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	0
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	0.000689655	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	0.000689655	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	0.000344828
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	0	0	0.00896552	0	0.00344828	0.00103448	0.000344828	0	0.000689655	0	0	0.000689655	0.00344828	0
щ	0.000689655	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	0.000689655	0.000344828
ю	0	0	0	0.00137931	0	0.00206897	0	0.00655172	0	0	0	0	0	0.000689655	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), (580,207), (959,267), (402,156), (753,384), (117,360), (956,301), (381,353), (675,360), (770,797), (2,293), (844,200), (286,200), (649,944), (559,404), (5,259), (191,724), (312,577), (440,588), (192,247), (735,300), (259,250), (521,67), (728,238), (396,298), (769,408), (356,238), (520,608), (226,355), (233,417), (605,417), (301,882), (702,405), (565,357), (441,47), (660,734), (363,269), (735,300), (246,608), (526,807), (598,632), (24,701), (615,270), (226,601), (582,701), (429,766), (715,293), (937,200), (379,200), (897,944), (435,94), (346,631), (532,135), (64,918), (243,321), (770,445), (395,127), (368,427), (718,564), (437,499), (507,139), (191,440), (747,499), (724,201), (566,758), (524,386), (214,386), (116,479), (593,458), (454,746), (237,684), (845,406), (753,384), (381,353), (2,293), (559,404), (208,176), (844,200), (5,259), (580,207), (286,200), (191,724), (959,267), (117,360), (675,360), (312,577), (402,156), (956,301), (770,797), (649,944), (232,834), (573,462), (737,455), (818,516), (729,105), (611,300), (401,419), (388,477), (642,300), (711,233), (224,484), (350,639), (319,639), (613,360), (143,423), (560,520), (250,706), (348,579), (35,567), (190,660), (397,282), (927,693), (926,602), (320,561), (512,260), (771,509), (72,561), (915,787), (564,887), (641,608), (889,608), (428,918), (34,476), (449,909), (46,382), (533,251), (521,67), (769,408), (226,355), (702,405), (440,588), (233,417), (565,357), (192,247), (605,417), (441,47), (735,300), (728,238), (356,238), (660,734), (259,250), (396,298), (520,608), (301,882), (729,105), (388,477), (224,484), (143,423), (232,834), (350,639), (560,520), (573,462), (319,639), (250,706), (737,455), (611,300), (642,300), (348,579), (818,516), (401,419), (711,233), (613,360), (884,198), (543,570), (472,825), (267,113), (77,121), (257,19), (219,489), (418,710), (226,19), (870,675), (489,455), (704,300), (735,300), (596,579), (694,206), (742,791), (91,605), (365,701), (764,250), (578,715), (621,344), (109,694), (197,53), (670,778), (111,358), (383,549), (391,778), (204,110), (340,920), (291,486), (570,486), (776,114), (852,570), (850,906), (757,193), (185,189), (598,632), (226,601), (715,293), (435,94), (363,269), (937,200), (346,631), (735,300), (379,200), (532,135), (246,608), (24,701), (582,701), (64,918), (526,807), (615,270), (429,766), (897,944), (77,121), (418,710), (489,455), (694,206), (884,198), (704,300), (742,791), (543,570), (735,300), (91,605), (472,825), (257,19), (226,19), (365,701), (267,113), (219,489), (870,675), (596,579), (841,815), (35,908), (149,282), (803,383), (120,695), (413,561), (853,632), (926,602), (165,561), (295,198), (812,267), (548,949), (796,949), (180,298), (158,166), (108,878), (666,351), (781,251), (718,564), (191,440), (566,758), (593,458), (243,321), (524,386), (454,746), (770,445), (214,386), (237,684), (395,127), (437,499), (747,499), (845,406), (368,427), (507,139), (724,201), (116,479), (926,602), (771,509), (564,887), (34,476), (35,567), (641,608), (449,909), (190,660), (889,608), (46,382), (397,282), (320,561), (72,561), (533,251), (927,693), (512,260), (915,787), (428,918), (197,53), (383,549), (340,920), (852,570), (764,250), (291,486), (850,906), (578,715), (570,486), (757,193), (621,344), (670,778), (391,778), (185,189),

(109,694), (111,358), (204,110), (776,114), (120,695), (926,602), (812,267), (158,166), (841,815), (548,949), (108,878), (35,908), (796,949), (666,351), (149,282), (413,561), (165,561), (781,251), (803,383), (853,632), (295,198), (180,298)
При чому, деякі ключі я отримував по декілька разів з різних лінійних порівнянь.

