



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 елемента 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 $a^{-1} \pmod n$ (або `None`);

`solve_linear_congruence(a, b, n)` - усі розв'язки рівняння $a \cdot x \equiv b \pmod n$.

```
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.

```
Найчастіші біграми мови: ст, но, то, на, ен
```

```
Топ-5 неперетинних біграм шифртексту:
```

```
вн: 51
```

```
тн: 51
```

```
дк: 48
```

```
хщ: 48
```

```
ун: 43
```

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: $a * (X1 - X2) \equiv (Y1 - Y2) \pmod{961}$, $b = (Y1 - a * X1) \pmod{961}$

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	убиватыбольшененадопслетогооаконужеубилноследуетецубытылхгшдарныйоначепришлосьбыубиватесамомуэтонешдноиашьдоброес
2. score=1.6706 a=716 b=870	эбрвттобрийшнрнсдгтмссетогоайокофумезбклноулдцщешуныкыглтгкдйришьаюаюещрщлоыйньзбртвтггсимефэтоуекднооярьдокрфес
3. score=1.3793 a=887 b=615	бщбсснэщзъчъцпцпбжжхщшоеозволаешбщизтогэдбфшзбехгдлзыйзбзюттэтовушльмьомлхгбщбсснгхуаяеыйоажзбтоеттлэояюшс
4. score=1.1650 a=747 b=436	ббфвьтибслршнжкднплсфетогошакоиупеббллнофлпдзееесууьждлбггдйраыщъабенршюлоеуьббфвьтвсврмеэтоцегдношкьдоярчес
5. score=1.1504 a=499 b=64	тбувстцбйлцшшнддъгусьетогоэаколуцетбглномлйдегефувъзылнгэдшрьоьгааиердшложьвътбувстксэмьэтокеэднояньдошряесо
6. score=1.1158 a=755 b=87	хббохоажбепбьйшйшьявалмуенпнманийфеухбйпнгпбсяуэугфкщъшэкэялпцщогкмдущецньфнекекщббохоажлудфдноенхуйяюкщгцедндцкурн
7. score=1.0327 a=397 b=314	хешфьмвеуавйгягяшукожэстыотъхютъдгхецановажунгопъичвикардмуанвчацхлгнлйоотиичхешфьмьэилпбнзыоргмунорциявопнагл
8. score=0.8498 a=453 b=491	тцссншщгзсъфцфцбтжхщдшнойощпокеншпщфцокзтбвхшшаемгьлозкйхбыйгстббшнкожьзодлмгтцссндхщяжыьноушхбцоцтклбоблюх
9. score=0.8491 a=622 b=230	щьфняжфьфлпгноярявсшфьвнажабкбаюдщъллхайлривецьчэдхтрлуядригшдкэхковлгпгптатдзщьфняжфцщлэюхнаявдрхашзятчашгрь
10. score=0.8366 a=850 b=523	жпрфьзкпнгжжененнящбкдлтютфктвмрджлогстэгзюдодрмхотркцшйфьэхoadкидвэшжэтрнрюжпрфьзтвириыльтфдйястйасргтщэждж
11. score=0.6989 a=936 b=456	ччуиарлчпзууэюэсюялцащеонотэбоибещчмэтобэдышлщэбкесфшэшойкопрерждзюхлпусобфкеччуиарвшнбндхеощройтоажффоопйщф
12. score=0.6449 a=189 b=560	рбквфтчбялошаннмдупосетогооакозучербшлновлсдеедрудерыслэгедкрыщъоаейщрышлопидьрбквфтфсхмдмьэтооеднохюцдолаес
	ожиаьачонэтогогтежхеттлан

=== ВІДКРИТИЙ ТЕКСТ ===

убивать больше ненадо по слогу окая кону же билно следуе тебе быти блгшдгарный и наче пришлось бы убивае самому з то не щди ни шды доброе со страдакье з то о тождествлении на основ акимо би наковъ пмпулесовку и войству сдственн оворялишви южмальной степе ки смещенный на русо сизмэпическая ценностъ ты той добротъ зюпичне оспаривает сй может бытъ з тов ообщемеханизм нашг шдбюго оучастия поотношении к друг оу чело веку сдбнойсно протупающий в чрезвычайном случае обремененного осознания своей вины писателя не сомне ния что з ашмпатия по причине тождества лекаря решительно определила вьборматенала до стоевского онос на чахонизэглостичь сзюхлджудейкой вшдлблбкновенного претстип кь капои поическог лореи ааозного опреждечемкконцусвоей гпозни вернутъ я кпервопруступнику кутцеубийце и сдехать веги оидсвое поэтичское пнзнание о публиковакье его по осмертног она слебьодневку ковего женьяркоосвепило щди нпизшдего жикютюмремя ко да до стоевский в германе вьблбуре ва емг орной страсть до стоевский зарулет койя внь упнло падо ктатологи чьской страсти кторый не шддае тзйной оцenneккск акой стороны не блонедостатка во правдания з