**Лабораторна работа №4**

**Тема:** Використання теорії множин до аналізу текстів та підбору здвигу в шифрі Цезарі (одноалфавітної заміни).

**Цель:** опрацювати методи аналізу множин на прикладі статистичного аналізу текстів при одноалфавітній заміні.

**Теоретические сведения**

У теорії множин є два основних первісних не означуваних понять: Множина і елемент, а основні не означувані відношення між ними описуються словами: належить, відповідає, передує, отже, поняття множина приймаємо без означення, тому пояснимо його прикладами.

Можна говорити про множину букв в алфавіті, про множину розв’язків, множину студентів І курсу і т.д. У повсякденному житті замість терміну множина вживають сукупність, череда, табун, зграя, екіпаж, колекція, клас, трупа і т.д.

У математиці під множиною розуміють сукупність, зібрання деяких предметів, об’єктів, які об’єднуються між собою характеристичною ознакою.

Математичний зміст терміну „множина” відрізняють від повсякденного, де його зв’язують з великою кількістю об’єктів. В математиці розглядаються множини, які складаються з декількох елементів або їх не має.

Об’єкти будь-якої природи (літери, числа, книги), з яких складається множина називається елементами.

**Завдання.** Які літери використовуються в записі слова „м а т е м а т и к а”? Яка їх потужність(кількість елементів)?

М={ *м, а, т, е, и, к*}

Зауваження:

1. в множині кожен елемент зустрічається лише один раз.
2. порядок запису елементів множин не має значення.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| літери | м | а | т | е | и | к |
| потужн | 2 | 3 | 2 | 1 | 1 | 1 |

Такий спосіб можна використовувати для аналізу шифрів. Наприклад.

Шифри одноалфавітної заміни є найпростішими серед інших шифрів заміни. Принцип їхньої дії побудований на тому, що кожній букві відкритого тексту ставиться у відповідність інша, але детермінована (незмінна) буква деякого алфавіту (алфавіту заміни). Через те, що кожній букві відкритого тексту відповідає єдина буква алфавіту заміни, всьому відкритому алфавіту відповідає єдиний незмінний алфавіт заміни, тому шифри цього класу називають шифрами одноалфавітної заміни.

Розглянемо шифр одноалфавітної заміни на прикладі так званого шифру Цезаря. Щоб розібрати і прочитати його тексти, потрібно всякий раз читати четверту букву замість першої відповідно до алфавіту, наприклад Д замість А, при цьому алфавіт представлявся як кільце – наступним за символом Я вважався символ А. Ми розглянемо узагальнений шифр Цезаря, в якому будемо зсовувати символи початкового алфавіту на довільну кількість позицій. Знак пробілу між словами не враховується.

**Алфавіт для шифрування:** АБВГДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Алф | А | Б | В | Г | Д | Е | Є | Ж | З | И |
| Зам | Е | Є | Ж | З | И | І | Ї | Й | К | Л |
|  |  |  |  |  |  |  |  |  |  |  |
| І | Ї | Й | К | Л | М | Н | О | П | Р | С |
| М | Н | О | П | Р | С | Т | У | Ф | Х | Ц |
|  |  |  |  |  |  |  |  |  |  |  |
| Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |
| Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Д |

Зашифруємо текст шифром Цезаря при ключі К=5:

Відкритий текст:

МНОЖИНА — ОДНЕ З ОСНОВНИХ ПОНЯТЬ СУЧАСНОЇ МАТЕМАТИКИ. СТРОГО ВОНО НЕ ВИЗНАЧАЄТЬСЯ, АЛЕ МОЖЕ БУТИ ДАНО ІНТУЇТИВНЕ ВИЗНАЧЕННЯ МНОЖИНИ ЯК СУКУПНОСТІ ПЕВНИХ І РІЗНИХ ОБ'ЄКТІВ ДОВІЛЬНОЇ ПРИРОДИ, ЯКА РОЗГЛЯДАЄТЬСЯ ЯК ОДНЕ ЦІЛЕ. ОБ'ЄКТИ, ЯКІ СКЛАДАЮТЬ МНОЖИНУ, НАЗИВАЮТЬСЯ ЇЇ ЕЛЕМЕНТАМИ. НАПРИКЛАД, МОЖНА ГОВОРИТИ ПРО МНОЖИНУ УСІХ КНИГ В ПЕВНІЙ БІБЛІОТЕЦІ, МНОЖИНУ ЛІТЕР УКРАЇНСЬКОГО АЛФАВІТУ АБО ПРО МНОЖИНУ ВСІХ КОРЕНІВ ПЕВНОГО РІВНЯННЯ.

Всього літер у тексті – 360.

Шифртекст:

СТУЙЛТЕУИТІКУЦТУЖТЛЬФУТДЧВЦШЯЕЦТУНСЕЧІСЕЧЛПЛЦЧХУЗУЖУТУТІЖЛКТЕЯЕЇЧВЦДЕРІСУЙІЄШЧЛИЕТУМТЧШНЧЛЖТІЖЛКТЕЯІТТДСТУЙЛТЛДПЦШПШФТУЦЧМФІЖТЛЬМХМКТЛЬУЄЇПЧМЖИУЖМРВТУНФХЛХУИЛДПЕХУКЗРДИЕЇЧВЦДДПУИТІЮМРІУЄЇПЧЛДПМЦПРЕИЕГЧВСТУЙЛТШТЕКЛЖЕГЧВЦДННІРІСІТЧЕСЛТЕФХЛПРЕИСУЙТЕЗУЖУХЛЧЛФХУСТУЙЛТШШЦМЬПТЛЗЖФІЖТМОЄМЄРМУЧІЮМСТУЙЛТШРМЧІХШПХЕНТЦВПУЗУЕРЩЕЖМЧШЕЄУФХУСТУЙЛТШЖЦМЬПУХІТМЖФІЖТУЗУХМЖТДТТД

Побудуємо діаграму розподілу частот символів відкритого і шифртексту:

Відкритий текст:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М |
| 23 | 6 | 17 | 6 | 8 | 18 | 4 | 8 | 6 | 25 | 18 | 6 | 1 | 14 | 10 | 12 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |
| 43 | 37 | 9 | 13 | 13 | 19 | 12 | 1 | 5 | 2 | 3 | 0 | 0 | 7 | 2 | 12 |