- 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), (580,207), (363,269) 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
йрзунхюлфхцупонубтргфужбзэщзнубжрхолырвмьрсодуькйрээялжэбжщюуосоумьчюхлхжлн
учэрщбтргщхчьяойзплцупрзэккпзнуожщюуожбаоргсоумоаипшгпшщумзаохйрхолхкнжрэгнэр
луцьугеяежмпзчжлеюсуугпшйчсохэсууггбхлрхвуппщйвонудщеэсюмгтфлэдцжвйялзьудоллрч
угнжрхолчэцкнжмпхврхькшгипщйчвюлщудочонучвокнжзумздоиеызмбаоугллхкпзрбчмжфих
гуфлцлхбэтээфцйчгбяйоаячшувумлурггрхплхехкфхнуюэшгргшекбамшэфцчвцчэтрхэефбккрг
гбниподеуггбилрхязурнийрдцмгглдоээзуюржевшйржеяейицуьлнгюужехлэрээйрдцщзчэшкфх
сзвэвзихелызфлсуяззюзээянюэрцпьчээпжхуэйбжрхолырзэмгтфлзжзвчеюжфбэоаьчжлльдэыю
пздлмуэгцншэеьпщзчфуилцумзрхыглздумзсзжебжээзэдщщюмефуцхбжлзфуубпжээйчаоухрээ
яюлщудочонушяячаонушлжэпжшэщзнунптщеягудхьлвяаэшэьгбрцныврхплжбьгзчгхфэяисзж
ерхыеокзчфхчявчцлфуслюэсобрьесзвяугжздофхеьзшллчяэзьздуькйрылоьйиилуонуэяьлрхгщз
чфуилеьлзюлщудоронуалькйчшэщзугвздхурхэпжнущгьчипячгбяйгбвмшгуглляуюлщудочону
чвфуфхмлябтщээфцглвуфбдцглхкйрзуслсзтэртугллчгашпбуозмвзплихдоикюзфлккнжлнылфу
ьздхикшгпиелчэвоцлэзьзшпьгкгзчаьгхбжаооеячмээлэглонжьрьтэлеьлзокшлйэллнусзрлсзгуцх
юлндпонжвудоеяфлзбйчфбзозчжлхеезфэдвлшаопбнжрхэуилгхидрхвххкюопжфпчоцхпладзуф
уязхчугшгцпзэзэхзеэйчфекхгхмхурвзшпшгюуфуьзязруячшярхпжцпушнлизязеэзэпжлряхщхб
рьгбрзэтщфпяхпххуфхяупзфлглгбшчцпежвонудщллжбзчмпвмрщйчшууэнюзудоюизбффчяба
шэзудоюигушулуфмыпцкгбккфплззухзжзцрчззулзфуфлщхгхэулуезндгуьабжеэшклуплгхцунх
дсшуыжфпчосзеэьгжзчрдцдвмайчугшгцпьгжбтцшэглйрьтккфхнурусефбккюзфлячгбяйьггбни
рхязурнихунуйрдцмгюзфлглупфмшгюизуеэзэбжрщгхрузлядйяцкцкфхфлокйрзуслябтщшгэгл
льшрщдхеэффзэьчгуадгуюлвескгбэрюоежшуадгумзгхгхежуоылямфпгцоашуфьйидлядбтрузл
ядйяихфлдэюурхшумзлзруьпйчнжлзцхядйяжкфхнуэзчлвхбждвгуюззужбпшщуоэдврузлугеур
хлнэнцпьгхеезэгвзомгхдудусзуэлвчопзшзаэлвлюйчшзпзвэюшффзэщзйкзчжлшцежйиязбфнлп
щпзклргзчамшэзудокфйчнуищпзклоклуплгхцунхаонжмоамеуаклудомпбтцчэтщзялдхымтллг
жзюлчвькышдвдоьлцляайчжлдгхлжэглчвмхихщуидмоамрщшпщцчохзрузлугшчшудувэзшюш
ьдгбузьюзяаолудошгртргькнжээзянптщйрсбеьзгсщбявэвофцячрукбипрхгуфзуедоеявцяирхлзь

зокьакгдонуцхцашуспрэдщюуцшйьщуидмоаоеэшгвзсзсэнжмарголрздунужбзчаоыззэчмжфяж