тог остранныг льонедостойног оповедкья чувствоянык акэ то не редкдбьвае тунемротиков на шлоконкретну з аменувдбремененнос подлог аждо до стоевский о гтго вановатъ а тэмч то нпривуюг рше получил вьбозможность вернутъ а я мросшь вьзбехавзаклечения я тирь мукребиторайно зтдбл толь ко предлог до стоевский блдстативно поюкцателенч то бь з то по нятч до статочно чистенчтдбь з то мпризнатъ я зонзналч то гачнъмь хаи граса ма по зе бесшдбюбноспнег ообусловленног оперявнь мипозь ва мибзрас судног оповедкья с лужатт о му до казательством иеще ко ечмрюноу оу он не успокаивалъ з по канетеря лъзго ии г рабъ хадля нег ота кже средством са мона казания не счтеное количество враз давалом шддойженословлю чьстнык словобольшенеи граты или нвю граты з то тденыи на рушалэ то слово каона рас казъ вае тпочтивзег да ес ли он сво имигьюи г ршай до во билсебь еедо крайне бедственного оположекия з то служил шддя нег оещ еоднимпато ло оическимудовлетворени емонмог передниипоноштыи уюкжаты вебяприситыепредоратыг орас каивает ся в томч то на вьшха з ацужане гостыаюг рше кюа и пос лев сей з той разг рузисовспна следидицой денчюг раначина ласе носова имло шда же на при вьсхакэ тоу ююкля так ка ка з аметил ч то от чег о ве дей стельности толь киможнбь ло оуе да ты спасения мс тельствокжог дане гь оудви г ало сь впереллуче мпо слепотеносег лиза кла дь ва ния последнег оиу шьствас вядовсего з тог оона ко нечненепо кьма ха ког да ег очуство вни бь лоудовлетворена ка за койи микк торь мон сам з ебя приговорил тог джэс че за ла з трудненность вработетог да онпозволялсебь сдехать не сколько шхг овнапупку спеху рас сматню ва рас каз бо лее мошлдог опис ате ля не трудног ада ты ка же да вно по за бьт ед ет сиепереговорякьяна шдхдтъ вь влекоя виг орной страсти усте фанацвей а по сь ва ти вшег омеждипь ойм до стоевскому биюкьз свотхочерковтнмастеравсборкько есмятениечувствы ть новелла двадцать четь реча савгпзниженцьэтот маленъ зюи шдеврпо ка зь вае т ка кбу дтолпы то ка ким безответственньм существом являе т ся же нцона ина киеудивительне ддя не еса мойзаконнарушенияеетолкае тнеогпданноегужненоевпечатлениенон овеллэ т асы ипо подврг нты егешхоаналитичьскоу толокованлиг овонотоднак без та койо правдъ ва жейтенденуи г ораз до большепо ка зь вае т совсемиоедбще человекое ил искоееобщемужко еит а ко етолкованиестоль ачнопшдсказанч то не твозможноснег онедопспуты дляущностхудо жьственног отворчестваларактернч то писателескоторь менясвзъ ваутдружьсзвотношениивотвнмаи рас спьсыотверждалч тои помянотое толкование емучжо ивовзевне шдидло вего намерения не смотря нч тог о рас ка зь вл ет ен ьнекторь едет аио ка кь расчитанье нато что бь указь ва ть натай нъ следз той новеллелик оветска япожила да ма поверяе тмса теомч то егупншло сь пережити бо лее да в дцаплеттотмуназдрано о до вевеша мь ть ду хсь новей кторь ечней бо лее не ну жда юсьот ка за ва шья зот ка зю хь то нибь ло на деждна сорок в тором о ду гпзниа на по па дае т во мремя о дню глиз свотх бесцельныхпутешествийи г орньизалмонакског о кадоног дысребь в сехбиюкья неевь коа кьпо нковъ ваутдверуки кторь еспотряса щейне посредственностьюи шло ойотржгитъзепереговарь емь не счастныгь ко мчувстваружэтируки крашо гоюи ошпи сателъ ка кь безовся ког оумь сла деае тего оновеником старг осьна блдг гищей зю гпо жьнениипотеря виего всь ка кь глубочайшечмочта нечпо зипа кжего за тлблвляе тпо ко нчтмь косвоечбезнадежнойгпзникнейзаскьямаксимпалъ за ставляе т же нчтнчс деловаты

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.