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

Виконали:

студенти групи ФБ-32

Кошеленко Н. Е.

Кухарук І. А.

Київ – 2025

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 (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.

Варіант 12

Реалізація математичних підпрограм

Реалізовано функції для математичних обчислень:

egcd(a, b) - Використовується для знаходження найбільшого спільного дільника $gcd(a, b)$ та коефіцієнтів x, y, що задовольняють рівняння:

$$a \cdot x + b \cdot y = gcd(a, b)$$

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

mod_inverse(a, m) - обчислення оберненого елемента за модулем;

Обернений елемент a^{-1} за модулем m існує, якщо й тільки якщо:

$$gcd(a, m) = 1$$

і обчислюється як: $a^{-1} \equiv x(mod m)$, де x - коефіцієнт з розширеного алгоритму Евкліда.

```
def mod_inverse(a, mod):
    g, x, _ = egcd(a, mod)
    if g != 1:
        return None
    return x % mod
```

solve_linear_congruence(a, b, m) - розв’язання лінійних порівнянь виду a·x ≡ b (mod m) з урахуванням кількох розв’язків.

```python
def solve_linear_congruence(a, b, mod):
    d = gcd(a, mod)
    if b % d != 0:
        return []
    a1, b1, mod1 = a // d, b // d, mod // d
    inv = mod_inverse(a1, mod1)
    if inv is None:
        return []
    x0 = (inv * b1) % mod1
    return [(x0 + k * mod1) % mod for k in range(d)]
```

Також реалізовано допоміжні функції для переходу між біграмами та їх числовим представленням.

Обчислення частот біграм

За допомогою коду з ЛР-1 проведено частотний аналіз шифртексту. Отримано таблицю найчастіших біграм (див. консольний вивід). Для подальшого аналізу взято **5 біграм із найбільшою частотою**.

```
- РЕЗУЛЬТАТИ ОБЧИСЛЕННЯ ЧАСТОТ БІГРАМ -

-----------------------------------------------
№   | Біграма  | Кількість  | Частота
-----------------------------------------------
1   | ул       | 112        | 0.0221607
2   | нж       | 87         | 0.0172141
3   | вэ       | 85         | 0.0168184
4   | ло       | 77         | 0.0152355
5   | ед       | 66         | 0.0130590
-----------------------------------------------
```

Вибір частих біграм мови

Для російської мови обрано п’ять найчастіших біграм: **ст, но, то, на, ен.** Ці біграми порівнювалися з п’ятьма найчастішими біграмами шифртексту, утворюючи можливі пари (X1, X2) ↔ (Y1, Y2).

Пошук ключів (a, b)

Для кожної пари біграм складено систему рівнянь:

$$a \cdot (X1 - X2) \equiv (Y1 - Y2) \ (mod\ 961)$$
$$b \equiv (Y1 - a \cdot X1) \ (mod\ 961)$$

- ТАБЛИЦЯ ОБЧИСЛЕНЬ ДЛЯ СИСТЕМИ (1): Пошук ключів (a, b) -

№	X1(біг)	X2(біг)	Y1(біг)	Y2(біг)	dX	dY	gcd	a	b
1	ст(545)	но(417)	ул(600)	нж(409)	128	191	1	9	500
2	ст(545)	но(417)	ул(600)	вэ(90)	128	510	1	19	816
3	ст(545)	но(417)	ул(600)	ло(355)	128	245	1	565	195
4	ст(545)	но(417)	ул(600)	ед(159)	128	441	1	56	832
5	ст(545)	но(417)	нж(409)	ул(600)	128	770	1	952	509
6	ст(545)	но(417)	нж(409)	вэ(90)	128	319	1	10	725
7	ст(545)	но(417)	нж(409)	ло(355)	128	54	1	556	104
8	ст(545)	но(417)	нж(409)	ед(159)	128	250	1	47	741
9	ст(545)	но(417)	вэ(90)	ул(600)	128	451	1	942	835
10	ст(545)	но(417)	вэ(90)	нж(409)	128	642	1	951	735
11	ст(545)	но(417)	вэ(90)	ло(355)	128	696	1	546	430
12	ст(545)	но(417)	вэ(90)	ед(159)	128	892	1	37	106
13	ст(545)	но(417)	ло(355)	ул(600)	128	716	1	396	760
14	ст(545)	но(417)	ло(355)	нж(409)	128	907	1	405	660
15	ст(545)	но(417)	ло(355)	вэ(90)	128	265	1	415	15
16	ст(545)	но(417)	ло(355)	ед(159)	128	196	1	452	31
17	ст(545)	но(417)	ед(159)	ул(600)	128	520	1	905	888
18	ст(545)	но(417)	ед(159)	нж(409)	128	711	1	914	788
19	ст(545)	но(417)	ед(159)	вэ(90)	128	69	1	924	143
20	ст(545)	но(417)	ед(159)	ло(355)	128	765	1	509	483
21	ст(545)	то(572)	ул(600)	нж(409)	934	191	1	598	469
22	ст(545)	то(572)	ул(600)	вэ(90)	934	510	1	515	537
23	ст(545)	то(572)	ул(600)	ло(355)	934	245	1	596	598
24	ст(545)	то(572)	ул(600)	ед(159)	934	441	1	304	212
25	ст(545)	то(572)	нж(409)	ул(600)	934	770	1	363	540
26	ст(545)	то(572)	нж(409)	вэ(90)	934	319	1	878	477
27	ст(545)	то(572)	нж(409)	ло(355)	934	54	1	959	538
28	ст(545)	то(572)	нж(409)	ед(159)	934	250	1	667	152
29	ст(545)	то(572)	вэ(90)	ул(600)	934	451	1	446	153
30	ст(545)	то(572)	вэ(90)	нж(409)	934	642	1	83	22
31	ст(545)	то(572)	вэ(90)	ло(355)	934	696	1	81	151
32	ст(545)	то(572)	вэ(90)	ед(159)	934	892	1	750	726
33	ст(545)	то(572)	ло(355)	ул(600)	934	716	1	365	357
34	ст(545)	то(572)	ло(355)	нж(409)	934	907	1	2	226
35	ст(545)	то(572)	ло(355)	вэ(90)	934	265	1	880	294
36	ст(545)	то(572)	ло(355)	ед(159)	934	196	1	669	930

