МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

Комп’ютерний практикум №3

з дисципліни

Криптографія

на тему:

# «**КРИПТОАНАЛІЗ АФІННОЇ БІГРАМНОЇ ПІДСТАНОВКИ**»

Виконав:

Студент групи ФБ-91

Шостак А. А.

Київ 2021

**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.

**Хід роботи:**

- Провести текст через фільтр (перевіряю, чи всі літери були замінені на відповідні їм у даній роботі та автоматизовано видаляю символ переходу на новий рядок).
- Реалізував усі необхідні операції для знаходження ключа.
- Провів аналіз частотності біграм, що не перетинаються, щоб поставити їм у відповідність найчастіші біграми російської мови. Отримав наступне:

| | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| а | 0 | 0.000344828 | 0 | 0 | 0.000344828 | 0.00344828 | 0 | 0.00103448 | 0 | 0 | 0.00103448 | 0.000344828 | 0.00344828 | 0.000689655 | 0.0110345 | 0.000689655 |
| б | 0.000344828 | 0 | 0 | 0 | 0 | 0.000344828 | 0 | 0.00793103 | 0 | 0.00103448 | 0 | 0 | 0.00103448 | 0.000689655 | 0 | 0.000344828 |
| в | 0.000344828 | 0 | 0 | 0.000344828 | 0 | 0.00241379 | 0 | 0.00655172 | 0 | 0 | 0.000344828 | 0.000689655 | 0.00206897 | 0 | 0.00448276 | 0 |
| г | 0 | 0.00827586 | 0 | 0 | 0 | 0 | 0 | 0.000344828 | 0 | 0 | 0 | 0.00517241 | 0 | 0.000689655 | 0 | 0 |
| д | 0.000344828 | 0 | 0.00586207 | 0.000689655 | 0 | 0.000344828 | 0 | 0.000689655 | 0 | 0.00103448 | 0.000344828 | 0.000689655 | 0 | 0.000344828 | 0.0193103 | 0.00241379 |
| е | 0 | 0 | 0 | 0 | 0 | 0.000344828 | 0.00413793 | 0.00241379 | 0.000344828 | 0.000344828 | 0.000689655 | 0.00137931 | 0 | 0 | 0 | 0.000344828 |
| ж | 0 | 0.012069 | 0.000344828 | 0.000689655 | 0 | 0.00206897 | 0 | 0.00586207 | 0 | 0 | 0.00103448 | 0.0062069 | 0 | 0 | 0 | 0.00103448 |
| з | 0 | 0.00137931 | 0 | 0.00103448 | 0 | 0 | 0 | 0.000689655 | 0 | 0 | 0.000689655 | 0.00793103 | 0.000689655 | 0 | 0.00103448 | 0 |
| и | 0 | 0.000689655 | 0 | 0.000344828 | 0.00206897 | 0.000689655 | 0 | 0.000689655 | 0 | 0 | 0.00241379 | 0.00517241 | 0 | 0 | 0 | 0.00517241 |
| й | 0 | 0 | 0 | 0.000689655 | 0 | 0 | 0 | 0.00103448 | 0.00275862 | 0 | 0.000344828 | 0 | 0 | 0 | 0 | 0 |
| к | 0 | 0.00172414 | 0 | 0.00172414 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0037931 | 0.00103448 | 0 | 0 | 0 | 0 |
| л | 0 | 0 | 0.00206897 | 0.00172414 | 0 | 0.00275862 | 0 | 0.00965517 | 0 | 0 | 0.000344828 | 0.00586207 | 0.000344828 | 0.000689655 | 0.00310345 | 0 |
| м | 0.00172414 | 0.00103448 | 0 | 0.0037931 | 0 | 0.00103448 | 0 | 0.00413793 | 0 | 0 | 0 | 0.00206897 | 0 | 0 | 0.00344828 | 0.0062069 |