Шифртекст:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М |
| 0 | 0 | 7 | 2 | 12 | 23 | 6 | 17 | 6 | 8 | 18 | 4 | 8 | 6 | 25 | 18 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |
| 6 | 1 | 14 | 10 | 12 | 43 | 37 | 9 | 13 | 13 | 19 | 12 | 1 | 5 | 2 | 3 |

З двох приведених діаграм розподілу частот, ми бачимо, що рядок чисел для відкритого тексту складається з чисел:

23, 6, 17, 6, 8, 18, 4, 8, 6, 25, 18, 6, 1, 14, 10, 12 , 43, 37, 9, 13, 13, 19, 12, 1, 5, 2, 3, 0, 0, 7, 2, 12

а рядок чисел для шифртексту складається з чисел:

0, 0, 7, 2, 12, 23, 6, 17, 6, 8, 18, 4, 8, 6, 25, 18, 6, 1, 14, 10, 12 , 43, 37, 9, 13, 13, 19, 12, 1, 5, 2, 3

Іншими словами, починаючи з шостого символу, числовий рядок для шифртексту ідентичний початку рядка для відкритого тексту, перші п’ять членів рядка повторюють останні п’ять членів рядка. Побудувавши діаграму, побачимо це в більш наглядній формі:

|  |
| --- |
| *Рис. 1. Діаграма розподілу частот відкритого і шифрованого текстів. де – відкритий текст; – шифртекст.* |

Причому порівнювати можна як окремі елементи (О – У (37)), так і групи символів (И, І – Л, М).

Перейдемо до аналізу шифру Цезаря тільки на основі шифртексту. Для цього ми повинні:

* побудувати діаграми розподілу частот для відкритого і шифрованого текстів у процентному відношенні, оскільки довжина відкритого і шифрованого текстів може відрізнятися;
* розташувати частоти у порядку зростання;
* знайти можливі значення ключа як різницю між відповідними значеннями частот.

Приведемо приклад:

*Таблиця 3 – Ранжовані частоти використання букв української мови*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| О | 0,0942 | р | 0,0448 | я | 0,0248 | ж | 0,0093 |
| А | 0,0807 | с | 0,0424 | з | 0,0232 | ю | 0,0093 |
| Н | 0,0681 | л | 0,0369 | б | 0,0177 | ц | 0,0083 |
| И | 0,0626 | к | 0,0354 | ь | 0,0177 | ш | 0,0076 |
| І | 0,0575 | д | 0,0338 | г | 0,0155 | ї | 0,0065 |
| В | 0,0535 | у | 0,0336 | ч | 0,0141 | є | 0,0061 |
| Т | 0,0535 | м | 0,0303 | й | 0,0138 | щ | 0,0056 |
| Е | 0,0495 | п | 0,0290 | х | 0,0119 | ф | 0,0028 |



*Рисунок 2. Гістограма частот використання букв алфавіту української мови*

Завдання лабораторної роботи.

1. Проаналізувати текст згідно варіанту за наступним алгоритмом.

Шифртекст:

СТУЙЛТЕУИТІКУЦТУЖТЛЬФУТДЧВЦШЯЕЦТУНСЕЧІСЕЧЛПЛЦЧХУЗУЖУТУТІЖЛКТЕЯЕЇЧВЦДЕРІСУЙІЄШЧЛИЕТУМТЧШНЧЛЖТІЖЛКТЕЯІТТДСТУЙЛТЛДПЦШПШФТУЦЧМФІЖТЛЬМХМКТЛЬУЄЇПЧМЖИУЖМРВТУНФХЛХУИЛДПЕХУКЗРДИЕЇЧВЦДДПУИТІЮМРІУЄЇПЧЛДПМЦПРЕИЕГЧВСТУЙЛТШТЕКЛЖЕГЧВЦДННІРІСІТЧЕСЛТЕФХЛПРЕИСУЙТЕЗУЖУХЛЧЛФХУСТУЙЛТШШЦМЬПТЛЗЖФІЖТМОЄМЄРМУЧІЮМСТУЙЛТШРМЧІХШПХЕНТЦВПУЗУЕРЩЕЖМЧШЕЄУФХУСТУЙЛТШЖЦМЬПУХІТМЖФІЖТУЗУХМЖТДТТД

Визначаємо потужність множин:

Шифртекст:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Є | Ж | З | И | І |
| 0 | 0 | 7 | 2 | 12 | 23 | 6 | 17 | 6 | 8 | 18 |
|  |  |  |  |  |  |  |  |  |  |  |
| Ї | Й | К | Л | М | Н | О | П | Р | С | Т |
| 4 | 8 | 6 | 25 | 18 | 6 | 1 | 14 | 10 | 1 | 43 |
|  |  |  |  |  |  |  |  |  |  |  |
| У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | Разом |
| 37 | 9 | 13 | 13 | 19 | 12 | 1 | 5 | 2 | 3 | 360 |

1. Сортуємо за потужністю входження літер в шифротекст, будуємо діаграму (необов’язково, але наглядно).

|  |
| --- |
| Рис. 3. Діаграма розподілу літер шифротексту. |

Визначаємо ключ (дана діаграма для всіх варіантів!!!):

Рис. 4. Діаграма розподілу літер тексту лабораторної роботи 1.

1. Повинна існувати взаємно однозначна відповідність між літерами із найчастішим входженням. Для цього потрібно врахувати номер відповідної літери в алфавіті.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

Між елементами діаграм немає постійної різниці. Це відбувається через те, що шифртекст має досить малу довжину (360 символів) і обчислення потужності входження символів було не таким точним. Тому вибираємо п’ять перших елементів і розраховуємо їх різницю у будь-яких сполученнях:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| текст | Н | О | А | И | Т | або-> | А | И |  |
| № | 17 | 18 | 1 | 10 | 22 |  | 1 | 10 |  |
| шифр | т | у | л | е | ч |  | е | л |  |
| № | 22 | 23 | 15 | 6 | 27 |  | 6 | 15 |  |
| різниця | 5 | 5 | 10 | 4 | 5 |  | 5 | 5 |  |

Враховуючи невелику кількість літер в тексті можливі різні комбінації.