170	на(403)	ен(168)	ло(355)	ул(600)	235	716	1	367	448
171	на(403)	ен(168)	ло(355)	нж(409)	235	907	1	834	603
172	на(403)	ен(168)	ло(355)	вэ(90)	235	265	1	819	882
173	на(403)	ен(168)	ло(355)	ед(159)	235	196	1	283	665
174	на(403)	ен(168)	ед(159)	ул(600)	235	520	1	84	903
175	на(403)	ен(168)	ед(159)	нж(409)	235	711	1	551	97
176	на(403)	ен(168)	ед(159)	ло(355)	235	765	1	678	810

Усього знайдено 176 унікальних пар (a, b).

Усього знайдено 176 унікальних пар (a, b). (повна табличка у виводі в терміналі)

Обрана пара біграм:
X1=545, X2=417; Y1=600, Y2=409

Рівняння для a:

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

a * (128) ≡ (191) (mod 961)

a * 128 ≡ 191 (mod 961)

Обернений елемент: 128^(-1) ≡ 473 (mod 961)

a ≡ 191 * 473 (mod 961) ⇒ a ≡ 9

Обчислення b з Y1 ≡ a*X1 + b (mod 961):

b ≡ 600 - 9*545 (mod 961) ⇒ b ≡ 500

Рівняння розв'язувалося за допомогою розширеного алгоритму Евкліда. Знайдено єдиний правильний ключ: **a = 9, b = 500.**

Дешифрування шифртексту

Виконано дешифрування шифртексту з використанням знайденого ключа.

Використовуємо обернене перетворення:

$$X \equiv a^{-1} \cdot (Y - b)(mod 961),$$

де a^{-1} - обернений до a за модулем 961.

Для кожної біграми Yi шифртексту обчислюється відповідна біграма відкритого тексту Xi. Результат об'єднується в рядок - це дешифрований текст.

Якщо текст неосмислений, пара (a,b) відкидається.

Ключ: a = 9, b = 500

Зашифрований текст:

ыжщжулмтчтрхгнбецтйвчцэожэжгктацтцофьшвэктднцшлнбоьшяцуагпуйкфсфктвэянекфохж
ивезцтеобпчвжмрцсофйхуулцзтцизхэуэдвщгцдхялотжшэфчйжчоштюясбшыжкхвяялосжнйуэ
длиачлвкуэсйвквэфчхвртулйдьрхлюкдлктржзжхшхвчдхэхвчдцдажллавтцптгэберцавюуфжйд
сдкоцдтжявчцвэнжйвзжзскофэуснжкофэусуйюэхбфчатыфпдяштержедцдхяяпуахвукфжчонж
сжхэрнюкхвобубблбррцркдлотубчтыбюэянекхэюбьжктулдвсычтболотлхэдфцтжьыцукфжйде
цукхвноьжвоцдхяхэтонжнйхвуухвянкэгпхэюууксйсьяныыцдхяодджйвянзцптллцжсшвьукутв
бтеукчвмтзэдлтндвсузвчтмэеуктьжктажсыыэеундоьаллнбеясщцыдясьоякктсжржыфадцдхэто
уледтэчвчднжеоыжхябччлщлбзыфджаищочжюфщтлодцчввуйдьрхлюкдлхэцщжлоэдфбтикфж
щеыжндзтулдтмэфчшочжедшбяпчлныптмэдчщжчвнжгдлозцдвмтгжжауээеджьпзойжэхтйцшт
цдчюбжтябэчщжчахэвууатпедеояяцыажскайлодвчтэхюжчтфээофщбешойдсжктаэцжштютчтр
хлосжцдяцрхиватщтктытхжфктнчтломлхксжгдыжытвэгшгдхонжнйстипзочжчоыждахктцзщь
жхэсьвкстющаачлшщаахэюбьжктйтцддлшщвулотлхэвузвшочцютыжишчвроярчлхухэхфщоу
дццдхдйтсузыцдхяйдывтнфчыттпещнжаштцуйюксйвэнесйктгэтцктсдяэшщьжьжроюянжянбее
укэнждвзтджйдтжжксйдлоэдфбтцдчдпосдпоьдыжжэбччдпоашчвюкчвлцжшгдяяцыйдкфнфр
шфефпйжчжчоцдцпжвндшохяжвчдюхвэяцфкдляцсовбмхюякэцпцшвцкищокттнчжчошохябчх
дйжгбубхэуэавчдедццдхякткххдяяьжржллтцктипйжавчжчоыжьжсбрцсцхкнжгдмэфчыфсосбте
вцукхвлцодджбтвэфшвьнжеважсжйвчцэояшуйрхатещхвьжбхшозпеддтажкоадяяякещууафчо
жкмлрвйоктажлоадяяатуледмэчвштдццтрясбчлцшуахэцщукцыйдушхвсбтевквэсйхктггжбхрэ
тцвэнжржктчлчжчоцдчлхбйдхэуунжржыфадцдтнгшптряяцгжоцутдштержзжжтсэюуажьшянн
жуллцсдыоштюэожиуцрэозжфэюбстчцоцйеавкттнчжчоджулустндвэтиояяптсшдлнжулноувчт
щжгдлодцуледштоозтсббзтнцдулнзашрцюкоэцшхвашайвкмлнооюцшадяовжашхуйгчтмэизед
хшрнчлндхожтсфшойжгдяяюэожиуцргсхкбщнжулыцтжзшвувэнжджбмдвчцвэцщуктцчвоуьй
двмлизржщжзшхвсухлзогддлцындрэцщукоэдчбфмбыбуахдтжяоукоэгташчлдвяхдйвухбедщоз
тсббзуледйдчпхууашотпчтулавмаыжщдюянжйвдлбзубгштцажшощозтсбэчнкяшыэфпшщдтйд
кфртлолпедйщвктцвбфпцшуйюкяяефцшмдлосдяокзубгштцжухвптуледмуяшфпшщщоуйнжз