| н | 0 | 0 | 0 | 0.000344828 | 0.00206897 | 0 | 0.0103448 | 0.000689655 | 0.00137931 | 0 | 0 | 0.00206897 | 0.000344828 | 0 | 0.000344828 | 0.00241379 |
| о | 0.00172414 | 0.000689655 | 0 | 0 | 0 | 0.000689655 | 0.000689655 | 0.00344828 | 0 | 0 | 0.00517241 | 0.00310345 | 0.000344828 | 0 | 0.000689655 | 0 |
| п | 0 | 0.00551724 | 0.000344828 | 0 | 0 | 0 | 0.00586207 | 0.00758621 | 0.00103448 | 0 | 0 | 0.00448276 | 0 | 0 | 0.00137931 | 0.000344828 |
| р | 0 | 0.00103448 | 0 | 0.00758621 | 0 | 0.000344828 | 0 | 0.000344828 | 0 | 0 | 0 | 0.00172414 | 0 | 0 | 0.000689655 | 0 |
| с | 0 | 0.00137931 | 0 | 0 | 0.00103448 | 0.00137931 | 0.000344828 | 0.00862069 | 0.000344828 | 0 | 0.00103448 | 0.00103448 | 0.000344828 | 0 | 0.00241379 | 0.00103448 |
| т | 0.00103448 | 0 | 0 | 0 | 0 | 0 | 0.000344828 | 0.00137931 | 0 | 0 | 0.00103448 | 0.000344828 | 0 | 0 | 0 | 0 |
| у | 0 | 0.000344828 | 0 | 0.01 | 0 | 0.000689655 | 0 | 0.000689655 | 0 | 0 | 0 | 0.000344828 | 0.00172414 | 0 | 0.00758621 | 0.00103448 |
| ф | 0 | 0.00172414 | 0 | 0.000344828 | 0 | 0.00206897 | 0.00103448 | 0.00275862 | 0 | 0 | 0 | 0.00827586 | 0.00172414 | 0 | 0.00103448 | 0.00689655 |
| х | 0.000344828 | 0.000344828 | 0.000344828 | 0 | 0 | 0.00310345 | 0 | 0.00344828 | 0 | 0 | 0.000344828 | 0.00172414 | 0.00172414 | 0 | 0 | 0.000344828 |
| ц | 0.000689655 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00689655 | 0.00275862 | 0 | 0.00103448 | 0 | 0.00827586 |
| ч | 0 | 0.00137931 | 0.00310345 | 0.000344828 | 0 | 0 | 0 | 0.000689655 | 0 | 0 | 0 | 0 | 0.00172414 | 0.00137931 | 0 | 0.00517241 | 0.000344828 |
| ш | 0 | 0.000344828 | 0 | 0.0134483 | 0 | 0.000344828 | 0.000344828 | 0.00172414 | 0 | 0 | 0 | 0.00517241 | 0.0037931 | 0 | 0 | 0 | 0.00413793 |
| щ | 0.000689655 | 0 | 0 | 0.00103448 | 0 | 0 | 0 | 0.00413793 | 0 | 0 | 0.00172414 | 0 | 0.000689655 | 0 | 0 | 0 | 0 |
| ы | 0.000344828 | 0 | 0.00137931 | 0.000344828 | 0 | 0.000689655 | 0.000344828 | 0.00103448 | 0 | 0 | 0 | 0.000344828 | 0.00206897 | 0.000689655 | 0 | 0 | 0.00137931 |
| ь | 0.00241379 | 0 | 0 | 0.00758621 | 0.00137931 | 0.000689655 | 0 | 0.0037931 | 0 | 0 | 0 | 0.00275862 | 0.00344828 | 0 | 0 | 0 | 0.000689655 |
| э | 0.000344828 | 0 | 0 | 0.00206897 | 0 | 0.00241379 | 0.000689655 | 0.00482759 | 0 | 0 | 0.000344828 | 0 | 0.000689655 | 0 | 0.000689655 | 0 | 0 |
| ю | 0 | 0 | 0 | 0.000689655 | 0.000344828 | 0 | 0 | 0.00517241 | 0.00137931 | 0 | 0.000689655 | 0.00517241 | 0 | 0 | 0 | 0.00275862 | 0 |
| я | 0.000344828 | 0.000689655 | 0 | 0 | 0.00482759 | 0.000689655 | 0.000689655 | 0.00482759 | 0.00206897 | 0.00103448 | 0 | 0.00241379 | 0.000344828 | 0 | 0.000344828 | 0.000344828 | |