1. Найчастіше значення, як ми бачимо, дорівнює 5, тому можна з досить великою імовірністю казати, що ключ дорівнює 5. До того ж різниця між найчастішими символами дорівнює також 5 але це може бути 32-5=27.
2. Порядок виконання лабораторної роботи
   1. Вивчити відомості з криптоаналізу.
   2. Усі тексти зашифровані шифром Цезаря ключем, не перевищуючим 32. Алфавіт для шифрування:
   3. АБВГДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ
   4. Номер завдання добирається відповідно номеру студента у журналі.
   5. Дешифрувати поданий текст (додаток 1), вказати відповідний йому відкритий текст, знайдений ключ. Студент повинен навести таблицю потужності входження літер відкритого і шифрованого текстів.
   6. Скласти звіт, у якому вказати всі результати виконання лабораторної роботи і відповідний дешифрований текст.
3. Приклад виконання завдання

**Варіант 0**

**Визначити тип шифротексту:**

* + Алфавит: АБВГДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ.
  + Шифротекст:

ФІЧЯШЬСЙЮЖФРУЙРЬІПЦЧШОРЧІГМПСЇЬІЧЧИЙНЛРЧМГСХМЙРПЧІДМЧРВШЇНФЯСЙИФСДСЯФШЬШПЬСПЧИЗЯЖЮИЧІЕШЗСЧЯАСГСНЗІЇШЧІЕШЗЛАЦФШЗЇМПАЦШЙЧШЧМЦШОМЙЙІОІЯРЮИЮЯЬШКРЦЦІЯМЦІЯРДЧРЦШПЧІДМЧЧИЦІНЮФШЬСЕМЩШИЮЧМЧЧИЦЩШЧИЯЯИЦЧШОРЧРИФМПІЦСЧИНЯМЬЦСЧЦЧШОРЧІЧІЯМЬЦСЧПСЇЬІЧЧИСЧЕРЦРЮРЧШЧСЦІЦРШЮЧШЙЧШКШЮХШЙІЦЧШОРЧІНЮАФАЩЧСЮЯЖЧІЇСЬФШХМФГСИШЇНЛЧІЧЧИЯШЄШ

**Статистика**

Шифртекст: Значущих для кодування =310

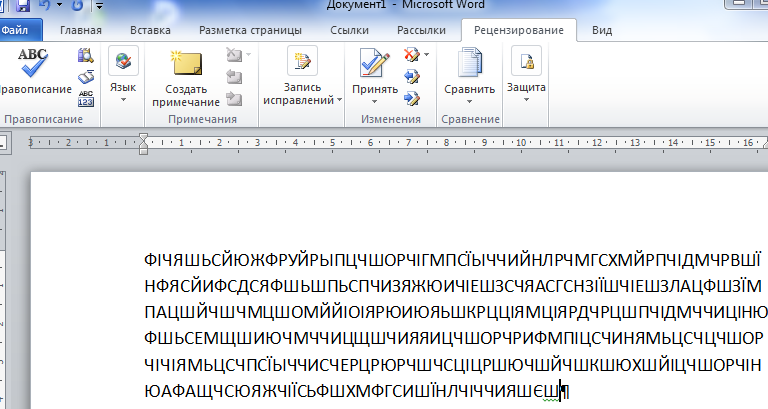
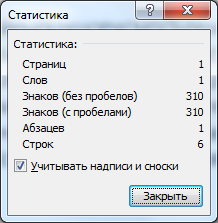
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М |
| 5 | 0 | 1 | 4 | 4 | 4 | 1 | 3 | 5 | 15 | 23 | 7 | 10 | 2 | 3 | 15 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |
| 7 | 6 | 9 | 18 | 20 | 0 | 1 | 11 | 3 | 19 | 44 | 30 | 3 | 11 | 11 | 15 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| текст | Н | О | А | И | Т | або-> | А | И | Т |
|  | 17 | 18 | 1 | 10 | 22 |  | 1 | 10 | 22 |
| шифр | ч | ш | і | с | ц |  |  |  | і |
|  | 27 | 28 | 12 | 21 | 26 |  |  |  | 12 |
|  | 10 | 10 | 11 | 11 | 4 |  |  |  | 10 |

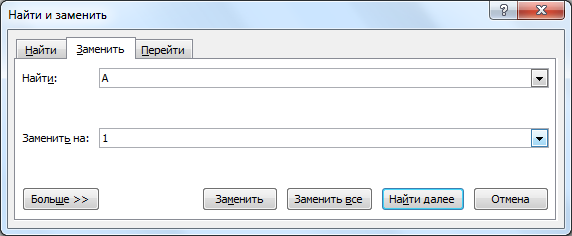
В результаті криптоаналізу шифротекста можливий ключ 10, 11, 22, 21.

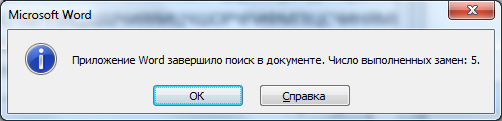
Перевірка: ФІЧЯШЬС -10 – канторі; або ФІЧЯШЬС- 11 – йаьснпи.

Очевидно, перший ключ є відповіддю. Програма для дешифровування на свій вибір. Це можна зробити у Word 2010 використовуючи статистику та режим заміни.

Зауваження. При заміні літери вводити краще цифру, а після отримання результату відміняти.





Коли обчислено значення зсуву (10) і є таблиця для підстановок перші заміни бажано теж зробити цифровими «А-И» на «0-9» і продовжувати з заміни «І-Р» на «А-И» і так далі, в кінці потрібно повернути «0-9» на «У-Я».