швувэнжбтктещвусдржюищоршепгхгейдшоашвкдвяятжьшвйлозтулгдбзйквэзвзжюжшэцжэу
вэыцукавноцткубщгшбейдяохэукоэгтршуэбрищхвьжаждбедцтмэеуьдйжяыбйшсыоандвякхлр
хейчвэфябштчтожмэфчптщоктсбхкобцпзоионжбяайюэыцсохяжудвштпйвкукюуаыыфйдйжшэ
дчсждпусштиэдчедснфччтоаюуьйбчулдтмэеунжкхдлезнжыжооавфехдкгьтюжчтвущмрхбоцт
рткхвбхугяглгшжштееощовбхуефлондяоейяыоцйеэобтййдэфшуйрхкзфшубштквчдкйфшьжи
фулуэтцчтмэизьшуэсэцряжйдюярхвосжйпцшцргывозпзопряпатулоквгмйгдеохдвайжшхедсбм
хщобоеощжэебтктлоайуэрхчшхвсшзльтхдмэизашайажцдмддллхбхужлчвьфждзэфошоажске
рвквэфпеджквэрхфйбчулеойвчдшосцдвштовзхскюэожиуцрэощлчлеошэфшигвэгыивьшещстэ
вкэтоюжчтещхвьжажскайулеокууажлбхяяодзхгштерхатскяпшзвмвэшттвыблооотпедзжйэюбу
эубчлцшйсажьшцщвэеудвнржшрнчлгйдвмлсжжкяйбчьжшккбхкчттлыцрдилцштцщлхбхлхвь
шчютоажштзоджсфчцжшсьхлрвзцяхцыждфйхкцдйжзжшэубутскюбломдвьботйуэхлуйчвчдьж
йэхквгрвчтпбфпуьешалппшзалалвкйоедувндсдяячвьфиокгвуцызжшйвквэтцчвштеатедлдошоа
жштчтеоцтловпшзалалвкоууьдлпйвкхлоблонтдтшосжчтяэйсжтркууежзтрягдлэйсюэожиуцргс
тнгшаастефвжьшхвсшзлгыашайулрцяыглоцайвэгыхкяйнзавьжзоынхкбелоюохяадтжулыылом
взтьжгцщдмбцзуййдсжажгэвэгсюжюяужржиоскхвэтяоукавьжифршфеекбщнжулавгцайвэьтгб
хугяглгштцчвчдшохяйдьжбьдфйжжэбоилхуйттжулыылобщьжьйцжбгяшнжржаважюяхжгдло
пижугцайвэьтивтцжтбтмэхувожтэфзофуулуэтцалцыивянхкатгдлэфчбхулйжедсцыцшсщтйвл
жьшхвюядзфейчулгдщжчжэхчлэфзофухвчднжлыэвзцсьнжкщхвяяюцукглрхчпчвэфяквээчзжг
эуабзуледйдчштееощодлешэеадтпчвтнулифдлйжулежбмдвчцвэнжржашфосцуйулгддкзщртло
ятржулкфтлешжшчвэфашфосцуйалвкоэчвщоьшвйрцхунжоочжьшхвяыьисжнжвопохдйтктюу
зсыоцбэфзофуепныджржчлнжртлокуаыыфйдйжшэутэфзоулсбутажьшянчтлодвщоефшокфдлг
эуашщавчтмэгтчбхэхубщдвпогпйжютувжжыбмхгдемьтщжажщэалвкоэгтмхмбьйяыашуйдбяо
юэдлешавэвпочжьшхвчтйвфехдгдмлвуодзхефсктцгышклшчвчдашфосцуйулгдивзищокдтлцш
гйвкшсьштееощобокйжвьшэоэфзофуфжзтрягдлэеушкмвьшуэтпгшезуйрхеляпхучбхэхуюбьтх
эхубщдвподлкфшэчвщосжьжмхгпгшаыыцшсаищоржуфхдквчцуэвууажлктсбтехлрвкэхфйжжэ
гштееощомлешэеаднжашгиьжгбсьхдмвьшуэтобтдллиьжджыэщгвээооцыстпераююбзрвкмйуэ
нжишрнчлжшхвсучлжтяяяпйжуэукэеяштцхлпжжауээецргсэфзоулсбфчцтмлвкоэчвщоивьшуэ
