Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Лабораторна робота з криптографії

Криптоаналіз афінної біграмної підстановки

Виконали:

Студенти групи ФБ-33

Бондар Марина Вікторівна,

Романовська Крістіна Миколаївна

Перевірив:

к.ф.-м.н., ст. викл. кафедри
математичних методів
захисту інформації Селюх
П.В

Київ 2025

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, 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

Для нумерування та числового представлення біграм, було використано формулу із методичних вказівок та реалізована функція.

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}.$$

m – к-ть літер алфавіту.

```
def bigram_to_num(bg: str) -> int:
    return ALPHABET.index(bg[0]) * M + ALPHABET.index(bg[1])


def num_to_bigram(num: int) -> str:
    return ALPHABET[num // M] + ALPHABET[num % M]
```

При розшифруванні виконується обернене перетворення:

$$X_i = a^{-1}(Y_i - b) \bmod m^2$$

```python
def decrypt_with_key(text: str, a: int, b: int) -> str:
    inva = modinv(a, MOD)
    if inva is None:
        raise ValueError("Не має оберненого за модулем 961")
    res = []
    for i in range(0, len(text), 2):
        bg = text[i:i+2]
        if len(bg) < 2:
            break
        y = bigram_to_num(bg)
        x = (inva * (y - b)) % MOD
        res.append(num_to_bigram(x))
    return "".join(res)
```

Для розшифрування був використаний алгоритм Евкліда.

```python
def egcd(a: int, b: int):
    if b == 0:
        return a, 1, 0
    g, x1, y1 = egcd(b, a % b)
    return g, y1, x1 - (a // b) * y1
def modinv(a: int, n: int):
    a %= n
    g, x, y = egcd(a, n)
    if g != 1:
        return None
    return x % n
```

Лінійне порівняння було реалізоване із урахуванням двох випадків $ax \equiv b \pmod{n}$
1) gcd(a, n) =1 В цьому випадку порівняння має один розв'язок
2)gcd(a,n) = d >1 Маємо дві можливості:

- Якщо *b* не ділиться на *d*, то порівняння не має розв'язків.
- Якщо *b* ділиться на *d*, то порівняння має рівно *d* розв'язків

```python
def solve_linear(a: int, b: int, n: int):
    a %= n
    b %= n
    g, x0, y0 = egcd(a, n)
    if b % g != 0:
        return []
    a1 = a // g
    b1 = b // g
    n1 = n // g
    inv_a1 = modinv(a1, n1)
    if inv_a1 is None:
        return []
    x_base = (inv_a1 * b1) % n1
    return sorted((x_base + k * n1) % n for k in range(g))
```

Генерація ключа відбувається за формулами:

1) Параметр ключа a:

$$Y^* - Y^{**} \equiv a(X^* - X^{**}) \pmod{m^2}.$$

2) Ключ b:

$$b = (Y^* - aX^*) \bmod m^2.$$

```
X1 = bigram_to_num(X1bg)
X2 = bigram_to_num(X2bg)
dX = (X1 - X2) % MOD

for Y1bg in top5_cipher:
    for Y2bg in top5_cipher:
        if Y1bg == Y2bg:
            continue
        Y1 = bigram_to_num(Y1bg)
        Y2 = bigram_to_num(Y2bg)
        dY = (Y1 - Y2) % MOD

        sols = solve_linear(dX, dY, MOD)
        for a in sols:
            if math.gcd(a, MOD) != 1:
                continue
            b = (Y1 - a * X1) % MOD
            candidate_keys.add((a, b))
```

Ентропійні критерії для порівння значення інтегральних характеристик тексту (ентропії символів та біграм, індекс відповідності) із еталонними для мови.

```
def index_of_coincidence(text: str) -> float:
    N = len(text)
    if N <= 1:
        return 0.0
    cnt = Counter(text)
    s = sum(c * (c - 1) for c in cnt.values())
    return s / (N * (N - 1))
```

Комбінована оцінка змістовності:

```python
def score_language(text: str) -> float:
    N = len(text)
    if N < 100:
        return -1e9
    ic = index_of_coincidence(text)
    score_ic = -abs(ic - 0.055) * 200
    ob = [text[i:i+2] for i in range(0, len(text) - 1)]
    total_bi = len(ob)
    common = {"ст", "но", "то", "на", "ен"}
    bad = {"йй", "ьь", "ыы", "шш", "жж", "цц"}
    if total_bi == 0:
        return -1e9
    common_count = sum(1 for bg in ob if bg in common)
    bad_count = sum(1 for bg in ob if bg in bad)
    frac_common = common_count / total_bi
    frac_bad = bad_count / total_bi
    score_common = frac_common * 50
    score_bad = -frac_bad * 200
    return score_ic + score_common + score_bad
```

Текст:

фобиьудлюфрищьдшмйожличйзпсфоэвужущфшвлихфчхвущмятктчььудлюфоущьдшмйожзжмабщэжфужмуощмюожуяьчьббксяблорвльигозпвчгчркьлыктцтчьщпямйбвбхудллыттебшвфоивфабщврбщдййыктигфоььфэкуигиочгэйпхшьдпвиштювеэигкбфоозжкьбшуыакбозйхнйбуеэщчуубущхшьрсаорвлькхшьозпьлйожнйзппвэжйзатлозжатюхнйатгврвряощзжоуявбибпзжфуевнбхьбусмгйзпбиаггижтгбаттжмжфотйкгзфууцтквыышбеймьшфозвуэбчгщрэбцуюффаапазббюбджьуйьттшьцвфаврйзаыигцтыгатлохфзфзоифзпяефуиатгхфвиаюювнйзпоуэбщрриюшяьфэкуигсэчтльпьфсаййзктжпющыгатлоыытькпгирвльйьштшбльигшьрвюшттщпричпщпцбтжбщигпьюжмьчэтьббкзчьлщлшюжмьштшббгщрэбпбфжжзришщфкювюффаеьхьыэгьцтэбпхкбхьшьигшьрвюшжщжхзжихойаэфуюьмьчслбмщхоиыщплияюбуявнйюбшуыакбжзпвриеурзвитгльгиеймьхиепзжлищпцбтжбщигшудежйяьогяжфтигльигдеутфухьдлоткйзппвюжьуйьттьубуэбииепььяуахфдмжеумьюьчьгбшьпьйьщфахапутюжмьчэтыйебуугшьятяхыуфбетыубгзжаттжагуушуеэтбщьзпдйбучвцпбщльйьщьдшмйожььчэлозжгонйччейожрвкссхбщюулеюьлгбпбигатксщкхолищмюуевжккьттдллыйьгьщьктяабщижйзшьахкбооозагхоивзжатчтяьнпюжфуэбрйгьпьрвксуэшьгвгикпбзяокгсгбзттябхудллыйьювеэигкбфоивфаапазббюбпхшьозйюйбозыуфуэбджщфшвливдейюьмйзпсфоэвушуыакбжщюопхшьрсаорвльигмжттебшвфоивлигьщьмуигатксижховдгодйэйяабщвщтхкбооозагхоивцбцирвгодйжбигыэугбпдйвигыщпрсаорвльигмжюьмьшьащюоииаюювнйзпоуэбубыуутрощматхьчфчхбщяшятялгьлбгбющзжьудгчхрфазсгхозрцпзфхук.

Розшифрований текст:

алымсельскимхозяйствомвструктурееэкономикипреобладалосельскоехозяйствовегодывнембылоболееполовиныучисленностизанятыхионодавалоприблизительнонационального доходасгодасталаосуществлятьсяпрограммаиндустриализациивенгриизапоследующиелетпромышленноепроизводствостранывозрасловразпосравнениюсдовоеннымуровнемнаиболеебыстрымитемпамиразвивалисьтакиеважнейшиесточкизрениятехническогоразвитиявсегонародногохозяйстваотрасликакэлектроэнергетикамашиностроениехимияпосуществузановобылсозданрядотраслейсовременногомашиностроениянапримерпроизводствоавтобусовиузловдляавтомашинтехникисвязимедицинскогооборудованияприборостроенияидрповыпускунекоторыхизделийпромышленностивенгриязанимаетзаметноеместовмировомпроизводствеиэкспортевчастностиэтанебольшаястранавсегонаселениямираобеспечиваетоколомировогоэкспортаавтобусовэлектролампмедикаментовразвитиеведущихотраслейнародногохо

зяйстваобусловилосущественныйподьемэкономикистранывцеломобьемнационального годоходавгод увозросприблизительновразапосравнениюсдовоенныммуровнемврезультатезначительногоиндустри ального развитияпроизошлиизмененияв экономической структуре венгрии доля промышленности в на циональном доходе страны увеличилась с в году до приблизительно изменилась структура самой прмы шленности в которой доля машиностроения и металлобработки поднялась до химия до всех этих показатели характеризуют венгрию как среднеразвитое индустриальное аграрное государство с развитым сельским хозяйством главное место среди отраслей венгерской индустрии занимает машиностроение на которое при ходится около половой продукции и свыше занятых в промышленности на этуотрасль приходится приме рно всего экспорта страны номенклатура производимых изделий весьма широка и составляет по оценкам доно менклатуры мировой машиностроительной продукции венгрия специализируется главным образо мна производстве автобусов дизельных моторов станков по

Топ-5 біграм шифртексту:
иг: 65
ль: 46
рв: 43
шь: 42
ний: 39

Результати аналізу та оцінка ключа
a = 397
b = 111
score = 3.425627836095208
IC = 0.0569

Висновоки: у ході виконання практикуму було засвоєно, як використовувати розширений алгоритм Евкліда для знаходження обернених елементів та розв'язання лінійних порівнянь ключового рівняння. Для автоматичного розпізнавання змістовного тексту була здійснена функція оцінки на статистичних властивостях мови. Цей аналіз включав використання індексу збігу та частотного профілю біграм для перевірки всіх кандидатів у ключі. У результаті виконання роботи було знайдено правильний ключ шляхом перебору та статистичної оцінки, що дозволило успішно тримати вихідний текст.