Крок 1.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифр | А | Б | В | Г | Д | Е | Є | Ж | З | И |
| код | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| код | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |

Крок 2.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифр | І | Ї | Й | К | Л | М | Н | О | П | Р |
| код | А | Б | В | Г | Д | Е | Є | Ж | З | И |

Крок 3.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифр | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь |
| код | І | Ї | Й | К | Л | М | Н | О | П | Р |

Крок 4.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифр | Ю | Я |  |  |  |  |  |  |  |  |
| код | С | Т |  |  |  |  |  |  |  |  |

Крок 5.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифр |  |  |  |  |  |  |  |  |  |  |
| код | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| код | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |

Вигляд таблиці підстановок в загальному виді.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| шифр | А | Б | В | Г | Д | Е | Є | Ж | З | И | І | Ї | Й | К | Л | М |
| код | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я | А | Б | В | Г | Д | Е |
|  | 5 | 0 | 1 | 4 | 4 | 4 | 1 | 3 | 5 | 15 | 23 | 7 | 10 | 2 | 3 | 15 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |
|  | Є | Ж | З | И | І | Ї | Й | К | Л | М | Н | О | П | Р | С | Т |
|  | 7 | 6 | 9 | 18 | 20 | 0 | 1 | 11 | 3 | 19 | 44 | 30 | 3 | 11 | 11 | 15 |

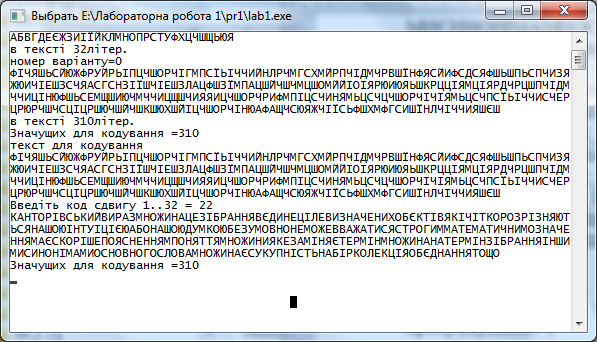
**Відкритий текст:**

КАНТОРІВСЬКИЙВИРАЗМНОЖИНАЦЕЗІБРАННЯВЄДИНЕЦІЛЕВИЗНАЧЕНИХОБЄКТІВЯКІЧІТКОРОЗРІЗНЯЮТЬСЯНАШОЮІНТУІЦІЄЮАБОНАШОЮДУМКОЮБЕЗУМОВНОНЕМОЖЕВВАЖАТИСЯСТРОГИММАТЕМАТИЧНИМОЗНАЧЕННЯМАЄСКОРІШЕПОЯСНЕННЯМПОНЯТТЯМНОЖИНИЯКЕЗАМІНЯЄТЕРМІНМНОЖИНАНАТЕРМІНЗІБРАННЯІНШИМИСИНОНІМАМИОСНОВНОГОСЛОВАМНОЖИНАЄСУКУПНІСТЬНАБІРКОЛЕКЦІЯОБЄДНАННЯТОЩО

**Розставте пробіли. Отриманий текст має вигляд.**

КАНТОРІВСЬКИЙ\_ВИРАЗ\_МНОЖИНА\_ЦЕ\_ЗІБРАННЯ\_В\_ЄДИНЕ\_ЦІЛЕ\_ВИЗНАЧЕНИХ\_ОБЄКТІВ\_ЯКІ\_ЧІТКО\_РОЗРІЗНЯЮТЬСЯ\_НАШОЮ\_ІНТУІЦІЄЮ\_АБО\_НАШОЮ\_ДУМКОЮ\_БЕЗУМОВНО\_НЕ\_МОЖЕ\_ВВАЖАТИСЯ\_СТРОГИМ\_МАТЕМАТИЧНИМ\_ОЗНАЧЕННЯМ\_МАЄ\_СКОРІШЕ\_ПОЯСНЕННЯМ\_ПОНЯТТЯ\_МНОЖИНИ\_ЯКЕ\_ЗАМІНЯЄ\_ТЕРМІН\_МНОЖИНА\_НА\_ТЕРМІН\_ЗІБРАННЯ\_ІНШИМИ\_СИНОНІМАМИ\_ОСНОВНОГО\_СЛОВА\_МНОЖИНА\_Є\_СУКУПНІСТЬ\_НАБІР\_КОЛЕКЦІЯ\_ОБЄДНАННЯ\_ТОЩО

При бажанні можна скласти програму на будь-якій мові програмування.

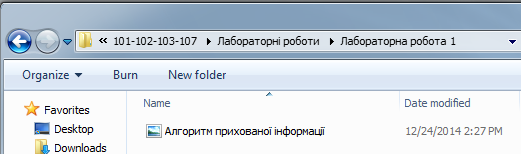


1. Цікавинка. Виконувати не обов’язково!

Стеганографія - це наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі. На відміну від криптографії, яка приховує зміст секретного повідомлення, стеганографія приховує сам факт його існування. Стеганографії зазвичай використовують спільно з методами криптографії, таким чином, доповнюючи її.

Перевага стеганографії над чистою криптографією полягає в тому, що повідомлення не привертають до себе уваги. Повідомлення, факт шифрування яких не прихований, викликають підозру і можуть бути самі по собі викривають в тих країнах, в яких заборонена криптографія. Таким чином, криптографія захищає зміст повідомлення, а стеганографія захищає сам факт наявності будь-яких прихованих послань.

Приклад конкретної стеганосистеми (на основі зображень JPEG) і схема її реалізації можна прочитати в