зудоргжздугзчэрщцкгбьчвхткпздчвхдплоччнзлеюоаодофхиэлвнужбзчихозошозлегушуйьекпз
урккпздчвхдпапйябжкгжзпзиллзцчзшрщтфзэлоэяэзшзсдихфзфлгчфрбялздулзмбвщежнужбзч
нжээсуугуонжрхжбнюфлзгцклулхжбэрдоьгюзфлбжхзшпщццпзлеэячпжзлсзбэташупэйзфхсщ
шгпбвачоцпзлеэмпрежэьгцпжбцкйрщудоыльзлчоьшпшэзудоепюрашяиеэлзлюйчцпйямхыкпз
уршэьчжбфцргцпжзюякфоздуупцкьасойиилгупрьгжзвхбшфхцшлллзкфсздозузуцчфуюлрхюз
мгшулгбрмггушулурувгбрипхзжкзчюзвэывфхмлцчьчнжлзфлнздуячозихзллзфушулемоюурха
осзухгхрхнужбзчгшаопбйзжбэрдоьгбязлидбжцэцкаонжмашужбэрдоьгюзфлсулзекгбшэзчмпв
здугщзусзоэшгмбвщяиэгуофетунпйчядхеезфэдвязлоипхэзчжллшаопбдвлзруьпамзозкфхнуду
мпргээшгворщшгамгхдомшфхвуцьмпфмьлспзшаопбдвдоллщухлядмхмхлмфжгбяудокючочва
шзяфлжбэрдоьгбягхидбжпущщшгпбмпжзьзвеокшчмхооюшдвшуамышфхмщзчьрсбдонущйсб
тхдуэедхфчугллэхсднукрпиэзлефуоздояхеэьгозфхжпзмвегхидчэялжбзчмпшкшлэтвоылапфмй
ихзээушшуфлгупрзэмежэдзпсшудухещхщуактзжгжзвхяюхзкрмпнудньчугаоюшмзчэрщцкмпр
гипуемзжбффвэяизбйчжзрэвеоюкфндфушулемоышлуфзэзщайчшггушуйьсуаклунуилфелудо
шгртрхьуфьщужбшгйрчоылзчвхадзумгпзчяокшлльишглжэюшнждоцхнрипзэеьяллгруашсзлз
жбсуьузлрудппшзлдщышшуиюкффлгушуфхюфлтцхжлгхдщеэшгфушпэрлзмгпзчягупрйчэзво
фхнууэюкшлэуилзлцчумфпхзчмфпхзкбмгщюеььчфеклушрщдхкрпбшгтзрхвхолдоцпцкцкфхд
плоччцлеэшкгбьчвхгхнубмлюдхядфэбжжбнюлзоакгдонуьзпзяпргдвсхщудоглщчвхщушггхяз
цхядцуюзялцуюзшэккеэлозуэрбялздуьзькышдвдонуеэеецчугшгцпмоаоцкфпщюшэщзлшаопб
нжеэрхэуилгчрэбжрщщужбйрфпсхядйяьумщьашурхдоикдзцшвойчкбрылрфпмзрчугяибхцло
жшэчойгсидщщюкфндячлзэздкшэщзруцьашргцпнуцчбжжбкфрхрлюодвжбчмзлсханчвйямхвх
долудььдгбсмыпюуцшйьшуйрфлюлбмфхядмгщхвузуцчюзхеанхзльсзязоэвзкфшкышцпокпллл
ххузэрхцудушпшгшклулуоздонуаозуплэзадзурхфуюзеэзэшкячьгфуюодвффсеззблчбпжячщуц
хльэуилхашуэеажцсжлщаячипфхфэвоглмоцкфсшулерхфуюзеэьчядшунфсзсдышаопбнжжбэр
ашффзэшгшкышцпокплжзфбнжуорщеэшкячьгфуюодвмзффсеззшпшгвовздозкпзязчшаопблв
фьткфпщюшэщггбещгхдугхжлсззлмхбтжпхэйчяжщхюобтчлжззляуибыюпиелэуыяядфхфэвог
лыадщшгртйрчомоцкпзязфггхдоээшкфпсурхрхдоикмпэждухелшаопбнжчбзэоеичгулеежшзфх
шужеюлвещудудхжбэрашффзэщзюоюуозндфуфхмлщуьдгбнлеэухдотфлрьгцпжзьзнужбзчаон
жмоллфзоэцкфпщючожбэрипдпйчжлщггбловздохэшкфпсурхээауйэшгзэглээшюяляуибыюшэ
ывшпшгблчбпжглльчлшпшээяюлдосбцпйярхоохуугуорхихфлщхвцывдщшгцклуьктзтэшкячц