двэтжтчжшэеущоажиисжнжвопойдашюугшяцвэршэожэцщукгшхвсухлзогдглцыштцшдлюбху
длуйбщдвпогпхкуьвэгыавскайтцуэгысдштбйстэвлжютмбфштешойэизкдтлцштцедсцалгыюэы
фулзоалешэеаддтказояпзойжшэцшдвешсэдчтфюяэфиэфоулцшбщдвпожоюэошхвьшдбэфиэдч
ажштпрыдщбхуяквбсэутэфзоулсбутедижлойжгдлоайукаташтцуйалцыуэукэетжзшвувэнжржт
жулыылойокйжвьшэоэфзофурцвэршэоатчлцтюярхцбхуажктолтцйдожкттнщтржештцсычбхэх
убщдвсжржедсцалгыуледрххддлцышрвэндтжяоукоэыисжнжвозтсбфчйжшоюэыфулзоалешэе
адлисжнжвоотдтказоэоееубясзтлогпйжзжчоэвлжбмэчуэукэецшмдлосдяоалешавэвсжейзышт
юянжулыцуледйдшвэтжтчжшэеущоажиисжнжвопозжбмвуыцвэршэойщхвыэчвщодткагыашю
эсйчтидтвьшуэуутпгшезуйрхеляпхучбхэхуюбэобтдлштгэвувэаттпераюбщдвпоещгшяхсжьжм
хгжыкбщшсштгжшйкфоошвьшуэщлуачляпрцчлнжртлояштееощойокйжвьшэоэфзофуфжсэтц
нжйлубфчзтклфчзцяыдлцыьжллчлешэеацвэршэоедсцыцстэвмфйтхджэутртжэцщукайгдьрхлу
атцвбрцщлфчуледктскуьюкаврледчояохэрхдлешавэвподвлыуоэфзофузцяыдлцыгдлэфччледск
усйдйжшэуашзфейчулгдтжзшвувэнждцвэршэосжшозтулзжюэчвьшуэрхшлешавьжзпчвжмшс
ыоуцвэршгседулдлэержхддауйьжефктадыжтпчвтнулифдлюжмдштлгэчтфюяэфиэфоулцшбщд
впожоашяшуйнжжтуфкврхипчлвэяоукхлубйтйдяохэукоэшыажшощондуледрхзжэкхвщоэфзо
фуфпзойдюооднлояшрнчлвнекэотпхкнетцуэеухлгшыдюхдткагшсбуачлешавщозтсбуатнвшфоо
юцшадяохэнжржэфзоулбщдвсжржвсйжпкрцхлцшдлюбхудлуйбщдвпогпхкуьвэгыавскайтцуэг
ыажсыщобоулкфтлештокйжвьшэоэфзофуфпцжшэхугохжашайвквээчэфзофущлцпйжэезжывч
цфотнбтофскваалтцфштцвйтцчтчццшпсыоцкбщрхвухлгшыдюярхбоыфчжжэгтажьшяннжулю
бчлцшгтоцйеуэзвзшвувэрхдпжтбхгдловужэгпчвьжкэнжржбтулсьалвкрвчцрцютяычжшйизуке
щвэгыедсцчтзтлойочдойукатюэыфулзомлешэеадщлчюдэуряжйдюянжчжщыйвчцвэйдмвавшт
адтндвэтиогдемшыашфосцуйулзжяжэувээфзоэвщозтпошфсквасжьжмхгпуйедтйвкпсэвкэхфск
ваьачвшташэоевчцфпйжкогдлогпалуэьтбхьжкхдфскваалцшржжккбдкрлешрхдфскваяжтйцшт
цалвкоэгтжвьфооашгиьжбацджэеуафодьфмдворжулгпзоюуулгдзцяыглцыашуыыцуэьтюочдло
дледоважклрхдфскваынзлтцгтжвьфооьжжатцяыилхуиоскдвбцвэяшууаважклыцрхгжтйцштца
лвкоэгттфюяэфиэгтжвьфоозцяыглцыщжажщэалвкоэеуафскваледоважклрцэфзофуботпхкнев
тэвздеоцряжмэдчйтчтфэуйцшуьрхддилхутнюкоэдчыцуйрхйледоважклойуэрхефскваууашюэс