Варіанти завдань.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ВАРІАНТ | | ШИФРОГРАММА | | |
|  | | НСУСХНГКФХСУЙЬРГЖСЕКЖНГСФРСЕЙХЗСУКЛПРСІЙРДЦОЙЇГНОГЖЗРКЕКЖСПЙПРКПЗЩАНЙППГХЗПГХЙНСПЄЗСУЄСПНГРХСУСПЦЖУЦЄКМТСОСЕЙРКПЙРЦОСЄСФХСОКХХВТСВЕГХЗСУКЛПРСІЙРДЦОГЇЦФХУКРЦХГЇЗРХЦЇКГЇПСПДГЄГХАПГГЕХСУЙХЗХРЙПЙПГХЗПГХЙНГПЙЕСРЙТСДГЬЙОЙЕРКМПСІОЙЕКФХАФХЕСУЗРРВПЗХГПСЕЙПГХЗПГХЙНЙХСДХСЧСУПГОАРСЛСЖРСФХГМРСЛФЙФХЗПЙТСРВХАКТУЙРЩЙТКЕЇГЖСТСПСЄСБВНСЛПСІРГДЦОСДЕЙНОГФХЙЇИЖЙРЙШТСЇЙЩКМЇПКФХУКЇРСПГРКХРЙШХУГЖЙЩКМРСЖГОЗНЙШСЖЙРЕКЖСЖРСЄСУСЇЖКОКЕПГХЗПГХЙНЙТЗУЮКХГНКЖСФЙХАЦФТКЮРКФТУСДЙДЦОЙЕЙНСРГРКЕІЗРЗЇГДГУСПТКФОВЕЙРЙНРЗРРВНГРХСУКЕФАНСЛХЗСУКЛПРСІЙР | | |
|  | | ХЇФЖСЦОМФОВОЇХШТОЇФНСНИНЄИНТНИЩЙХЧОПСЖФЩХЧЖБНУЖТХШЬЦЙЧЙБФХШЩЙРЩЖСМИЖФНЯЦЖЧЖЇХСШОИЖЗХЖФЩНФХУОРЩЙХЧОПУФХЛНФИНФНСТЖСЧНМХИЖШНЩЬЖАОЄХЇФЖБЖШЩНФЖУЖЩЙУЖЩНСОИЦХШНТЖЕБНШДФЖВЩЬБФОШЩДШЮХЧУЬТДХИЖФНЯЖФЩНФХУОРИИЖЛЖТЖМЖСЧЖГЙФЙЦХУОБЖЩНАОШЬЦЙЧЙБФХШЩОЖЗХФЙФЖЇЖИЖЩНПУИЙТНСХІХМФЖБЙФФЄЬЩХРБЖШЄСОФВЖШСЖЛОУХИОЇЦХИОЇЖТДФОВЖІЧЬЦЖУЖЩЙУЖЩНСОИМХШЙЧЙЇНТЖШИХПМЬШНТТЄФЖЦХВЬСЖЯЗОТДВХЗІЧЬФЩХИЖФНЯЩЖЩХБФНЯЦЧНФАНЦОИОСХФАЙЦАОРФЖЄСНЯУХІТЖЗЗЬЩНЦХЗЬЇХИЖФЖФЙШЬЦЙЧЙБТНИЖЩЙХЧОЄУФХЛНФ | | |
|  | | ЮШКНЮУЕЬЗЬПИЮУЦНЗЧШЦЧЦХЦІЗХЦТПУЕТЗЯЦШФЗУЕХОАЗИЦЗТЩПЦФЗЬОВХОАЩОЩЬКФЖТПЩУЮМЗЬЕЯЮХЙЗФКХЬЦФЩЮВЗЩХЦРЬКЦШПРФХЦМОХЗНХЗВОЬЕЯЮХЙЗФКХЬЦФІЩПЛРТУЗЩОВХЦРФЗЬКФЗЬОТОІЗМУОІПЩЬЕБОАЙЦЩУПЙМКХЕЩКШКЙПХГЦЇЦЧПЙТШКЩУЄЛЬЦСЯЗТЬДЦНХЗВХОСІХКЩЦТЮЩЬЗХЦІУКХХЖЗТЩПЦФЗЬОВХЦРЬКЦШПРФХЦМОХНШЦИОУОЬЗТПІОЙЗЬХПФЗЬКФЗЬОТОПФОЩУОЬКУПХЗГЦЇЦЩЬЦУПЬЬЖЖТИШЗЩЩКУЙЇПУЕИКШЬТЇКЙКУЕЬЗПХЩЕЦЇЦЙХПЬКЦШПЖФХЦМОХБКФЗЬКФЗЬОВХЗЬКЦШПЖХЗЖТПСЇШЮХЬЮЛЬЕЩЖИПУЕГПЩЬЕШЦНЙПУПІЩЮВЗЩХЦРФЗЬКФЗЬОТОЖТХКЧКШКШІХЦРЬЗТПЙОЩТШКЬХЦР | | |
|  | | ФУТДЧЧДСТУЙЛТЛЦФУЦУЄЛКЕИЕТТДСТУЙЛТИРДТЕАЛЬЮМРІОИУЦЧЕЧТВУЄШИІЖЛПРЕИІТТДУЦТУЖЧЕПКЖЕТУНМТЧШНЧЛЖТУНЕЄУТЕНЖТУНЧІУХМНСТУЙЛТДПЕЖЗУРУЖТЛЬЦЖУНЬФУРУЙІТТДЬКЄІХМЗЕЇМИІНЧЕХІКШРВЧЕЧЛКЕЦТУЖТЛПЕЧІУХМНЗПЕТЧУХЕЖМТЧШНЧЛЖТМОЧІУХМНСТУЙЛТФУТДЧЧДСТУЙЛТЕТЕРІЙЛЧВИУФІХЖЛТТЛЬТІЖЛКТЕЯЕРВТЛЬФУТДЧВЧУЄЧУЖУТУТІСУЙІЄШЧЛУКТЕЯІТУЯІХІКМТАМЄМРВАФХУЦЧМЧІХСМТЛЕЄУУЄЇПЧЛЕФУДЦТГЇЧВЦДТЕФХЛПРЕИЕЬЕФІРГГЯЛИУТЕАУНШДЖЛЧЕМТЧШМЮМНЧЕПЛСЛФУТДЧЧДСЛЖСЕЧІСЕЧЛЮМЇЧЕПУЙФУТДЧЧДЯЛЦРУФХДСЕЧУЯПЕФРУБЛТЕЧУБУ | | |
