НТУУ «Київський політехнічний інститут ім. Ігоря Сікорського»

Навчально-науковий Фізико-технічний інститут

# Криптографія

Комп’ютерний практикум №3

Варіант №6

Виконали:

Студенти 3 курсу НН ФТІ

групи ФБ-31

Гаврилюк Володимир

Гек Роман

**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 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 ) , ( ba 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.

## Виконання

Для основного скрипта lab3.py були написані допоміжні і критично важливі модулі text_analyzer.py та modular_math.py

modular_math потрібен для математичних функцій, таких як розширений алгоритм евкліда, пошук оберненого за модулем, розв'язок рівнянь.

В text_analyzer реалізована очистка шифротексту, підрахування частот монограм, біграм (з перетином для оцінки якості тексту, без перетину для дешифрування), підрахунок ентропії (для оцінки якості тексту) тощо.
В цьому модулі найголовніша функція – це функція оцінки якості

Вона враховує декілька критеріїв для перевірки:
1. Ентропія монограм, і якщо ентропія в межах норм російської мови, то збільшуємо оцінку.

2. Ентропія біграм, і аналогічно додаємо бали, якщо вона в нормі

3. Сума найчастіших і найрідших букв російської мови. Аналогічно додаємо бали, якщо найчастіших багато і найрідших мало

4. Подвоєння: у випадковому тексті їх мало, у мові їх більше

Суть атаки на шифр полягає в тому, що афінний шифр – це лише математична заміна. Вона не заховає статистику мови при шифруванні. Якщо найчастіша біграма в російський мові "ст", то при шифруванні вона перетвориться на якусь іншу, наприклад "ще" або ще щось.

У нашому шифротексті найчастіші біграми були такі:

```
Топ-5 найчастіших біграм у шифртексті:
  1. 'ще' - 0.0133 (46 разів)
  2. 'хе' - 0.0127 (44 разів)
  3. 'чв' - 0.0122 (42 разів)
  4. 'ле' - 0.0116 (40 разів)
  5. 'цв' - 0.0110 (38 разів)
```

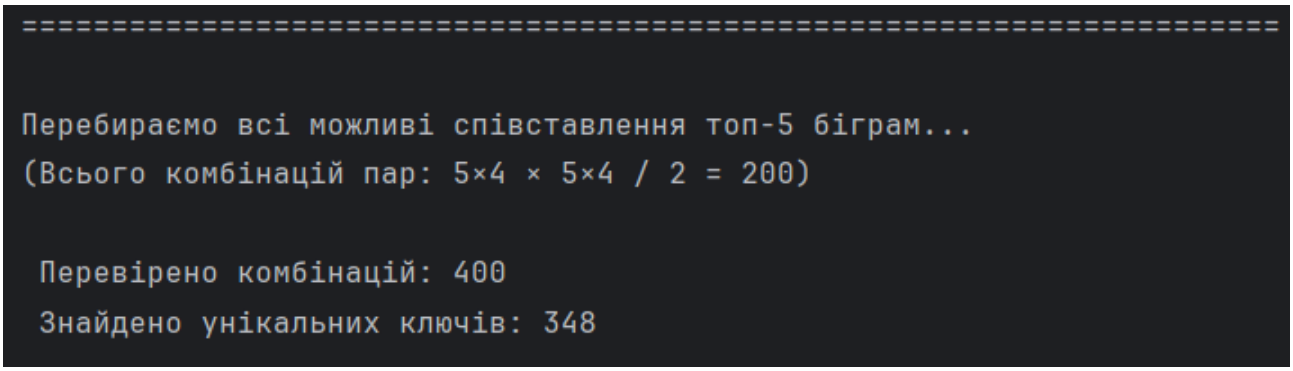
Генерація ключів відбувається шляхом побудови гіпотез. Ми не можемо точно знати в яку шифро-біграму перетворилася початкова, чиста біграма.