| | р | с | т | у | ф | х | ц | ч | ш | щ | ы | ь | э | ю | я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| а | 0 | 0 | 0 | 0.000344828 | 0 | 0.000689655 | 0 | 0 | 0.00310345 | 0 | 0 | 0.000344828 | 0.00172414 | 0 | 0.000344828 |
| б | 0.00344828 | 0 | 0.00344828 | 0 | 0.000344828 | 0.000344828 | 0.000344828 | 0 | 0.000689655 | 0 | 0 | 0 | 0.00137931 | 0 | 0.00241379 |
| в | 0 | 0 | 0 | 0.00344828 | 0.000344828 | 0.00482759 | 0.000689655 | 0.00103448 | 0.000344828 | 0.000689655 | 0 | 0 | 0.00206897 | 0 | 0.000689655 |
| г | 0 | 0 | 0 | 0.00862069 | 0 | 0.00793103 | 0.00689655 | 0.00172414 | 0.000689655 | 0.000689655 | 0 | 0 | 0 | 0 | 0 |
| д | 0 | 0.000689655 | 0 | 0.0103448 | 0 | 0.00586207 | 0.00206897 | 0.00103448 | 0 | 0.000344828 | 0 | 0.000344828 | 0.000689655 | 0 | 0 |
| е | 0 | 0.000344828 | 0 | 0.000689655 | 0 | 0 | 0 | 0 | 0 | 0.000344828 | 0 | 0.00310345 | 0.01 | 0.000689655 | 0.00172414 |
| ж | 0 | 0 | 0 | 0 | 0.00172414 | 0 | 0 | 0.000344828 | 0 | 0 | 0 | 0 | 0.00206897 | 0 | 0 |
| з | 0 | 0 | 0 | 0.0103448 | 0 | 0 | 0 | 0.0113793 | 0.00172414 | 0 | 0 | 0 | 0.00862069 | 0.000344828 | 0.00172414 |
| и | 0.000344828 | 0.000689655 | 0 | 0 | 0 | 0.0037931 | 0 | 0.000344828 | 0.000344828 | 0.000344828 | 0.000689655 | 0 | 0.00689655 | 0.000344828 | 0 |
| й | 0.00689655 | 0 | 0 | 0 | 0 | 0.000689655 | 0 | 0.00689655 | 0 | 0 | 0 | 0.00241379 | 0.00103448 | 0 | 0.00448276 |
| к | 0.00103448 | 0 | 0 | 0 | 0.00344828 | 0.00103448 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.000344828 | 0 |
| л | 0.00172414 | 0 | 0.000689655 | 0.00689655 | 0 | 0.00172414 | 0 | 0.000344828 | 0.00137931 | 0 | 0 | 0.00275862 | 0.000344828 | 0.00137931 | 0 |
| м | 0 | 0 | 0 | 0.000344828 | 0 | 0.00413793 | 0 | 0 | 0.000689655 | 0.000689655 | 0 | 0 | 0.00103448 | 0 | 0 |
| н | 0.000344828 | 0 | 0 | 0.0168966 | 0.000344828 | 0.00137931 | 0 | 0 | 0.000689655 | 0 | 0 | 0 | 0 | 0.00137931 | 0 |
| о | 0 | 0 | 0 | 0.000344828 | 0 | 0 | 0 | 0.000344828 | 0.000344828 | 0.000689655 | 0 | 0.00103448 | 0.00344828 | 0.00137931 | 0 |
| п | 0.00137931 | 0.000344828 | 0 | 0.000344828 | 0 | 0.000689655 | 0 | 0.00241379 | 0.00241379 | 0.000689655 | 0 | 0 | 0.000689655 | 0 | 0 |
| р | 0.000344828 | 0 | 0.00172414 | 0.00482759 | 0 | 0.0162069 | 0 | 0.00241379 | 0 | 0.00758621 | 0.000344828 | 0 | 0.00241379 | 0 | 0.000344828 |
| с | 0 | 0 | 0 | 0.0037931 | 0 | 0.00137931 | 0 | 0 | 0 | 0.000689655 | 0 | 0 | 0.000344828 | 0.000344828 | 0 |
| т | 0.000344828 | 0 | 0 | 0.000344828 | 0.00275862 | 0.000344828 | 0.000344828 | 0.000344828 | 0 | 0.00344828 | 0 | 0 | 0.00103448 | 0 | 0.000344828 |
| у | 0.00275862 | 0 | 0 | 0 | 0 | 0.00206897 | 0 | 0 | 0.00241379 | 0 | 0 | 0 | 0.00137931 | 0 | 0 |
| ф | 0.000344828 | 0.000344828 | 0 | 0.0103448 | 0.00413793 | 0.0127586 | 0.00206897 | 0.000689655 | 0 | 0 | 0 | 0 | 0.00241379 | 0.000344828 | 0 |
| х | 0 | 0 | 0 | 0.00275862 | 0 | 0.000344828 | 0 | 0.000689655 | 0 | 0 | 0 | 0 | 0.00206897 | 0.000344828 | 0 |
| ц | 0.000344828 | 0.000689655 | 0 | 0.0037931 | 0 | 0.00482759 | 0 | 0.00448276 | 0.00172414 | 0 | 0 | 0.00103448 | 0.00172414 | 0 | 0 |
| ч | 0.000689655 | 0 | 0 | 0 | 0 | 0.000689655 | 0 | 0.000689655 | 0.000344828 | 0 | 0 | 0.000689655 | 0.00275862 | 0 | 0.00241379 |
| ш | 0.000689655 | 0 | 0 | 0.00896552 | 0 | 0.00344828 | 0.00103448 | 0.000344828 | 0 | 0.000689655 | 0 | 0 | 0.000689655 | 0.0034828 | 0 |
| щ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00310345 | 0 | 0 | 0 | 0 | 0.00137931 | 0.000344828 |
| ы | 0.00137931 | 0 | 0.000689655 | 0.00241379 | 0 | 0 | 0 | 0.0062069 | 0.000344828 | 0 | 0 | 0 | 0 | 0.000344828 | 0 |
| ь | 0.0062069 | 0 | 0.00206897 | 0.00275862 | 0 | 0.000689655 | 0 | 0 | 0 | 0 | 0 | 0 | 0.00586207 | 0 | 0.00241379 |
| э | 0.000689655 | 0 | 0 | 0.00275862 | 0.000689655 | 0.00103448 | 0 | 0.000344828 | 0.00310345 | 0 | 0 | 0.000344828 | 0.000689655 | 0 | 0.000344828 |
| ю | 0 | 0 | 0 | 0.00137931 | 0 | 0.00206897 | 0 | 0.00655172 | 0 | 0 | 0 | 0 | 0 | 0.00689655 | 0 |