|  | | ЮЯТЦЧЙНЙШТШЩЬРТЩШЬРВБИАЧВРТБТШЩЬРТЩЙНОАЇБЦЬЛТДЕТГЯШЩЬРТЩЙЧУБОЯВЦЯЙФЩАИЦЬМЬЙЧГЙЛУБВШЩЬРТЩЙШОЖЦЙЩЕУЛЦТПЛЙШЩЬРТЩЙЮЙЯЩТДЄТАОЧШЩЬРТЩЙЯЬСЛЇСЦУЛНОЇЦЬМЬЯУЛЩЇЩЩЇБЙУЩЩЙЮТАИШУШЩЬРТЩТЮЬСЩЙЄЙІБИАЇЇЦЮЯЙЛТЧЬЛОЧТЦТШТЧУБОЯЙШТНЧЇНОЇЦТДШЩЬРТЩВШЙБОШЙБТЕУЛРТЛЙІБИАЇАБЙЧУЮЬСЩЙЄОЩЩЇЩЙЮЯТЦЧЙНШЩЬРТЩЙЕУЧТДЄТАОЧШЩЬРТЩЙЩЙБВЯЙЧИЩТДЄТАОЧШЩЬРТЩЙЯЙЕУЬЩЙЧИЩТДЄТАОЧШЩЬРТЩЙНУХАЩТДЄТАОЧБЬЗЬЬКПЦБТСЇЦТДАЦЧЙНЙПБИАЇСЙНЙЩЙШЩЬРТЩЙЩЙСТЛЙІБИАЇФФОЧОШОЩБЙШТОЧОШОЩБТШЩЬРТЩЮЬСЩЙЄЙБТШОШЬШЙЧТШТЧУБОЯЙШТЧЙБТЩАИЦЬМЬЙЧГЙЛУБВСЩЙЦЩЙЧОРЩЬАБУОЧОШОЩБЙШЩЬРТЩУПАБТЧУСЙЕУПІЮОЯЖЬФЧУБОЯТМЯОЕИЦЬМЬАЧЬЛЙУАЩВЛЙБТНЧЇБЬМЬЗЬКЮУНЦЯОАЧТБТЗЬНОЇЦТХОЧОШОЩБЩОЩЙЧОРТБИШЩЬРТЩУЛРТЛЙІБИСЙЮОЯОЄОЩЩЇЮЬСЩЙЄОЩЩЇУАЩВЛЙЩЩЇ | | |
|  | | РСТЇКСЧСДЙКЄДВЦБХОЛСЮИССТВГОАТОЛПБОЛХЦБММИПИРИСЦЛЄХОЛСЮИССДЦТЕЦТЛХСЧІСДЦЧФДПБСИЮКХПТАТІЮКХПТРИПИРИСЦЛЄЬЛІМРСТЇКСКЧУФТЦКЄСТРЧФДЙЛРСТЇКСДІСИХОЛСЮИССТВЗПГЙДЗДССГРСТЇКСКЧЦЄТФИСТМЙЕЧЗБГОКЩИПИРИСЦЛЄЕЧЗИРТЄКОТФКХЦТЄЧЄДЦКЗЄДЦДОЛХУТХТЕКЄТХСТЄЛТЕТЩЛЙСКЩПИЇКЦБУТЙСДЮИССГРСТЇКСКЙДЗТУТРТЖТВШЛЖЧФСКЩЗЧЇТОГОАТЙДЗДСЛЗИГОЛТЕІОЦКЦТРСТЇКСДЬКЩТЕІОЦЛЄУТЙСДЮДІЦБХГЧШЛЖЧФСКЩЗЧЇОДЩЄГОКЩРЛХЦКЦБХГУИФИПЛОЧХЛЩИПИРИСЦЛЄЄЛЗУТЄЛЗСТМРСТЇКСКЙТХЦДССБТЖТЙДЧЄДЇИССГЄКУПКЄДІАТЄЦДОКНХУТХЛЕРТЇЧЦБЕЧЦКЙДЗДСЛЦЛПБОКХОЛСЮИССЛРСТЇКСКУТФГЗТОЙДУКХЧИПИРИСЦЛЄРСТЇКСКУФКЬБТРЧУТЙСДЮИССЛІСИЛХЦТЦСКР | | |
|  | | ЕЯШТГШЮДУЕЯЧЄЧКВВТБШФМЦВЕБВРБЧИШТУЬЮОБЄВДШРЕЛЮВЩЄУВДШЩАБВХЧБПЖРДВЦСЯНТАБВХЧБЧНЮБВРВСВЕОАВЕЄШЬБВСВВПФЮЄОАОЄУАОЄЧЇБВСВТВЕЯШТХУББНЄВАЖБУВПИШТБВДВЦДШЦБНЄЧЄОЮШТРОДШЦБШВПФЮЄЧНЮУЯУАУБЄШАБВХЧБОНЮОЕЮЯОТОФЄЛЕНЦФТЧБВСВУЯУАУБЄОЦВЮДУАОАБВХЧБЧАВХЖЄЛРЧЕЄЖГОЄЧРДВЯШУЯУАУБЄШРНЮВЩЕЛШБЙВЩАБВХЧБЧТДЖСЧЬЕГВЕШПЦОТОББНАБВХЧБСДЖБЄЖФЄЛЕНБОЦОЦБОЇУББШЦОСОЯЛБВЩРЯОЕЄЧРВЕЄШОПВГВДВТХЖРОЯЛБВЩГДВІУТЖДЧТЯНРЕШИВПФЮЄШРКВЖЄРВДММЄЛВГЧЕЖРОБЖАБВХЧБЖЄОЮЧЬРЧДОЦЇЧЄОФЄЛЕНЄОЮАБВХЧБОРЕШИЄОЮЧИУЯУАУБЄШРТЯННЮЧИРЧЮВБЖФЄЛЕНРЯОЕЄЧРШЕЄЛЦОЦБОЇУБЖРЯОЕЄЧРШЕЄЛАОМЄЛРЕШУЯУАУБЄЧАБВХЧБЧШЄШЯЛЮЧРВБЧЦОАШЕЄЛРУДЄЧЮОЯЛБВЩДЧЕЮЧШБВТШЦОГЧЕЖМЄЛТРВЮДОГЮЖІУЬЕГВЕШПФПШЯЛЙЦОСОЯЛБЧАЕГВЕВПВАЦОТОББНАБВХЧБ | | |