йчткоаитвтфквяжмэуттнсквьыцуэьтэтжтбтщтловуаьыфбфмбчдвоадмгкфчдюшхэяштцуэьтбту
лжвьфооашайашгыщоижндшхгдембзажтшайлозтсбьтжтркуурхвуфшотщокатцгтжвьфооцсхд
йзуйалжтукэецргыбфштзжтвчвчджквэьтэфйжзшвбцдададибдлюэржгдийзыштюянжулппжтщ
пзомлгысжьжмхгжыттпещыцшсэюдэуряжлойжгдлобокйжвьшэоэфзофуфжюштейсштбоовщо
эфяохэнжцшмдлосдяохэофгвавштефжэатйзуймлашрцтцуттндвэтзтлодлуууьсысжовдкрвндмв
ьфинхююэуэтжгдйощдмбтцсбшыроулвууэукуацжэкуьвэьтуледчжгдлояцукглрхижэувэйдзщр
хбоувчтщжгдлойоажцачлтцнднщштцюэулалзряжмэцжжауээецряжмэшыроулвуфжюштевты
эсйулйжзбгокйжвьшэоэфзофурдатщдуотжиыжкитэвмлгшзоьжзоукоэшзфейчулдтмэшыроулв
ухвэтяомосжйвьшдбэфмхюэыфулзоалешэеадзцяыдлцыьжллутгштееощояцдевцстыэтцгтсдсы
ьжулюэхввквэгыыцчледскнзоцйеуэрхшвэфзофухусжоцвэнжашюугшхуджйтэвьфкояяьжллцж
явьфкогдлоьачвштипзолоадглзщхвщобоажьфждглщжчжэхшоэдоцйеуэрхдвцшмдлосдяобчхжж
вквмрхцугшцпзомлэчтпцшщожэизтжжтжэтцуээчтжтшайулгдвооцйеавдлустнщтулдтмэуацпа
луэгыашцщещрхунуэсжеоуледчжкхцбхуьдлодцедиоедюжыэюбяпдэтлтцашхбхлрдилхутнюкб
чашуйсьынвэуойдуфдтлойжзшрнчллопоажшоршхюбщдвсжипйжзхтквэнжулэочдойукатудедт
лгшнжкщгшьжйюдэуряжлойжгдлойокйжвьшэоэфзофушыжкитэвмвбехэнжулрвлысдмэшыаш
аьцтиваачвйдшоиовуоцтнуйнжржзшвувээочлбфсбтцчвнжжэфчадувжпчлвэяоукоэизюэчвьшу
эрхчпчвдлалвкбчажндсдштшоптхжмэчвщохбтевцшсчнхктгутжкгыловэхвштэтрясдршгепоад
штзоукоэчлезлозтсбфчщдшхюэыфулзоалешэеадэотпцжюяхжгдлогпгштжйдцдштевууеуптхж
мэчвяязжгэуахуцпжтцтяыдлтнщтжисжнжвозтсбйсщюлттлыцнжулнокйжвьшэоэфзофуфжсэтц
фчюэыфулзоалешэеадзцяыдлцыэфзоулсбшыюэошхвьшдбэфедштивгпжтщпзомлгысжьжмхгж
ыттпещыцшсьжндсдлодлешавэвпошфскващоашайашгыщоийвкмлцыйдэтецбщрхяцпташайаш
гыщокбчлцшгтктажтшайулдтмэцжявьфкогдглэфзоултцчлвкюучлвкюбвуюокаэошйашайашгы
щомледоважклнжржтнсквьыцуэгыхбтевцшсыодфскваяпцшядшосдяоюбхуяквбсэфчэфзоулсб
фчжвьфооэфйжэтедьжмхэфеднтолзлешцпгшхлцшсшепйдмюяшгбчлцшшыедхшрнхлвцстьжж
ауээевтщожтукэевтэлешдокхулепстыэфшеэотэфзоулпошфскваэфеднтолашайашгыщовбчлцш
уттндвэтиогддлцшмдлосдяоаожтукэецргсэфедилцшбщрхгпжтщпзомлгытжтйуэрхгпжтюуимд
вчцвэнжшклжявьфкогдломлешавьжжэфошфскваууюууажлажюяхжгдяяцыюудвыэгткоштшот
лубюуашайашгыщокучлнжцыэвлшдвьжедрхндлтщдмходдэвцуйрхдвчдпрэоалылжтщойэгташ
айашгыщомвфехдмэгтшкмюдэуряжлойжгдлозцптржйдйжщжчжщыйвчцвэнжржсждпчттвхвь
шуэеэхбчлцшеуяпхкнейсэвйоэфзоулебчдподпжтщпзомлгыджыэчвмлцыйдашюугшашайашгы
щомледоважклнжржтнсквьыцуэгымхнжтлешавэвпошфсквамхнжтлешавэвпошфсквазцяыдлц
ычвнжжэеукдтлцшхуедсцалгыэфзоулсбфчюэошхвьшдбэфмхмхнжтвавштадчлнжртлоижэувэу
уаьыфашфосцуйулзжвоажьшянчтловуьжгдйжжэфжсэтцгжбмдвчцвэнжржедтйвквэгыьшвйтоь
жгдиэуацпйжэезжывчцрцвкбщюэфшеэндцпжтцтяыдлцыулгпвэустперыдшосдяояжбмдвчцвэн
жржьшвйрццстжзжтфяэчвяякдтлцштцожиуяштцуэгымхмбуууьнжажщштецтшояяйджэжлжтм
эьтыцкттэьтжэжглодюубьжмхщлчвавштадбтйачввйфшулдтмэизчлнжртлодцофьшвэлодюубь
жмхщлчвшрыдюянжчбхэхубщдвподюубьжмхулрнюкоэчвяяештцвэпштееощолпйжыфтлыцрх
швюкештцвэмьэелойдптчтлолштееощодледоважклхвлыуоашцшуйнжнтуаедмозтсбьткдтлцш
вцждулнжулгисжнжвосжнтуаедмозтсбутажыжйтлогжтжюжкхржшэчледлеалнжгпхкуьвэьтул
едрхмхнжтлешавэвпошфсквауюгшфшядшосдяоалешавэвпошлтцфштцафскважтсфяыьжйжел
ешавэвсжржмхмбшыжкитэвйеубхэтпйжодяпжтшкуьвэгыхэкхедиддлтнмттлыцнжтнжвыжжкв
эофбэгжазуйюучвяятжчлдтэвчцгызжзшвувээозпйжуледовчцдвьжюучвыэизюэхлешукоэтцжм
двчцвэрхшюцшдпцдштйттпчвтннжржтпйжодалтцфшнжржашайыжйтлоийбчулифембззтжтф
бхкяныэгыашфосцуйулгдяпчлжтэквэгымхнжтюцшвокфдлтпйжувашчвйдчжчоэвлпуйзжтйбчу
леовуедфэцжюштерхшюубьжйжилуббзндтфйждтряадштзоукоэуатнцдржтжулыылокэхввквэг
ыбцвкбцвэьтсжшозтулгдоцтнуйнжржзшвувэавтцгшртовчцтцуэьтеощжиледоважклцрвэеэхле
шавэвподфскваюэхвашчвжкгыглчдоьяцфеджлэчвщозжжкещвэгыщжажщэалвкоэизьшвйтциз
жтуфквтцзпюбтцдчэфзоулбщдвпойвбехэнтршхюбщдвсжгшхвашайвквэьтжвьфрпчлгшзоьжзо
алжтюжгдлокбхуожклнжулюуаьыфтпйжтжвошойэеуьйшзуйууавимдвчцвтэвцжыэщгвэьтсжщ
юмояовэаицдулбщнжулюэубсьэхипйжютолйжулсйшзуйтцйдптчтлолпйжавчжчоэфдтшозтлоб
ехледыэхлешэеацтшайктгэуэььгпзодтцтрхфэцщвэгыщлуахбыипюбрьтолсйяыктсжьжмхфтзш
цпбчсббзуледнпцжыэщгвэгсрудвыэхудэхввквэгсуледйдсжщюмояовэаицдулбщнжулыцвкюбт
нзочдлоиагшадлознвкмагырцулзойочдшоогдткрфшгыажьшяннжулыцэфзоулсббзжвьфмдшю

