

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

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки
Варіант - 10

Виконали:
Студенти групи ФБ-35
Кохта Андрій, Церман Марія, Ворона Сергій

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

Постановка задачі: 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 (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.

Текст до очищення:

```
юммутмкйсйумтцбишчоцхйнкхйяхклзкургтвдньлмгсбтмейашрэлшоэгклсмтцэлжфбтдлычтфяляунгфищйээргчсбьцжм  
ьижнулхщьлкюэклксыямямбйжцтпогсбэищзмхшсчмддуилойэйугюцдтруцвдуампзэйбузэццюжнвкбхгвргфбчишчжпэгкнрш  
эццлбгвптмвннгшргэмбхогрирумчилцнвцвпжэбтцтвпелжжэйуццлксцбоцюццнзмчяуфбятцбжееэйлкдмеццатмбцца  
ймумгхьцнцгюццдхшзеэпнсбжэяцбгилнгтзяунивпеесмямешуйэйшйэсозгкшйяментэьхрхюзгкхййзгкнйфцгзбйаьцхрг  
ычксдьяцэллтлгтмбхьэецшюхщйххштбьцтмтээьхржжэпмтэсмжжбйаьццирийэсмеивфээсгйллжмцкэсткяжюцтдлкш  
укикейяржэйингзлахрхмйшмймнзиьцтмнипйхуфубьльвфоцлйямярсмюмгчжюбфмтмжюжэкчээмхйейаклккддуилридйй  
укнйриеэцукссмтцбгопямржшйцлритбмкэьбьцогфгебээжживфшквдусгбгвццнтчойцкшбдярхтфьлжнммжэцксмхуоцяффу
```

Очищена строка текста:

```
юммуткйсйумтцбишчоцхйнкхйяхклзкургтвдньлмгсбтмейашрэлшоэгклсмтцэлжфбтдлычтфяляунгфищйээргчсбьцжмьижнулхщьлкюэклксыямямбйжцтпогсбэищзмхшсчмддуилойэйугюцдтруцвдуампзэйбу
```

Порівняння припущення найчастіших біграм з найчастішими біграмами рос мови в лабораторній №1:

```
lab1: ['то', 'ен', 'ст', 'ни', 'но']  
Припущення: ['ст', 'но', 'то', 'на', 'ен']  
У lab1 не вистачає: на
```

П'ять найчастіших біграм шифротексту lab3:

```
['сг', 'жэ', 'ям', 'нг', 'тм']
```

Результат атаки на алгоритм:

```
attack_on_algorithm()  
✓ [18] 26ms  
['сг', 'жэ', 'ям', 'нг', 'тм']  
Припущення: 'ст' -> 'сг' ТА 'но' -> 'тм'  
ЗНАЙДЕНИЙ КЛЮЧ: (a=300, b=400)
```

Розшифрований текст:

```
поздновечеромнаверандесиделколяичтотописалвтемнотебумагуитутолкомнелъзбылоразглядетьвремяотвременионвосклицалагаилииэто
```

Висновки: У процесі виконання лабораторної роботи з криптоаналізом афінної біграмної підстановки, я дізнався як можна з нуля маючи шифрований текст рос мови розширювати його за допомоги криптоаналізу та біграмної підстановки, дізнався про розширений алгоритм віженера, про те як проводиться цей аналіз та як відбувається атака на алгоритм.