|  | | ЩГЦИЕПЩЖІЛДЕЗИЮИСЕХДЕЗИСАДЕЗИЮЄЖЬЄЖЕУЦХЦДДЮГСИЦГСИЬЛДЬЙУЬБВСХЕБУУЕХЬИОЗРЄЕДРИИРГДЕШЬДЬРБСДЦГЮЗИЬИОШЕХДЕФЕЦВЦГЦДИСИСБСГДЕШЬДСДСЩЬУСЧИОЗРЄЕЖЕШДОЕПГДЕШЬДЕПЮЄЕЩДСЛСЧИОЗРЩДСБЕГЄЦЖЦБЖЦЗВЦДДЕФЕБЕВСДСЄЖЬБВСХРБНЕХЕЗВЮХШІЧИОЗРГДЕШЬДСЕТЧБИЮУРБЮЄЕУЬДДЮЩСХЕУЕВОДРИЬЄЦУДЮАУВСЗИЬУЕЗИЮЮУЄЕХСВОМЕГІЩРЗЕУІЧИОЗРНЕИСБЬЙЕТЧБИЮУДЦЮЗДІЧИЕЩЖІЛДЮМЦЗБСЩСИЬНЕМІБСДСГДЕШЬДСЄЕЖЕШДРДЮШЕФЕВЕЗЬИЬЯЯДЦЮЗДІПЛЕПЄЕЖЕШДПГДЕШЬДІГЕШДСЕЩДСЛСИЬЩСХЕЄЕГЕФЕПТІХОРБЕЯЗІЄЦЖЦЛВЬУЕЯУВСЗИЬУЕЗИЮЖСЩЕГЮЩИЬГИУЦЖХШЦДДРГГДЕШЬДСДЦЄЕЖЕШДРГЕШДСЩСГЮДПУСИЬЖЮУДЕЗЬВОДЦАЕГІИУЦЖХШЦДДРЮЗДІПИОЦВЦГЦДИЬРБЮДСВЦШСИОГДЕШЬДЮ | | |
|  | | СЙЄОПРИЇПЇЄДЙОПРИЇПЇЙПВІЇДВАФЯУБТЙДПЇОЇБМЮРДРПЇУМНВЄВАФЯУБІФЇЧУВОЇЧЖНЖОЖПФЙДОПРИЇПВПВІЇДВЗФЯУБСЙЄОПРИЇПРАОПРИЇПЇФРЄЙЙФЙНЯМЇФРЄЙМРНЇМРИПЇЛЖНЖОЖПФОПРИЇПЇПВНЖИЇФЯФВМРИОПРИЇПЙМВИХФЯФВМРИЮРОПРИЇПВОЙУФЇФЯУБХОПРИЇПЙІПВМЇПВНЖИПРУФЙСЙЄОПРИЇППВІЇДВАФЯУБІПВМВОЇДМНАЩЖППБПЖДВИМРСЖТЖМРПВФЇУЯЮРЄРТЙДПАЗФРЄЙЙФЙНЯМЇФРЄЙМРНЇРЄПРЩВУПРДЇМРПХАФЯУБЄДВДМНАЩЖППБЄРЙЄРМТЙОФРЕРБМЮРДМНАЩЖПРДЙДМНАЩЖПРДФРЄЙДМНАЩЖПРДРУФВППЙЄДВЦВМФЇЩВУФРДЇМРТЇУФРДХАФЯУБСТЇЄРДЖЄЖППЙФДЖТЄИЖПЯСТРТЙДПЙУФЯЄДРЧІВЄВПЇЧОПРИЇП | | |
|  | | АБСВМЗЦЧЯМРЮЯАУХЯМЮХДМЧЖЯЦОЬМГДХОАГДЦРЬЛЮЯАУХЯЮАУЯМООСГДХВЛРДСАВСДХЩАЮЯАУХЯЯХЖАБСВМЗЦШВСФЕЬЙДМДАЮОХЩАЯМЯЯЛЛЩХЖНЕРЕДЙДМЩАУЮЯАУХЯХФМРАБАЮАПАКЗХЖАБСВМЗЦШЮАУЯМЩАЯГДВЕКОМДХЦФФМРМЯХЖЮЯАУХЯЯАОЦЮЯАУХЯХЯСЖМШЦРСЛЩЦЮЯАУХЯХАНТРЯМЯЯЛЮЮЯАУХЯЯМФХОМТДЙГЛЮЯАУХЯМДХЖСЬСЮСЯДЦОЛЩЦЯМЬСУМДЙЖАИМНАРЯЦШФЮЯАУХЯИХГХЮОАЬЦИЯААБСВМЗЦЛАНТРЯМЯЯЛЮЯАУХЯФМБХГЕТДЙГЛДМЩБСВСДХЯАЮЮЯАУХЯЦЯМФХОМТДЙГЛЮЯАУХЯМЇАГЩЬМРМТДЙГЛФДХЖЦДЦЬЙЩХДХЖСЬСЮСЯДЦОЛЩЦЯМЬСУМДЙЮЯАУХЯМЮЦАРЯАИМГЯАЩМУЕДЙЇАЮЯАУХЯХЦЯСБСВСДХЯМКДЙГЛЛЩЇАБСВСДХЯБЕГДМЮЯАУХЯМ | | |