**Найчастіші біграми:**
**array[4][14] = 56 - > «до»**
**array[13][19] = 49 - > «ну»**
**array[16][21] = 47 - > «рх»**
**array[24][19] = 40 - > «шу»**
**array[24][3] = 39 - > «шг»**

- Перебираю усі можливі комбінації (за винятком використання однакових біграм з ШТ та ВТ) за провожу процес знаходження параметрів a та b, використовуючи лінійні порівняння. Усі можливі ключі:
(208,176), (835,577), (959,267), (402,156), (753,384), (520,484), (117,360), (956,301), (126,944), (441,76), (773,293), (2,293), (844,200), (649,944), (559,404), (5,259), (188,267), (312,577), (440,588), (177,734), (735,300), (259,250), (521,67), (139,796), (728,238), (396,298), (784,882), (822,820), (859,355), (226,355), (233,417), (301,882), (702,405), (565,357), (102,300), (660,734), (701,571), (638,310), (483,217), (939,596), (260,311), (311,186), (94,341), (727,655), (323,572), (650,696), (235,665), (478,665), (867,541), (390,572), (22,286), (234,227), (726,217), (571,310), (232,834), (303,579), (737,455), (818,516), (729,105), (580,734), (611,300), (401,419), (658,360), (381,205), (86,484), (224,484), (350,639), (613,360), (143,423), (560,520), (875,455), (348,579), (493,817), (764,155), (485,372), (537,862), (468,349), (752,124), (938,403), (732,776), (197,50), (209,81), (423,794), (476,794), (23,763), (702,50), (424,304), (229,390), (538,372), (259,155), (261,500), (461,93), (709,434), (680,863), (700,761), (172,868), (327,620), (331,874), (500,207), (789,393), (337,827), (252,827), (634,641), (89,207), (281,398), (630,387), (624,434), (872,93), (0,744), (0,0).
- Провожу процес розшифровки з усіма ключами та перевіряю отриманий текст на шум: підраховую частотність біграм та окремих літер — якщо значення частотності будь-якої біграми перевищує біграму «ст» або частотність будь-якої літери перевищує частотність літери «о» — я відношу розшифрований текст до так званого шуму, оскільки ці характеристики мають зберігатися. Якщо текст пройшов перевірку на шум — він виводиться на екран з вказанням ключів. В іншому випадку — його вивід на екран ігнорується. Використовуючи ці «прийоми» я отримав настіпні ключі: (208,176), (177,734) та (735,300). Проте змістовним текст виявився лише при розшифруванні з використанням ключа **(735,300).**

**ШТ (23 варіант):**

дплргшрщзчфуилшччьолрхсжфпцнбтйяэзьзншпзвлплщуфонубинптщьаьчжлсзбцдщзчпжйргб
схфэчвездусззлгудудуэедхтярхездуежшзфхшуфхцппшлхтрфхюхдпшгташкнжрэокфхшруздуу
шлушудойгтфдхуртзлефунптщзчжлдщвзоюэтфхфлаэзонузгтфйинпшэеьщлрбнладнптщзчщуь
лдщзчшгуомээаээзээябрипьеуггбилцчбжрщэнзуфонубиязйэщйбиэхфчугвздуокйрыюбдбжика
мэрцэьгфхнхзшщюбжллжзщэйхщхзлмхизязеэцэпжлряхщхбрьгбрцэтщфпяхпхвуобзэрглларчуг
вздуфущухлфетжэррэоьейпжнуежлонусуфуцарголжчцлжбккеяолбтплщущэвмфхнджбглюлп
блющзгнчоргзчдозэргфуруюдрхыедхфудоррлойяокзчфхчявчшжочбяелуэпжхпзядхсехескпзс
пщйбжсзтэрщаоргллрчугзягужблтжбэрзлчзлгуофхяхщщипугдвпладеьчрвмьруозчгунмбяпвок
рщеэрящлиршкшлбруоежжзядоюшэьчсздхфоглупшгчоцхоюьчышйькхдхамфжуобтдхюххеск
йрзунхюлфхцупонубтргфужбзэщзнубжрхолырвмьрсодукйрээялжэбжщюуосоумьчюхлхжлн
учэрщбтргщхчьяойзплцупрзэккпзнуожщюуожбаоргсоумоаипшгпшцумзаохйрхолхкнжрэгнэр
луцьугеяежмпзчжлеюсуугпшйчсохэсууггбхлрхвуппщйвонудщеэсюмгтфлэдцжвйялзьудоллрч
угнжрхолчэцкнжмпхврхькшгипщйчвюлщудочонучвокнжзумздоиеызмбаоугллхкпзрбчмжфих