цшвокфглтпйжтжбмэчтпйжуюцшвокфдлмхмбяпгшзжзбхлаацшэофпцдштйттпчвтнрхйвашчвмхмбыцьжйжзбхлаацшэомх

Дешифрований текст:

лодостьеленывбездействиивнешнемвовнутреннейборьбеитревогеподругунеенебылоизовсехдевицпосещавшихдомстаховыхонанесошласьнисоднойродительскаявластьникогданетяготеланаделенойасшестнадцатилетнеговозрастаонасталапочтисовсемнезависимаоназажиласобственнойсвоеюжизньюножизньюодинокойеедушаиразгораласьипогасалаодинокоонабиласькакптицавклеткеаклеткинебылониктонестеснялееиниктонеудерживалаонарваласьитомиласьонаиногдасамасебянепонималадажебоялась самойсебявсечтоокружалоееказалосьейнетобессмысленнымнетонепонятнымкакжитьбезлюбвиалюбитьнекогодумалаонаистрашностановилосьейотэтихдумотэтихощущенийвосемнадцатилетоначутьнеумерлаотзлокачественнойлихорадкипотрясенныйдооснованиявесьееорганизмотприродыздоровыйикрепкийдолгонемогсправитьсяпоследниеследыболезниисчезлинаконецноотецеленыниколаевнывсеещенебезозлобленияотолковалобеенервахиногдаейприходиловголовучтоонажелаетчеготочегониктонежелаеточемниктонемыслитвцелойроссиипотомонаутихаладажесмеяласьнадсобойбеспечнопроводиладеньзаднемновнезапночтотосильноебезымянноесчемонасовладетьнеумелатакизакипаловнейтакипросилосьвырватьсянаружугрозапроходилаопускалисьусталыеневзлетевшиекрыльянопорывыэтинеобходилисьейдаромкаконанистараласьневыдатьтогочтовнейпроисходилотоскавзволнованнойдушисказываласьвсамомеенаружномспокойствииироднымееечастобыливправепожиматьплечамиудивлятьсяинепониматьеестранностейвденьскоторогоначалсянашрассказеленадольшеобыкновенногонеотходилаотокнаонамногодумалаоберсеньевеосвоемразговореснимпотребностьвзащитеинформациивозникаетвсвязиснеобходимостьюобеспечитьсекретностьисследованийвстратегическихобластяхправильнораспределятьинформациюопромышленныхразработкахирегулироватьинформациюоличностивсовременномобщественачаловосьмидесятыхгодоврассматриваетсякакначальныйпунктогдасоциальныепротестывдемократическихстранахпомоглисплестисьглобальнойсетихакеровполитическийфлиртнапочвенарушенияправчеловекапородилтьмуорганизацийхакероввмассестранмирапочтиодновременноменеечемзагодэтигруппыузналипрелестьсотрудничестваихчленысвободнообменивалисьидеямичерезнациональныеграницычастопоукраденнымпаролямдающимбесплатныйдоступктелефоннойсетинесколькопричинобъединившисьвместесделалимеждународныйкомпьютерныйразбойлекгимидейственнымновыетехнологиисоздавшиеболеемощныеидешевыекомпьютерыразвитиекоммуникацийдлясвязиимеждународныйхарактерстандартовустановленныхтранснациональнымикорпорациямивпринципеестьлишьдвавидаугрозыраскрытиеивидоизмененииеданныхраскрытиеданныхпредполагаетчтоком утослучайноилипослецеленаправленныхдействийстализвестенсмыслинформацииэтотвиднарушениявстречаетсянаиболеечастопоследствиямогутбытьсамыеразныееслипохищентекстсткнигисправочниканакоторуюпотраченымесяцыработыдесятковлюдейтодляколлективаавторовэтокатастрофаипотеримогутвыражатьсявтысячахдолларроводнакоесликнигаужеизданатодостаточнолишьслегкапожуритьпохитителяирассказатьослучившемсяватделеновостейгазетыилипотелевидениюпохитительможетсделатькнигевеликолепнуюрекламуоченьважнуюинформациюоберегаемуюотраскрытияпредставляютсведенияолюдяхисториболезнисьмасостоянияхсчетоввбанкаходнакопомнениюбольшогочисласпециалистовугрозыличностисведениемкомпьютеровостались натомжеуровнеивтомжесостоянииичтоидообширногоиспользованияэвмведениевсовременномтуризмстановитсявсеболееважнойбыстроразвивающейсяотрасльюхозяйстваходыоттуризмастановятсяважнойчастьювалютныхпоступленийвомногихстранахразвитиетуризмаспособствуетростуобщественногопроизводстваулучшениюегоструктурыроступроизводительноститрудавомногихотрасляхэкономикидаженеимеющихктуризмупрямогоотношениямеждународноетуристскоепотреблениестимулируетмногочисленныеэкономическиепроцессыоткрывающиедополнительныерынкидляпродукциинетуристскихотраслейсоздаваятемсамымусловиядлярастапроизводствавсеэтифакторыделаютразвитиеиндустриитуризмаоченьважнымдлястранспереходнымтипомэкономикиеономическиетрудностикоторыепереживаютэтигосударстванемогутнесказатьсянауровнеразвитиятуризманоприэтомкаждаястранаимеетвэтомотношениисвоюспецификуцельданнойработырассмотретьипроанализироватьорганизациютуристскойдеятельностивстранепереходнымтипомэкономикинапримеревенгриивначалерассматрива

