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

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Виконала студентка гр. ФБ-24:
Тішевська Анна

Київ–2025

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.

У скрипті lab3.py реалізовано:

egcd(a, b) - розширений алгоритм Евкліда (повертає g, x, y, де ax+by=g);

inv_mod(a, n) - обернений елемент a^{-1} (mod n) (або None);

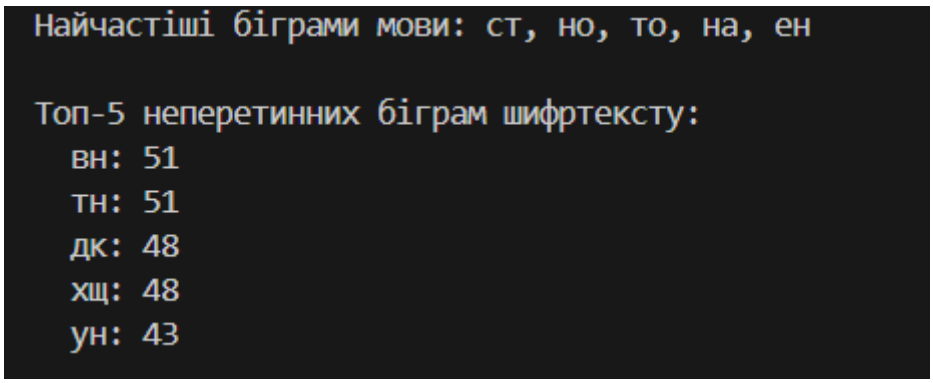
solve_linear_congruence(a, b, n) - **усі** розв'язки рівняння a·x ≡ b (mod n).

```python
def egcd(a: int, b: int):
    if b == 0:
        return (abs(a), 1 if a >= 0 else -1, 0)
    g, x1, y1 = egcd(b, a % b)
    return (g, y1, x1 - (a // b) * y1)

def inv_mod(a: int, n: int) -> Optional[int]:
    a %= n
    g, x, _ = egcd(a, n)
    return (x % n) if g == 1 else None

def solve_linear_congruence(a: int, b: int, n: int) -> List[int]:
    a %= n; b %= n
    g = math.gcd(a, n)
    if b % g != 0:
        return []
    if g == 1:
        ia = inv_mod(a, n)
        return [(ia * b) % n] if ia is not None else []
    a1, b1, n1 = a // g, b // g, n // g
    ia1 = inv_mod(a1, n1)
    if ia1 is None:
        return []
    x0 = (ia1 * b1) % n1
    return [(x0 + k * n1) % n for k in range(g)]
```

Функції тестувались у ході подальших етапів при обчисленні a та b.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму No1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

У скрипті використано функції з лаби №1 (normalize_with_space, remove_spaces, bigram_counts, крок step=2). Скрипт сам друкує результат.



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).

Скрипт перебирає всі впорядковані пари з мовних топ-5 і шифрових топ-5, розв’язує $a\cdot(X1-X2)\equiv(Y1-Y2)$ та обчислює b.
У консолі показується **детальний лог** перших --show-pairs зіставлень (за замовчуванням 30), а **повна таблиця** зберігається у **candidates_step3.csv**.

```
Формула: a * (X1 - X2) ≡ (Y1 - Y2) (mod 961),  b = (Y1 - a*X1) mod 961

Мова ('ст', 'но')  →  Шифр ('вн', 'дк')
  dX=128, dY=902
    a=923, b=604

Мова ('ст', 'но')  →  Шифр ('вн', 'хщ')
  dX=128, dY=360
    a=183, b=284

Мова ('ст', 'но')  →  Шифр ('тн', 'дк')
  dX=128, dY=437
    a= 86, b=790

Мова ('ст', 'но')  →  Шифр ('тн', 'хщ')
  dX=128, dY=856
    a=307, b=470

Мова ('ст', 'но')  →  Шифр ('дк', 'вн')
  dX=128, dY=59
    a= 38, b=566
```

```
Згенеровано унікальних кандидатів ключа: 307
```