гуфлцлхбэтээфцйчгбяйоаячшувумлурргрхплхехкфхнуюэшгргшекбамшэфцчвцчэтрхэефбккрг
гбниподеуггбилрхязурнийрдцмгглдоээзуюржевшйржеяейицуьлнгюужехлэрээйрдцщзчэшкфх
сзвэвзихелызфлсуяззюзээянюэрцпьчээпжхуэйбжрхолырзэмгтфлзжзвчеюжфбэоаьчжлльдэыю
пздлмуэгцншэеьпщзчфуилцумзрхыглздумзсзжебжээзэдщщюмефуцхбжлзфуубпжээйчаоухрээ
яюлщудочонушяячаонушлжэпжшэщзнунптщеягудхьлвяаэшэыгбрцныврхплжбьгзчгхфэяисзж
ерхыеокзчфхчявчцлфуслюэсобрьесзвяугжздофхеьзшллчяэзьздуькйрылоьйиилуонуэяьлрхгщз
чфуилеьлзюлщудоронуалькйчшэщзугвздхурхэпжнущгьчипячгбяйгбвмшгуглляуюлщудочону
чвфуфхмлябтщээфцглвуфбдцглхкйрзуслсзтэртугллчгашпбуозмвзплихдоикюзфлккнжлнылфу
ьздхикшгпиелчэвоцлэзьзшпьгкгзчаьгхбжаооеячмээлэглонжьрьтэлеьлзокшлйэллнусзрлсзгуцх
юлндпонжвудоеяфлзбйчфбзозчжлхеезфэдвлшаопбнжрхэуилгхидрхвхкхюопжфпчоцхпладзуф
уязхчугшгцпзэзэхзеэйчфекхгхмхурвзшпшгюуфуьзязруячшярхпжцпушнлизязеэзэпжлряхщхб
рьгбрзэтщфпяхпххуфхяупзфлглгбшчцпежвонудщллжбзчмпвмрщйчшууэнюзудоюизбффчяба
шэзудоюигушулуфмыпцкгбккфплззухзжзцрчззулзфуфлщхгхэулуезндгуьабжеэшклуплгхцунх
дсшуыжфпчосзеэьгжзчрдцдвмайчугшгцпьгжбтцшэглйрьтккфхнурусефбккюзфлячгбяйьггбни
рхязурнихунуйрдцмгюзфлглупфмшгюизуеэзэбжрщгхрузлядйяцкцкфхфлокйрзуслябтщшгэгл
льшрщдхеэффзэьчгуадгуюлвескгбэрюоежшуадгумзгхгхежуоылямфпгцоашуфьйидлядбтрузл
ядйяихфлдэюурхшумзлзруьпйчнжлзцхядйяжкфхнуэзчлвхбждвгуюззужбпшщуоэдврузлугеур
хлнэнцпыгхеезэгвзомгхдудусзуэлвчопзшзаэлвлюйчшзпзвэюшффзэщзйкзчжлшцежйиязбфнлп
щпзклргзчамшэзудокфйчнуищпзклоклуплгхцунхаонжмоамеуаклудомпбтцчэтщзялдхымтллг
жзюлчвькышдвдоьлцляайчжлдгхлжэглчвмхихщуидмоамрщшпщцчохзрузлугшчшудувэзшюш
ьдгбузьюзяаолудошгртргькнжээзянптщйрсбеьзгсщбявэвофцячрукбипрхгуфзуедоеявцяирхлзь
зокьакгдонуцхцашуспрэдщюуцшйьщуидмоаоеэшгвзсзсэнжмарголрздунужбзчаоызэзчмжфяж
зудоргжздугзчэрщцкгбьчвхткпздчвхдплоччнзлеюоаодофхиэлвнужбзчихозошозлегушуйьекпз
урккпздчвхдпапйябжкгжзпзиллзцчзшрщтфзэлоэяэзшзсдихфзфлгчфрбялздулзмбвщежнужбзч
нжээсуугуонжрхжбнюфлзгцклулхжбэрдоьгюзфлбжхзшпщццпзлеэячпжзлсзбэташупэйзфхсщ
шгпбвачоцпзлеэмпрежэьгцпжбцкйрщудоыльзлчоьшпшэзудоепюрашяиеэлзлюйчцпйямхыкпз
уршэьчжбфцргцпжзюякфоздуупцкьасойиилгупрьгжзвхбшфхцшлллзкфсздозузуцчфуюлрхюз
мгшулгбрмггушулурувгбрипхзжкзчюзвэывфхмлцчьчнжлзфлнздуячозихзллзфушулемоюурха
осзухгхрхнужбзчгшаопбйзжбэрдоьгбязлидбжцэцкаонжмашужбэрдоьгюзфлсулзекгбшэзчмпв
здугщзусзоэшгмбвщяиэгуофетунпйчядхеезфэдвязлоипхэзчжллшаопбдвлзруьпамзозкфхнуду
мпргээшгворщшгамгхдомшфхвуцьмпфмьлспзшаопбдвдоллщухлядмхмхлмфжгбяудокючочва
шзяфлжбэрдоьгбягхидбжпущщшгпбмпжзьзвеокшчмхооюшдвшуамышфхмщзчьрсбдонущйсб
тхдуэедхфчугллэхсднукрпиэзлефуоздояхеэьгозфхжпзмвегхидчэялжбзчмпшкшлэтвоылапфмй
ихзээушшуфлгупрзэмежэдзпсшудухещхщуактзжгжзвхяюхзкрмпнудньчугаоюшмзчэрщцкмпр
гипуемзжбффвэяизбйчжзрэвеоюкфндфушулемоышлуфзэзщайчшггушуйьсуаклунуилфелудо
шгртрхьуфьщужбшгйрчоылзчвхадзумгпзчяокшлльишглжэюшнждоцхнрипзэеьяллгруашсзлз
жбсуьузлрудппшзлдщышшуиюкффлгушуфхюфлтцхжлгхдщеэшгфушпэрлзмгпзчягупрйчэзво
фхнууэюкшлэуилзлцчумфпхзчмфпхзкбмгщюеььчфеклушрщдхкрпбшгтзрхвхолдоцпцкцкфхд
плоччцлеэшкгбьчвхгхнубмлюдхядфэбжжбнюлзоакгдонуьзпзяпргдвсхщудоглщчвхщушггхяз
цхядцуюзялцуюзшэккеэлозуэрбялздуьзькышдвдонуеэеецчугшгцпмоаоцкфпщюшэщзлшаопб
нжеэрхэуилгчрэбжрщщужбйрфпсхядйяьумщьашурхдоикдзцшвойчкбрылрфпмзрчугяибхцло
жшэчойгсидщщюкфндячлзэздкшэщзруцьашргцпнуччбжжбкфрхрлюодвжбчмзлсханчвйямхвх
долудььдгбсмыпюуцшйьшуйрфлюлбмфхядмгщхвузуцчюзхеанхзльсзязоэвзкфшкышцпокплл
ххузэрхцудушпшгшклулуоздонуаозуплэзадзурхфуюзеэзэшкячьгфуюодвффсеззблчбпжячщуц
хльэуилхашуэеажцсжлщаячипфхфэвоглмоцкфсшулерхфуюзеэьчядшунфсзсдышаопбнжжбэр
ашффзэшгшкышцпокплжзфбнжуорщеэшкячьгфуюодвмзффсеззшпшгвовздозкпзязчшаопблв
фьткфпщюшэщггбещгхдугхжлсззлмхбтжпхэйчяжщхюобтчлжззляуибыюпиелэуыяядфхфэвог
лыадщшгртйрчомоцкпзязфггхдоээшкфпсурхрхдоикмпэждухелшаопбнжчбзэоеичгулеежшзфх
шужеюлвещудудхжбэрашффзэщзюоюуозндфуфхмлщуьдгбнлеэухдотфлрьгцпжзьзнужбзчаон
жмоллфзоэцкфпщючожбэрипдпйчжлщггбловздохэшкфпсурхээауйэшгзэглэзшюяляуибыюшэ