ютсятеоретикометодическиеположенияисследованиязатемдаетсяоценкаразличныхфакторовр
азвитияиндустриитуризмавенгрииприродноресурсныйкультурноисторическийиинфраструкт
урныйпотенциалкомплексноетуристскоерайонированиедалееепроводитсяанализсовременного
состоянияиндустриитуризмавенгриииеотдельныхкомпонентовнафонеобщегоуровняэкономич
ескогоразвитиястрановыдаетсяоценкасоциальноэкономическойролииндустриитуризмавэконом
икевенгриииивзаключениепроводитсяобщийанализорганизациитуристскойдеятельностивстра
нахспереходнымтипомэкономикивобщемивенгриивчастностивенгияпринадлежакстранамспе
реходнымтипомэкономикиимеетмногиеспецифическиечертыкоторыеотличаютееотдруги
хстранэтоготипавотношенииразвитияиндустриитуризмаосновнойтакойчертойявляетсяточтот
уризмвенгрииразвиваетсяужедавноешевначаледвадцатоговекавэтойстранесложилисьтрадици
онныетуристскиесвязитуризмявляетсяважнойотраслью народногохозяйствасовременнойвенгр
иииколичествоиностранныхтуристовпосещающихвенгриюрастетизгодавгодтомунемалоспособ
ствуетбогатейшийкультурноисторическийиприродноресурсныйпотенциалатакженациональн
аяполитикастраныоблаституризмапринаписанииработыбылиииспользованыматериалывенгер
скоготуристическогобюроинформационноготуристическогобюроглаваторетикометодические
положенияисследованияпонятиеиструктураиндустриитуризмапоодномуизопределенийтуриз
мэтопроизводствоиобменуслугитоваровудовлетворяющихличныематериальныеидуховныепо
требностикоторыесвязанысвременнымпребываниемвнепостоянногоместажительствавцеляхо
тдыхалеченияразвлеченияитакдалееиндустриятуризмаэтофункциональнохозяйственнаясисте
маобеспечивающаяпроизводствоиобментуритстичекихуслугкоторыеподразделяютсянауслуг
игостеприимствапроживаниепитаниебытовыеуслугиторговлякультурныеуслугиоздоровитель
ныеуслугиприэтомглавнымиусалугамигостеприимстваявляютсяпроживаниепитаниетранспор
тныеуслугибытовыеуслугиторговлявтомчислесувенирамиспортивныеоздоровительныекульт
урныеуслугиявляютсядополнительнымиуслугитранспортавтуризмеиспользуетсяавиационны
йжелезнодорожныйавтомобильныйиводныйтранспорткданнымуслугампринадлежитэкскурси
онноеобслуживаниеперемещениемеждупунктамимаршрутабронированиеместуслугипредпри
ятийоказывающихпосредническиерекламныемаркетинговыеуслугисюдавходитреализацияпу
тевоксоставлениетуроврекламамаркетинговаядеятельностьпредприятиякоторыеобеспечиваю
тфункционированиеиндустриитуризмаобразуютееинституционноорганизационнуюсистемув
неевходятправовоеобеспечениетаможняконсульскаяслужбафинансоваяибанковскаясистеман
алогообложениестрахованиевалютныйобменнаучныеисследованияиподготовкакадровинстит
уционноорганизационнаясистемаобразуетнадстройкуиндустриитуризмаееебазисомявляетсят
ерриториальнохозяйственнаясистемаспецификойструктурыиндустриитуризмаявляетсяточтое
еразвитиевызываетновыезанятостинаселенияивотрасляхсвязанныхстуризмомкосвенноприме
ромможетслужитьточтообслуживаниигостейпринимаютучастиеиполучаютдоходылицасвязан
ныесорганизациейзоелищныхмероприятийспортивныхсоревнованийсосредствамисвязисетью
общественногопитанияпрачечныхбанковистраховыхкомпанийврачиработникипунктовпрокат
аавтомобилейпродажибензинасувенировработникиполиграфическойпромышленностиитакда
леехарактернойчертойфункционированияиндустриитуризмаявляетсясезонностьсвязаннаяпре
ждевсегосналичиемсвободноговремениотпусковосновноймассыпотенциальныхиностранны
хпосетителейпоказателисезонностиоказываютбольшоевлияниенастепеньзагрузкиматериальн
отехническойбазыиндустриитуризмаиииспользованиеперсоналатемсамымсезонностьвомного
мопределяетобщеюэкономическуюэффективностьиндустриитуризмаосновойиндустриитуриз
маявляетсятуристскаяинфраструктуратевсепредприятиякоторыеобеспечиваютоказаниетурис
тскихуслугтипредприятияделятсянапервичныевсепредприятиякоторыенепосредственнообслу
живаютттуристовотелимотеликемпингиитдпредприятиятранспортногообслуживанияоказыва
ющиеуслугипореализациикомплекснойтуристскойуслугитуроператорытурагентытуроперато
ркрупнаяфирмкотораяразрабатываеторганизуетиреализуеттурыивыступаетнарынкетуристки
хуслугтурагентпредприятиекотороеобеспечиваеторганизациюиреализациютуравторичныепр
едприятиясозданныепреимущественнодляобслуживаниятуристовноихуслугамимогутпользов
атьсяиместныежителиктакимпредприятиямотносятсярестораныкафебарысауныводныестанци
иитдтретичныепредприятиясозданныедляфункционированиявсегонародохозяйственногоком
плексастраныкоторымипользуютсяитуристыктакимпредприятиямотносятсянапримерпред
приятиятранспортногообслуживаниярыноктуристскихуслугрыноктуристскихуслугявляетсяо