пнуугуошэцсшуугцклувурчозымншльзуэеаждйиыжгртйрмптщпбффьуцуадезмпежшэгцуохуи
лшбффихфлщхтчесжлюлльчлшпшээяюлеэрхвллхгчнуялчяэеаждйиынощюэрцппшеэмгщцгхе
экффзфлнуюырщфхуллкзчвхьлигфздоцкшлахьлткшлахьлзлцчшэккфпмацпмзгхбжрщпбжфжп
роворщдхбжикшлчпшгдущуиемовзмззлфьаосзаэнлашнжлвнужбзчкфюшйиухгчдгдщллфзф
лшунуугуошэккпзфзоэамыпвммэффцхрхдщеэдйхурхадзудооуоэшкячцпячьааяблчбюкфпмам
пшуадгуфьщузлиэбттфрхухуоуозчпжвзпшаопбвзфьщуаорлвешужкгбэршпшгнжаорлвепоьазу
вхяюэтаоцллзжбьгмпхэвзьдгбфуфечлзлашнжлваосзкбьгзуухуцшйьжлисшувфнубэшгцпвзду
мхбшюшдвэгюфюифьщурчвзиллзрчэзлгипушежвуфьжлбжгушулуумыпцкпздчмхихзуцхфумх
злючячсуоэжфрхбэюуоэээпжээсоцэмеэечэмпйядсшухчфямлдщфпфмшгмшлудошгдвзэжлобя
чаэфцьчугщзрхфуюзеэюшнжуонлцчисшуэжьчэзьухюзуфьщувурбуоабфффхмлядйяргагьчжлд
щллборщтфюшфпьуцхоэрщеэташупэрщнжзбпжзчгуцчрлхкшлльозюггушуйьэудакгдонуцхгч
умвкюзлзоэфжокшлсздощздуюгипушнжикйрьляергипушнжшчухдоеийхх

Розшифрований текст (23 варіант):

владыкогосподиуслышимсмолящихсятебеукреписилоютвоеюблагочестивейшегосамодеревне
йшеговеликогогосугрямшегоимпептопалекрндповловичапомяниппвдуегоикротостьвозгждье
мупоблагостиегоеюжехпнитнытвойвозлюбленныйизраильблагословиегосоветыначинанияид
елаутвердивсемогущноютвоеюдесницеюхрствоегоиподаждьемупобедунавпвякожемоисеюня
ллийгедеонунамадзлидавидунаголзусохранивоинствоегоположилукмедянмышцамвоимятвое
ополчившихсяипрепояшиихсилоюнабпньприимиоружиеищитивосстанивпомощьмшугпосты

дятсяипоспмятсямыслящийнамзлаягбудутпредлицемверноготивоинстваякопрахпредлицемве
тпзнгелтвойсильныйдабудетоскорбляяйипогоняяйихдаприидетимсетьюженесвегютиихловит
бюжесокрычгобыметихгодутподновмипбовтвоихивпопраниевоеммшимдабудутгосподинеизн
еможетутебесортивомногихивллыхтыесибогданепревозможетпротивутебечеловекбожеотецм
шихпомянищедротытвояимилостияжеотвекасутьнеотвержимсотлицатвоегонижевозгнушайся
недостоинствоммшимнопомилуймсповелицеймилоститвоейипомножествущедроттвоихпрезр
ибезжкониягрехинашасердцечистосозиждивмсидухппвобновивоутробенашейвсехмсукрепи
вероювтяутвердимдеждоюодушевиистинноюдругкодругулюбовиювооружиединодушиемнап
пведноежщищениеодержанияежедалесинамиотцеммшимданевознесетсяжезлнечестивыхнаж
ребийосвященныхгосподибожемшвнегожеверуеминанегожеупобемнепосраминасотцяниямил