ывшпшгблчбпжгллычлшпшээяюлдосбцпйярхоохуугуорхихфлщхвцывдщшгцклуьктзтэшкячц
пнуугуошэцсшуугцклувурчозымншльзуэеаждйиыжгртйрмптщпбффьуцуадезмпежшэгцуохуи
лшбффихфлщхтчесжлюллычлшпшээяюлеэрхвллхгчнуялчяэеаждйиынощюэрцппшеэмгщцгхе
экффзфлнуюырщфхуллкзчвхьлигфздоцкшлахьлткшлахьлзлцчшэккфпмацпмзгхбжрщпбжфжп
рововорщдхбжикшлчпшгдущуиемовзмззлфьаосзаэнлашнжлвнужбзчкфюшйиухгчдгдщллфзф
лшунуугуошэккпзфзоэамыпвммэффцхрхдщеэдйхурхадзудооуоэшкячцпячьааяблчбюкфпмам
пшуадгуфьщузлиэбттфрхухуоуозчпжвзпшаопбвзфьщуаорлвешужкгбэршпшгнжаорлвепоьазу
вхяюэтаоцллзжбьгмпхэвзьдгбфуфечлзлашнжлваосзкбьгзуухуцшйьжлисшувфнубэшгцпвзду
мхбшюшдвэгюфюифьщурчвзиллзрчэзлгипушежвуфьжлбжгушулуумыпцкпздчмхихзуцхфумх
злючячсуоэжфрхбэюуоэээпжээсоцэмеэечэмпйядсшухчфямлдщфпфмшгмшлудошгдвзэжлобя
чаэфцьчугщзрхфуюзеэюшнжуонлцчисшуэжьчэзьухюзуфьщувурбуоабфффхмлядйяргагьчжлд
щллборщтфюшфпьуцхоэрщеэташупэрщнжзбпжзчгуцчрлхкшлльозюггушуйьэудакгдонуцхгч
умвкюзлзоэфжокшлсздощздуюгипушнжикйрьляергипушнжшчухдоеийхх