сновнымфакторомразвитиятуристскойинфраструктурырыноксистемаотношенийобменамежд упроизводствомипотреблениемтоваровнаосновеобщественногоразделениятрудаитоварногоп роизводствавеличинарынкаопределяетсястепеньюспециализацииобщественноготрудавсюсов окупностьфакторовформированиярынкаможноподразделитьнавнутренниеивнешниевнешние факторыэтосистемамежгосударственныхотношенийвнутренниефакторыэтосоциальноэконом ическиефакторыстабильностьуровеньразвитияпродуктивныхсилуровеньжизнинаселенияразв итиетранспортасвязипроизводногеографическиефакторывчастностиэкономикогеографическоеп оложениеособовыгоднотранзитноеположениестранырыноктуристскихуслугсферареализации туристскихтоваровиуслугрегуляторомтуристскогорынкаявляетсязаконспросаипредложенияо нвыражаетобъективнообусловленнуюнеобходимостьсоответствиявовремениивпространствес тоимостныхинатуральновещественныхформплатежеспособногоспросаитоварногопредложен иядействующихчерезколебанияпроизводстваипотреблениярынокформируетспросспроснаход итсяподвоздействиемразнообразныхфакторовтакихкакуровеньматериальногоблагосостояния населенияувеличениеколичествасвободноговременисовершенствованиевидовтранспортацен ынатуристскиеуслугинаспросвлияюттакжевозможностивовлеченияидополнительныхтрудовых ресурсоввпиковыйтуристическийсезонгеграфическоераспределениеуслугпотерриториитребо ваниякомфортностимеждуспросомиличнымидоходамисуществуетсоотношениекоэффициент эластичностинакаждыйпроцентростадоходовнаселенияпроисходитувеличениезатратнатуриз мвсреднемнанижеприведенызначенияэтогокоэффициентадлянекоторыхевропейскихстранпоо тношениюкместномунаселениюстранакоэффициентэластичностивеликобританиягерманиябе льгияавстрияиталияшвейцарияпотребностивтуристскихуслугахформируютспособщийспрос формируетрынкипервойкатегорииаплатежеспособныйспросрынквторойкатегорииры

(Текст збережено у файл: decrypted_a9_b500.txt)

Висновки:

У ході виконання роботи ми розібралися з принципом дії афінного шифру біграм і на практиці застосували метод частотного аналізу для його розкриття.

Ми реалізували програму, яка автоматично обчислює частоти біграм, формує рівняння для пошуку ключів та перевіряє кожен варіант розшифрування.

У результаті аналізу вдалося знайти правильний ключ a=9,b=500 і відновити осмислений текст.
Це дозволило зрозуміти, як математичні методи - зокрема робота з оберненими елементами та лінійними порівняннями - можуть бути ефективно використані в криптоаналізі.

Завдяки роботі ми не лише закріпили знання з модулярної арифметики, а й побачили, як теорія перетворюється на реальний інструмент для розшифрування повідомлень.