оститвоеяисотворизнамениевоблагоякогвидятненавидящиймсиправосквнуюверумшуипоспм
ятсяипогибнутидауведятвсестпныякоимятебегосподьимылюдиетвоиявиммгосподинынемило
стьтвоюиспасениетвоегждьнамвозвеселисердцерабовтвоихомилоститвоейпопзиврагинашиис
окрушиихподногиверныхтвоихвскоретыбоесижступлениепомощьипобегуповающимнатяитеб
еславувоссыкемотцуисынуисвятомудухуинынеиприсноивовекивекобминьвтомсостоянииирас
крытостидушевнойвкотороммходиксьмсчэтамолитбсильноподействовалананееонаслучкйждо
есловоопобедемоисеямамаликаигедеонанамадзлидавиданаголзуиопзорениииерусалиматвоег
оипросилабогастойнежностьюиразмягченностьюкотороюбылопереполненоеесердценонепон
илкхорошенькоочемонапросикбоввэтоймолитвеонавсейдушойучаствовалавпрошенииодухеп
пвомобукрепленииисердцавероюмдеждоюиовоодушевлениииихлюбовьюноонанемогкмолиться
опоппнииподногивраговсвоихкоггоназанесколькоминутпередэтимтолькожеккиметьихбольш
ечтобылюбитьихмолитьсяжнихноомтоженемогласомнебтьсявппвотечисемойколенопреклонн
оймолитвыомощущалавдушесвоейбкгоговейныйитрепетныйужасперед наказаниемпостигши
млюдейзаихгрехиивособенностизасвоигрехиипросикбовотомчтобыонпростилихвсехиееиглб
ыимвсемиейспокойствияисчастиявжизнииеййжлосьчтобогслышитеемолитвустогоднякакпьер
уезжаяотростовыхивспоминаяблагодарныйвзгляднаташисмотрелмкометустоявшуюмнебеипо
чувствоблчтодлянегооткрылосьчтотоновоевечномучившийеговопросотщетеибезумностивсег
оземногопересслпредссвлятьсяемуэтотстпшныйвопросжчемкчемукоторыйпрежде предссвлял
сяемувсерединевсякогозанятиятеперьжменилсядлянегонедругимвопросоминеответоммпреж
нийвопрорпредставлениемееслышаллионисамливелничтожныепзговорычиталлионилиузнава
лпроподлостьибессмысленностьлюдскуюоннеужасалсяйкпрежденеспрашивалсебяизчегохло
почутлюдикогдавсесскпткоинеизвестноновспомимлеевтомвидевкоторомонвиделеевпоследн
ийпзивсесомнениягоисчежлинепотомучтоомотвецкмвопросыкоторыепредставлялисьемуноп
отомучтопредставлениеонейпереносилоегомгновенновдругуюсветлуюобластьдушевнойдеяте
льностивкоторойнемоглобытьппвогоиливиноватоговобкстькпсотыилюбвидлякоторойстоило
житьййбымерзостьжитейскаянипредставляксьемуонговорилсебенуипусййтакойтообокплгос
ударствоицарюгосугрствоихрьвоздаютемупочестзонавчепулыбнуксьмнеипросилаприехатьия
люблюееиниктоникогданеузнаетэтогодуллонпьервсескжеездилвобществотакжемногопиливе