**Розшифрований текст (23 варіант):**

владыкогосподиуслышинасмолящихсятебеукреписилоютвоеюблагочестивейшегосамодержа
внейшеговеликогогосударянашегоимператорааалександрапавловичапомяниправдуегоикротос
тьвоздаждьемупоблагостиегоеюжехранитнытвойвозлюбленныйизраильблагословиегосоветы
начинанияиделаутвердивсемогущноютвоеюдесницеюцарствоегоиподаждьемупобедунаврага
якожемоисеюнаамаликагедеонунамадиамаидавидунаголиафасохранивоинствоегоположилук
медянмышцамвоимятвоеополчившихсяипрепояшиихсилоюнабраньприимиоружиеищитивосс
танивпомощьнашудапостыдятсяипосрамятсямыслящийнамзлаядабудутпредлицемверноготив
оинстваякопрахпредлицемветраиангелтвойсильныйдабудетоскорбляяйипогоняяйихдаприиде
тимсетьюженесведаютиихловитваюжесокрышадаобыметихдападутподногамирабовтвоихивп
опраниевоемнашимдабудутгосподинеизнеможетутебеспасативомногихивмалыхтыесибогдан
епревозможетпротивутебечеловекбожеотецнашихпомянищедротытвояимилостияжеотвекасу
тьнеотвержинасотлицатвоегонижевозгнушайсянедостоинствомнашимнопомилуйнасповелиц
еймилоститвоейипомножествущедроттвоихпрезрибеззаконияигрехинашасердцечистосозижд
ивнасидухправобновивоутробенашейвсехнасукрепивероювтяутвердинадеждоюодушевииисти
нноюдругкодругулюбовиювооружиединодушиемнаправедноезащищениеодержанияежедалес
инамиотцемнашимданевознесетсяжезлнечестивыхнажребийосвященныхгосподибоженашвне
гожеверуеминанегожеуповаемнепосраминасотчаяниямилоститвоеяисотворизнамениевоблаго
якодавидятненавидящийнасиправославнуюверунашуипосрамятсяипогибнутидауведятвсестр
аныякоимятебегосподьимылюдиетвоиявинамгосподинынемилостьтвоюиспасениетвоедаждьн
амвозвеселисердцерабовтвоихомилоститвоейпоразиврагинашиисокрушиихподногиверныхтв
оихвскоретыбоесизаступлениепомощьипобедауповающимнатяитебеславувоссылаемотцуисы
нуисвятомудухуинынеиприсноивовекивековаминьвтомсостояниираскрытостидушевнойвкот
оромнаходиласьнаташаэтамолитвасильноподействовалананееонаслушалакаждоесловоопобед
емоисеянаамаликаигедеонанамадиамаидавиданаголиафаиоразорениииерусалиматвоегоипрос
илабогастойнежностьюиразмягченностьюкотороюбылопереполненоеесердценонепонималах
орошенькоочемонапросилабогавэтоймолитвеонавсейдушойучаствовалавпрошенииодухеправ
омобукрепленииисердцавероюнадеждоюиовоодушевлениииихлюбовьюноонанемогламолиться
опопранииподногивраговсвоихкогдаоназанесколькоминутпередэтимтолькожелалаиметьихбо
льшечтобылюбитьихмолитьсязанихноонатоженемогласомневатьсявправотечитаемойколеноп
реклонноймолитвыонаощущалавдушесвоейблагоговейныйитрепетныйужаспереднаказанием
постигшимлюдейзаихгрехиивособенностизасвоигрехиипросилабогаотомчтобыонпростилихв
сехиееидалбыимвсемиейспокойствияисчастиявжизнииейказалосьчтобогслышитеемолитвуст
огоднякакпьеруезжаяотростовыхивспоминаяблагодарныйвзгляднаташисмотрелнакометустоя
вшуюнанебеипочувствовалчтодлянегооткрылосьчтотоновоевечномучившийеговопросотщете
ибезумностивсегоземногопересталпредставлятьсяемуэтотстрашныйвопросзачемкчемукотор