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

Скрипт дешифрує всім набором ключів (a, b), рахує просту метрику «російськості» (часті літери, часті біграми, штраф за «погані» біграми) й сортує результати.

```
ТОП-12 кандидатів за метрикою:
 1. score=1.7231  a=654  b=777  | убиватыбольшененадопослетогокаконужеубилноследуетецубьтыблхгшдарньйюначепришлосыбьубиватесамомуэтонешдноиюшьыдоброес
острадакюеэтоотожденствлен
 2. score=1.6706  a=716  b=870  | збрвттобрлйшрнрнсдгпмссетогойакофумезбклноулцдщешюуньккыглтгкдйрщьяюмакюешрцшлойыньзбрвттгсцмемфэтоуекднокюрыдокрфес
одтпагааюжэтобтйжкедтдлрн
 3. score=1.3793  a=887  b=615  | бщбсснзщьэчьпцпцнбпжшхцшйоеозвлолеашбщнзтогздбфшэшбехгдлззыйзбзютгэтовушлюмьгомлхгбщбсснгхуяяеыйожшзбтоеттлэояюкюшс
оенхвшвфтшыйокюнгрршенязпц
 4. score=1.1650  a=747  b=436  | ббфвьтибслршжнжнкдпплсфетогошакоиупебблпнофлплдэеьесууьжыдлбггдюраьщюьабенрюшлоеыуьббфвьтвсвмрмеэтоцегдношкмыдоярчес
онтяатаыюцэтоктцжнентелжн
 5. score=1.1504  a=499  b=64  | тбувстщбйлцшшншндлыпусьетогоэаколуцетбглномлйлдегефувьзыьлнгэдшроьгюааиеирдшложывьтбувстксэмхмбэтокюеэдновюныдощряесо
гтгацадютэтоатлжфегтэлшн
 6. score=1.1158  a=755  b=87  | хббхоажбепбыйшщяввалмуенпнмманйфеухбйпюнгпбясуэугфкщыешпэкйяпцвщогкмдуецньфнжекщхббхоажлудфдноенхуйяюнщгцеднцкурн
наимрмггмоенпащиьунаппйш
 7. score=1.0327  a=397  b=314  | хешфьмвеуавйгягшукюжэсгыотоьхяотьдгхецановажунгюпюьичвикардмуанвчацкхлгинлйоотиичхешфьмыэипбпнзыоргмунорцяивопнагл
огмшхяхпцфзыофмнтеггмщагя
 8. score=0.8498  a=453  b=491  | тщссснищгзсьфцфцьбтжщхдшнойощвпокенштщфзцокзтбвшкшаемгьлозкйхбйюйгстбвбшнюжьзодлмгтщссндхщяжяыыноушхбцощткклбобюлшх
оенивлвйтоыноюнпрюшенжэфц
 9. score=0.8491  a=622  b=230  | щьфняжфьфллпноноярвсшфьвнажабкбаючдвщьллхайлцривцвьчздхтрлуядригшдкзхковпгпптадтздщьфняжыфщэпэюхнаявдрхашзятчащгрвь
айжккчкьзихнафжлубвйжвлно
10. score=0.8366  a=850  b=523  | жпрфьзкпнгхжененнящчбвкдлтютфквтвмрджпогстэгзяудодрмюхтркгцщйяфэьхоадкидвэшжзтнрюхжпрфьзтвииринылтфдйястйасргтщэшдж
туэукххуахылтдзэйждузпген
11. score=0.6989  a=936  b=456  | ччуиарлчпэууэюэюсйуяцачщеонотзбоибещччмэтобэдйьщлщэбкесфшэышойюпрерждзющхпкусобфкеччуиарващнбндхеошщойтоажффюоопйищф
ошрхзпзбжэхеозрыкдщщрйээю
12. score=0.6449  a=189  b=560  | рбквфтчбялошананмдупюсэетоговакозучербшловлсдеедерудьрыслэгедкррьцюеайешрьшлопыдьрбквфтфсхмдмьэтояеедноххюцыдолраес
ожтиаьачюнэтогтежхежттлан
```

У цій роботі я виконувала криптоаналіз афінного шифру на біграмах. Спочатку реалізувала необхідні математичні функції - розширений алгоритм Евкліда, пошук оберненого елемента за модулем і розв’язання лінійних конгруенцій, тому що саме на цих операціях базується підбір ключа для афінного перетворення. Далі, використовуючи код із першого комп’ютерного практикуму, я виконала частотний аналіз шифртексту і знайшла п’ять найчастіших неперетинних біграм. Потім зіставила їх із п’ятьма найчастішими біграмами російської мови та для кожної пари розв’язала систему модульних рівнянь, щоб отримати всі можливі варіанти параметрів шифру - ключів (a, b). Для кожного знайденого ключа я автоматично дешифрувала весь текст і оцінила «російськість» результату за частотою типових літер і біграм. У підсумку з усіх варіантів був відібраний той, який дав осмислений російський текст, тобто я фактично відновила вихідне повідомлення без знання ключа. Таким чином, лабораторна демонструє, як на практиці працює частотний криптоаналіз біграмного афінного шифру - не шляхом повного перебору, а за рахунок математичної логіки й статистики мови.