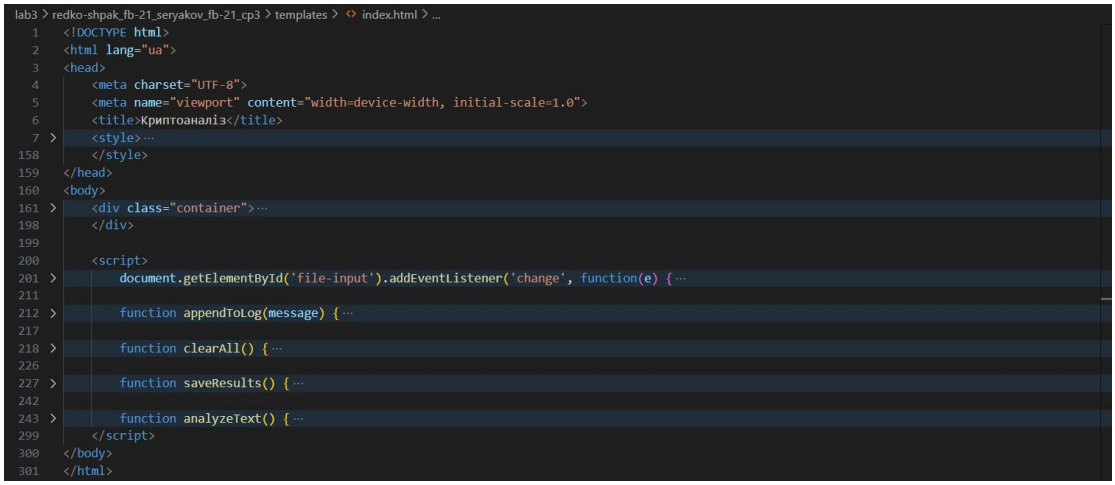
- ✓ перевіряє частоти частих літер ('о', 'е', 'а')
- ✓ перевіряє частоти рідких літер ('ф', 'щ', 'ь')
- ✓ перевіряє заборонені біграми
- ✓ перевіряє частоти найбільш поширених біграм
- ✓ має налаштовані порогові значення для кожного з критеріїв
- ✓ має комплексний метод is_meaningful_text(), який комбінує всі критерії

✧ **CryptanalysisSystem** - основний клас аналізу

- ✓ зчитує та фільтрує текст
- ✓ знаходить найчастіші біграми
- ✓ перебирає варіанти співставлення біграм
- ✓ далі знаходить можливі ключі
- ✓ пробує дешифрувати та перевіряє змістовність тексту
- ✓ в кінці виводить весь результат

Також, для графічного інтерфейсу була використана бібліотека Flask.

Та відовідно був написаний **html+css** код:

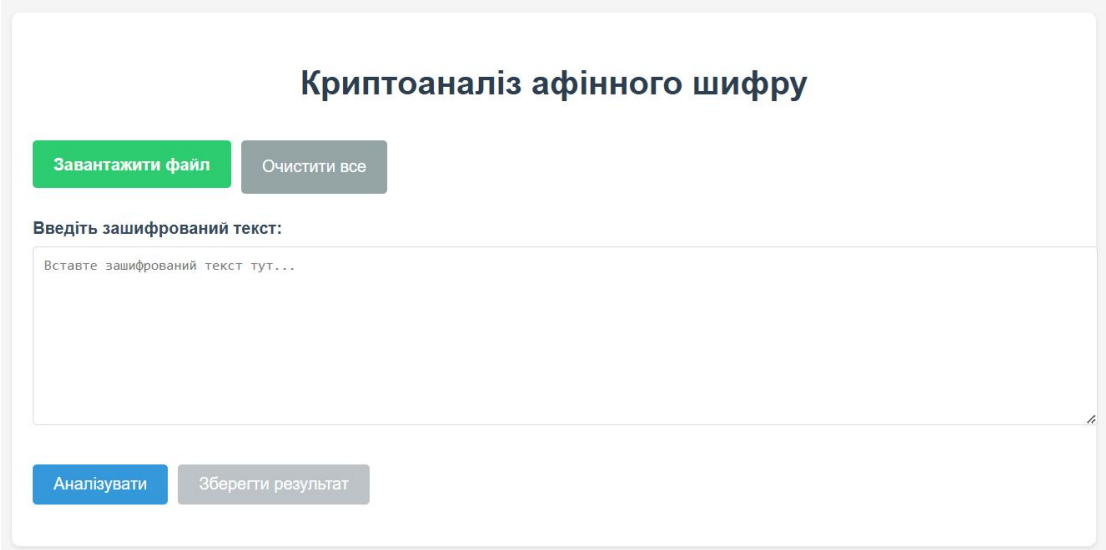


Принцип роботи афінного шифру біграмної заміни

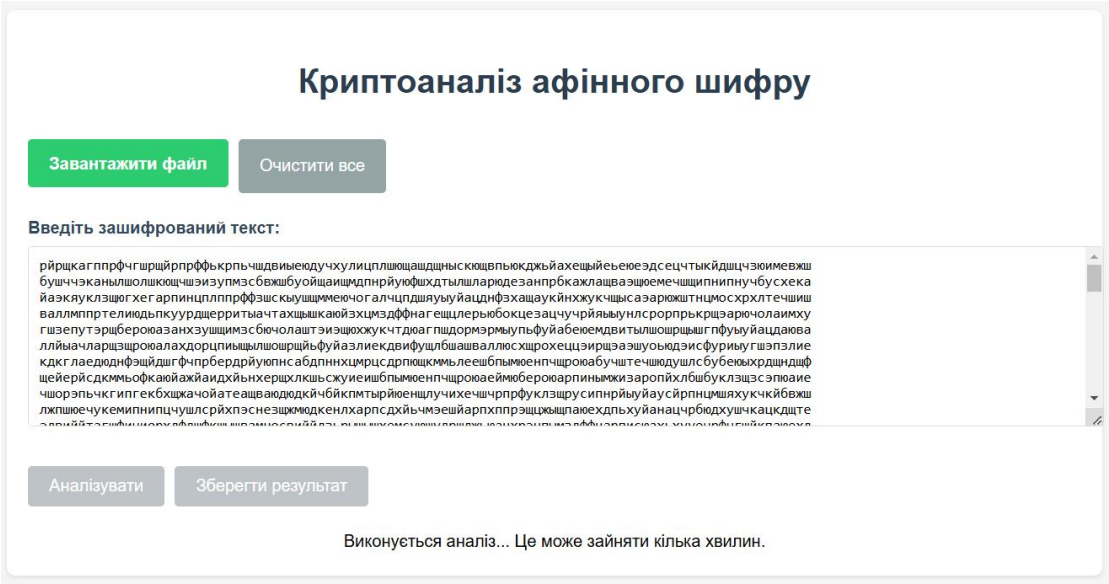
Текст розбивається на пари символів (біграми). Далі кожна біграма (x_1, x_2) перетворюється в число $X = x_1m + x_2$, де m - розмір алфавіту (31 для російської мови). До числа X застосовується афінне перетворення: $Y = (aX + b) \bmod m^2$. Отримане число Y знову розбивається на пару символів шифротексту

Демонстрація роботи:

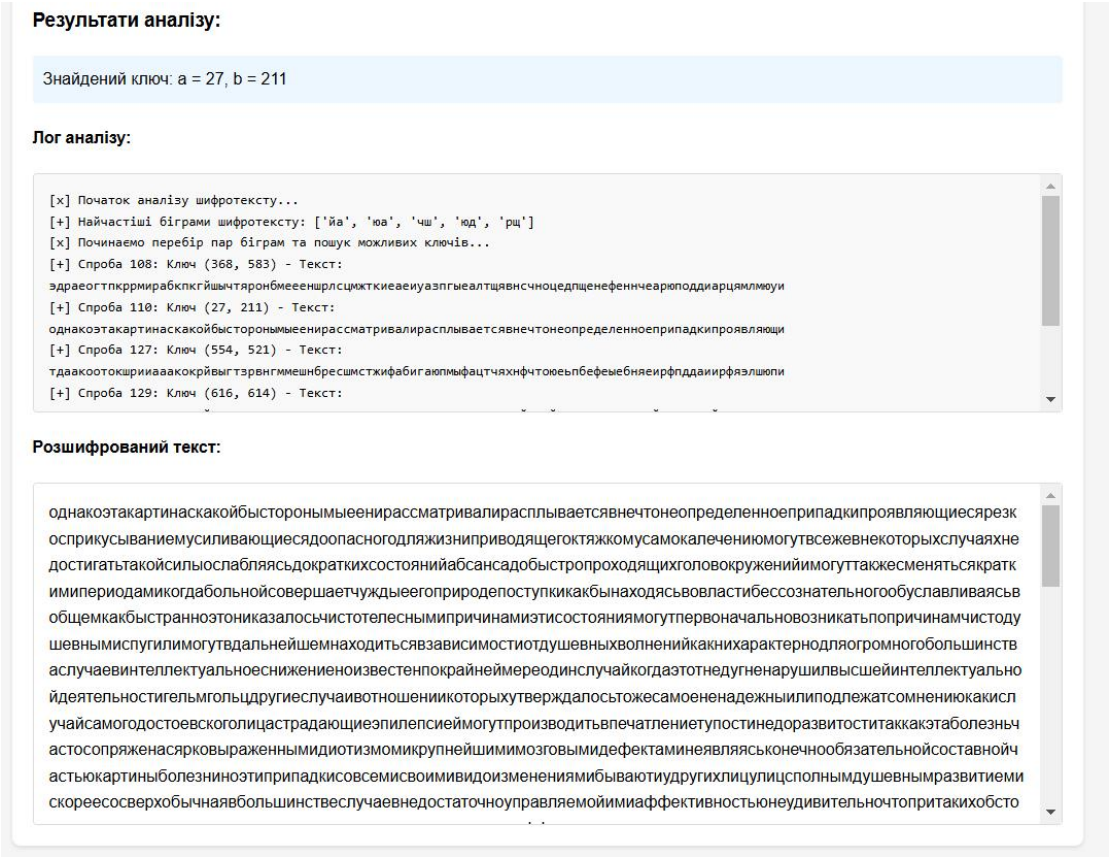
Наша програма має наступний вигляд при запуску:



Ми можемо або вручну написати/вставити зашифрований текст або використати завантаження. Використаю другий варіант, завантажу наш варіант **(варіант №2)** та запущу аналіз:



Результат:



Також проскролю лог:

Лог аналізу:

```
[+] Спроба 110: Ключ (27, 211) - Текст:
однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноеприпадкипроявляющи
[+] Спроба 127: Ключ (554, 521) - Текст:
тдаакоотокшрииааакокрйвыгтзрвнгммешнбресшмстжифабигаюпмыфацтчяхнфчтоюеьпбефеыебняеирфпддаиирфяэлшюпи
[+] Спроба 129: Ключ (616, 614) - Текст:
ндшакортмкщреишаюкмкюйшыетирснвмчеинврцсчмутгинаюиыаопгынаштаяенйчтойелпмеаезернкейрепядэийрэяллрюми
[+] Спроба 138: Ключ (895, 552) - Текст:
ждиакощтгкорзииафкгккйяыотэрзннмьеюнцрхсгмэтеиэааилашпйыэавтеяьнжчтомехппегекежннеюрппчдяиюрвямллюои

[✓] Знайдено успішний розшифрований текст після 219 спроб.
```

Перевірка збереження в файл:

cryptanalysis_results.txt: Блокнот

Файл Редагування Формат Вигляд Довідка

```
Результати криптоаналізу

Знайдений ключ: a = 27, b = 211

Лог аналізу:
[x] Початок аналізу шифротексту...
[+] Найчастіші біграми шифротексту: ['йа', 'юа', 'чш', 'юд', 'рщ']
[x] Починаємо перебір пар біграм та пошук можливих ключів...
[+] Спроба 108: Ключ (368, 583) - Текст: эдраеогтпкррмирабкпкгйшычтяронбмееенш рлсцмжткиеае
[+] Спроба 110: Ключ (27, 211) - Текст: однакоэтакартинаскакойбысторонымыеенирассматривали
[+] Спроба 127: Ключ (554, 521) - Текст: тдаакоотокшрииааакокрйвыгтзрвнгммешнбресшмстжифаб
[+] Спроба 129: Ключ (616, 614) - Текст: ндшакортмкщреишаюкмкюйшыетирснвмчеинврцсчмутгинаю
[+] Спроба 138: Ключ (895, 552) - Текст: ждиакощтгкорзииафкгккйяыотэрзннмьеюнцрхсгмэтеиэаа

[✓] Знайдено успішний розшифрований текст після 219 спроб.


Розшифрований текст:
однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноеприпадки
мимозговымидефектаминеявляяськонечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадки
когоотводараздраженияэпилептическаяреакциякаковыменемможноназватьвсеэтовместевзятоенесом
едположениечтоприпадкиначалисьудостоевскогоужевдетствечтоонивначалехарактеризовалисьболеес
былещемальчикомкаквнезапнаябезотчетнаяподавленностьчувствокаконпозжерассказывалсвоемудругу
```

Рд 1, ствп 1 | 100% | UNIX (LF) | UTF-8

З виводу програми бачимо:

Знайдені найчастіші біграми шифротексту: ['йа', 'юа', 'чш', 'юд', 'рщ']

Програма виконала 219 спроб підбору ключа

Успішний ключ був знайдений: **a = 27, b = 211**

Початок розшифрованого тексту: **"однакоэтакартина..."**

Правильність розшифрування підтверджується:

Наявністю осмислених слів, відповідністю статистичних характеристик тексту російській мові та проходженням всіх критеріїв автоматичного розпізнавання.

Висновки

В результаті виконання лабораторної роботи реалізовано повний цикл криптоаналізу афінного шифру біграмної заміни. Використано частотний аналіз для знаходження можливих ключів та створено ефективний автоматичний розпізнавач осмисленого тексту.

Наша програма успішно знаходить правильний ключ та розшифровує текст.