лтужепраздную юирассеяннуюжизньпотомучтокрометехчасовкоторыеонпроводилуростовыхмд
обылопроводитьиоссльноевремяипривычкиизнакомстбсделанныеимвмосквенепреодолимовл
еклиегоктойжизникотопязахбтикегоновпоследнеевремякогдастеатпвойныприходиливсеболее
иболеетревожныеслухиикоггздоровьемсшисталопоппвлятьсяионаперессквозбужгтьвнемпре
жнеечувствобережливойелостиимсслоовкдебтьболееиболеенепонятноедлянегобеспокойство
ончувствовалчтотоположениевкоторомонмходилсянемоглопродолетьсядолгочтомступаеткат
астрофадолженствуюшяизменитьвсюегожизньиснетерпениемотыскивалвовсемпризмкиэтойп
риблиеющейсяйсстрофыпьерубылооткрытооднимизбптьевлсоновследующеевыведенноеизап
окалипсириоанмбогословапророчествоотносительномполеонанаписавпоэтойазбукецифрамис
лобвыходитчтосуммаэтихчиселпвнатиичтопоэтомумполеонестьтотзверьокоторомпредсказан
овапокалипсисекрометогонаписавпоэтойжеазбукесловатоестьпределкоторыйбылположензве
рюгкгоктивелийихульнасумлэтихчиселизображающихопятьпвнатиизчеговыходитчтопределв

кстинаполеоммступилвмгодувкоторомфранцузскомуимпепторуминулогогпредсказаниеэтооч
еньпопзилопьераионцстозадавалсебевопросотомчтоименноположитпределвластизверятоесть
наполеоминаоснованиитехжеизображенийсловцифрамиивычисленияместаралсямйтиответм
жнилвшийеговопроспьернаписалвответенаэтотвопросонсчелбуквыносуммацифрвыходилаго
раздобольшеилименьшетиодинразжнилясьэтимивычисленияционмпирлсвоеимясуммацифрт
ожедалеконевышконизмениворфогпфиюпоссвиввместоприавилприавиливсенеполучалжекем
огорезультататоггемупришловголовучтоежелибыответнаискомыйвопросизаключлсявегоиме
нитовответенепременнобылабыназбмегонациомльностьоннаписалисочтяцифрыполучилтоль
кобылолишнихозмцететосамоеекотороебылооткинутовпередсловомоткинувточноскжехотяи
неправильноепьерполучилискомыйответравноетиоткрытиеэтовзволновалоегойккакойсвязью
былонсоединенстемвеликимсобытиемкотороебылопредсйжнобпойлипсисеоннезмлнооннина
минутунеусумнилсявэтойсвязиеголюбовькростовойантихристнашествиемполеонакометаивсе
этовместедолжнобылосозретьразпзитьсяивывестиегоизтогозаколдобнногоничтожногомирам
осковскихпривычеквкоторыхончувствоблсебяпленеппымипривестиегоквеликомуподвигуиве
ликомусцстиюятч

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.