ыйпреждепредставлялсяемувсерединевсякогозанятиятеперьзаменилсядлянегонедругимвопро
соминеответомнапрежнийвопросапредставлениемееслышаллионисамливелничтожныеразгов
орычиталлионилиузнавалпроподлостьибессмысленностьлюдскуюоннеужасалсякакпреждене
спрашивалсебяизчегохлопочутлюдикогдавсетаккраткоинеизвестноновспоминалеевтомвидев
которомонвиделеевпоследнийразивсесомнениягоисчезалинепотомучтоонаотвечаланавопрос
ыкоторыепредставлялисьемунопотомучтопредставлениеонейпереносилоегомгновенновдругу
юсветлуюобластьдушевнойдеятельностивкоторойнемоглобытьправогоиливиноватоговобласт
ькрасотыилюбвидлякоторойстоиложитькакаябымерзостьжитейскаянипредставляласьемуонго
ворилсебенуипускайтакойтообокралгосударствоицаряагосударствоицарьвоздаютемупочести
аонавчераулыбнуласьмнеипросилаприехатьиялюблюееиниктоникоганеузнаетэтогодумалон
пьервсетакжеездилвобществотакжемногопиливелтужепразднуюирассеяннуюжизньпотомучт
окрометехчасовкоторыеонпроводилуростовыхнадобылопроводитьиостальноевремяипривычк
иизнакомствасделанныеимвмосквенепреодолимовлеклиегоктойжизникотораязахватилаегоно
впоследнеевремякогдастеатравойныприходиливсеболееиболеетревожныеслухиикогдаздоров
ьенаташисталопоправлятьсяионаперестalавозбуждатьвнемпрежнеечувствобережливойжалос
тиимсталоовладеватьболееиболеенепонятноедлянегобеспокойствоончувствовалчтотоположе
ниевкоторомоннаходилсянемоглопродолжатьсядолгочтонаступаеткатастрофадолженствующ
аяизменитьвсюегожизньиснетерпениемотыскивалвовсемпризнакиэтойприближающейсяката
строфыпьерубылооткрытооднимизбратьевмасоновследующеевыведенноеизапокалипсисаиоа
ннабогословапророчествоотносительнонаполеонанаписавпоэтойазбукецифрамисловавыходи
тчтосуммаэтихчиселравнатиичтопоэтомунаполеонестьтотзверьокоторомпредсказановапокал
ипсисекрометогонаписавпоэтойжеазбукесловатоестьпределкоторыйбылположензверюглагол
ативеликаихульнасуммаэтихчиселизображающихопятьравнатиизчеговыходитчтопределвласт
инаполеонанаступилвмгодувкоторомфранцузскомуимператоруминулогодапредсказаниеэтоо
ченьпоразилопьераиончастозадавалсебевопросотомчтоименноположитпределвластизверятое
стьнаполеонаинаоснованииитехжеизображенийсловцифрамиивычисленияхмистаралсянайтиотв
етназанимавшийеговопроспьернаписалвответенаэтотвопросонсчелбуквыносуммацифрвыход
илагораздобольшеилименьшетиодинраззанимаясьэтимивычисленияхмионнаписалсвоеимясум
мацифртожедалеконевышлаонизмениворфографиюпоставиввместоприбавилприбавиливсене
получалжелаемогорезультататогдаемупришловголовучтоежелибыответнаискомыйвопросиза
ключалсявегоименитовответенепременнобылабыназванаегонациональностьоннаписалисочтя
цифрыполучилтолькобылолишнихозначаететосамоеекотороебылооткинутовпередсловомотк
инувточнотакжехотяинеправильноепьерполучилискомыйответравноетиоткрытиеэтовзволнов
алоегокаккакойсвязьюбылонсоединенстемвеликимсобытиемкотороебылопредсказановапока
липсисеоннезналноонниначинутунеусумнилсявэтойсвязиеголюбовькростовойантихристнаш
ествиенаполеонакометаивсеэтовместедолжнобылосозретьразразитьсяивывестиегоизтогозако
лдованногоничтожногомирамосковскихпривычеквкоторыхончувствовалсебяплененнымипри
вестиегоквеликомуподвигуивеликомусчастиюаатч

**Ключ: (735,300).**

**Висновки:** В ході виконання даної лабораторної роботи я навчився проводити атаку на шифр афінної підстановки на біграмах, вдосконалив свої навички у частотному аналізі та вдосконалив свої вміння в модульній арифметиці.