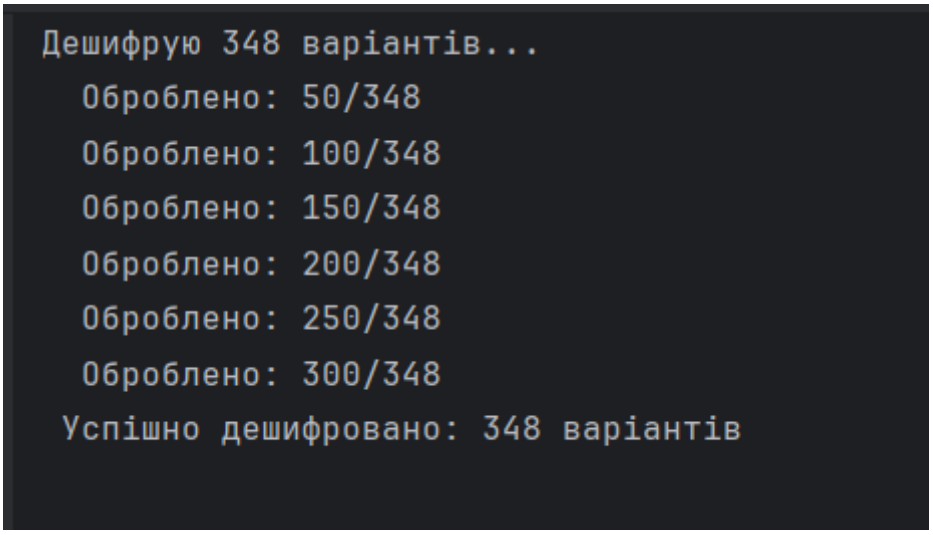
Для генерації ключа ми складаємо систему з двох рівнянь і віднімаємо від першого друге, щоби зникло b

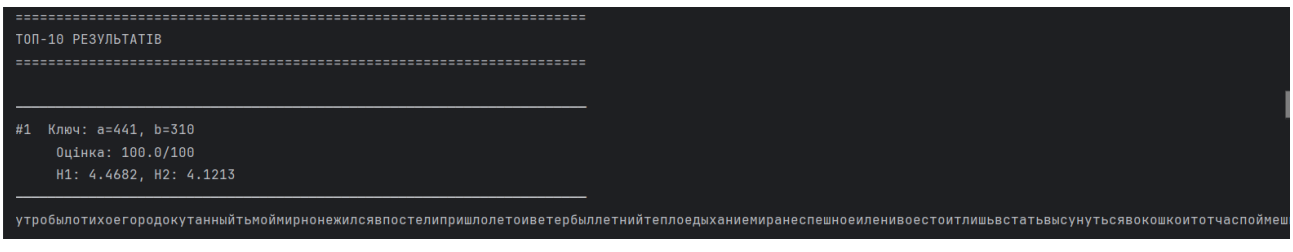
$$Y_1 = (aX_1 + b)\ mod\ m^2$$
$$Y_2 = (aX_2 + b)\ mod\ m^2$$

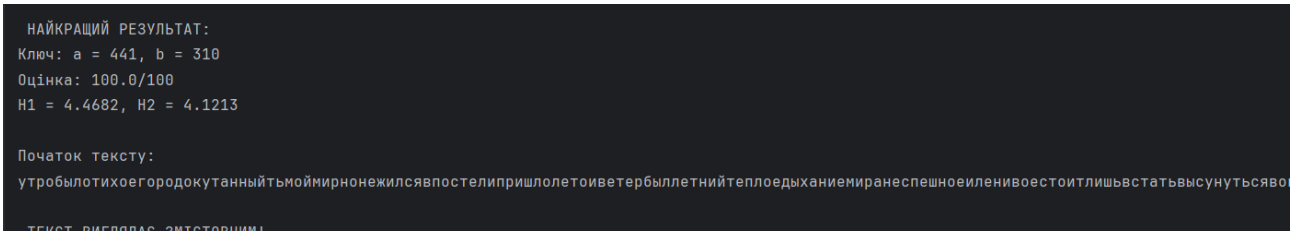
$$(Y_1 - Y_2) = a\ (X_1 - X_2)\ mod\ m^2$$

Тепер ми маємо лінійне рівняння для знаходження a, і коли його знайдемо, то b обрахується простою підстановкою



Утробылотихоегородокутанныйтьмоймирнонежилсявпостелипришлолетои ветербыллетнийтеплоедыханиемиранеспешноеиленивоестоитлишьвстатьв ысунутьсявокошкоитотчаспоймешьвотонаначинаетсянастоящаясвободаи жизньвотонопервоеутролетадуглассполдингдвенадцатилетотродутолькочт ооткрылглазаикаквтеплуюречкупогрузилсявпредр

**Висновок**

У цій лабораторній роботі ми успішно зламали афінний біграмний шифр. Ми довели на практиці, що статистика при такому шифруванні нікуди не поділася, і за допомогою неї можна успішно дешифрувати повідомлення.

Ми припустили, що на великому тексті для дешифрування буде достатньо п’яти найчастіших біграм, щоб хоча би дві з них співпали з еталонними й дали правильну систему рівнянь для знаходження ключа.