|  | | КЛБМЩТЄЖКЬВАЙЩЙЙШОЩЛБМБОЕЙПЇЙКГЕЙЇКГПОЦЬПОЕЛКФЕМБЙЄЙЩЮЕЛЩАКИАКЮЄІЦЙКЖНПИПЛЙКНОЄЇЙКГЕЙОЩИКЬВАЙЩЙЙШЇЙКГЕЙНИІЩАЩВОЦНШДОЕСБІБЇБЙОЄЮШИЄЙЩІБГЩОЦСКУЩЬКАЙЄЗДЇЙКГЕЙАЩЙКЖНПИПЛЙКНОЄЩЛБМБОЕЙЇЙКГЕЙЇЄНОЕОЦОЄІЦИЕОЄБІБЇБЙОЕШИЄКАЙКУЩНЙКЙЩІБГЩОЦИКГЙЄЗДЇЙКГЕЙМЄДЙЕТБЧЇЙКГЕЙЄЙЩДЕЮЩВОЦНШЇЙКГЕЙЩОЕСБІБЇБЙОЄЮШИЄЙЩІБГЩОЦЇЙКГЕЙЄЄЙБЙЩІБГЩОЦЇЙКГЕЙЄКОГБНЕЇБОМЕУЙКЧМЄДЙЕТБЧЇЙКГЕЙЄЙЩДЕЮЩВОЦНШЇЙКГЕЙЩХКНИІЩАЩВОЦНШДПНЄСБІБЇБЙОЄЮЇЙКГЕЙЕШИЄЙБЇЄНОШОЦНШЮЩОЩИКГПНЄСБІБЇБЙОЄЮЇЙКГЕЙЕШИЄЙБЇЄНОШОЦНШЮ | | |
|  | | ЯУЧЦУЩЛЮЦРТХИЮЛХИЮПГЦРТЮЛЧЩРСІЯЇИМОЩЯГЦЧЇЇИНИЮПЕЧЇЬРЩЧОЙФЗКЯЇИЦРХЦЧНПЦПМШРКХЦЧНПЦИХПКЛЗУЧСАРУЬЧЇИЦЧСХЦЧНПЦПЗУЯЦИОПЇИЖЮЄЯЦРЇЛЩЬИФЄЦЧЖХЦЧНПЦЧЖИІЧЯЦРЇЛЩЬЯХЧХЦИШЩПУФИКЇЛФЛХЛЦЮИЩЦРТИФЙЛІЩРЮИУЧЖЯЦРЇЛЩЬИФЄЦЧЖХЦЧНПЦЧЖХЧНЦИЇЇИНИЮПХЦЧНПЦЯКРТЬЦПБГПЬЛФЯЇПЕРТИФЙЛІЩРХЦЧНПЦЯУЧХШФЛУЬЦПБГПЬЛФЇИЩПАХЛЮПВРХЦЧНПЦЯВРФПБГПЬЛФЇЮЩИКПВРТЦРТШФИЦРХЛЮЩРСХЦЧНПЦЯЇЬРБЮЧГЧУШФЧЕПЦПИІЧХЦЧНПЦЯЇЬРБЙЛЧХЛЮЩПГЦПБЧІМУЮРЇЮЧІЮЧХЦЧНПЦЯХЦЧНПЦЮЧГЧУЦИШФЧЕПЦРЮЧЕЧЗУЕЧОИАРУЬЧЇИЦИЯЦРЇЛЩЬИФЄЦИХЦЧНПЦИЮЧКЧШЧЇЦЛЦЦЗХХЦЧНПЦПЦИОПЇИМЮЄЬЗХЦЧНПЦИЇЬРБЛФЛХЛЦЮРЇЯЦРЇЛЩЬИФЄЦЧСХЦЧНПЦПЗУРЦЛЦИФЛНИЮЄХЦЧНПЦР | | |
|  | | ТГПЖЮУЙЄАХШИІУДРЄЙЕЄЖЬЯЄЙЗИЯВЄТЇЯЕЄЖЬЯЄЙХІАЛЄУЇЙИУДРЄЯЛНЯІШДЇЖЧЖЗЖХЄШЄЄТЕЕЄЖЬЯЄЯХІАЛЗУИЄЯЛЄУЇЙИУДРЄЯЛНЯІШДФЙЧШЕЄЖЬЯЄУХІАЛЄШЗУИЄЯЛЄУЇЙИУДРЄЯЛНЯІШДЮУЮЄУНЯЕЖЙХЯЦДТЧАЇЖЇЖЬЄЖІЇШВХДУІЇЯХЖІЇАХХШЧШЄЯЛХЯПШЇШЖИШЇЯГЖЕЄЖЬЯЄЄЯЛЖЗШИУМАВУІЖМАУЇЯХЄАІЇРГЖЕЙЇУЇЯХЄАІЇРЧЯІЇИЯФЙЇЯХЄАІЇРАЧШЕЗЖЇШЄЇЄАІЇРАЄХЖДСЇЯХЄАІЇРЗИУХЯДУЮУГЖЄЯЧШЕЖИЦУЄУЮУЮЄУНЯЕЖПЖЗИУХЯДУЧШЕЖИЦУЄУЗИЯЗЙІГУСЇРЙЮУЦУДРЄШЄЄТЧДТІЙГЙЗЄЖІЇАЕЄЖЬЯЄЧШГУИЇАХЗИТЕЯВЧЖФЙЇЖГЕЄЖЬЯЄЖГИШЕЖИЖЮЦДТЄШЕЖПШЖЧЄЙЧЙЬШХУЬДЯХЙЖЗШИУМАСЄУЧЕЄЖЬЯЄУЕЯ | | |
|  | | ЩЬЕХЇКИЧБЖІЇФЖБЖЩИЦЛКЕИЖЖЗИЯБЗВЗХАБЧХЮКТЙФЖЗИЯБЗХЧЙВНІХЇЧФЕБНІЬЇРБДЕИЖІИЗЬЗКЗХЄЬЯБКТІЬЇРВДЖЗИЯБЗВХЩЇЛШБДЖЗИЯБЗВЩЇЛШВДЖЗИЯБЗВЩЬЕХЇКВЧЩИЦЛКИЕІЇБЇИЩЗИЛАХШХЄТЗУЮКТЙФЗХЧБІХЩИЕЩИЧВЄТЗИГЙЕВЗПЬЗЗИГЙЛЕЛІЗИЙКВЖЗИЯБЗЩЄФКИШИСИЦЧВЩЇВАЗБКБАХІБЙЗХЦИЇЛЩЬЕХЇКИЧИШИЩИЦЛКЕЛЧВЩЖЗИЯБЗБФЕХЙЕЄХЩХЮКТЙФАЬЄЬЖЬЗКВЧАХІБЙЛУКТЗЬЛМВШЛЇЗБНХЧЕЇЛШЄБНЩЛЯЕХНВЗХАБЧХУКТЕИЇКЬЯЬЖЧЬЕКИЇИЖХЦИЧІИЇФЩЕИЧХЗБЖЗХЦИЇИЖЩИЧЯБЗИУЕИЇКЬЯЛЗХАБЧХУКТЕВЄТЕВЙКТДИШИЕИИЇЩБЗХКЩЧХЕИЇКЬЯВИЩЗХЕИЧИГЩИЧЯБЗБЧЧХЯХУКТЙФЇВЧЗБЖБКИЩВВКВЄТЕБКИЩВЕИЄБЇВЧЗВГНЗВЧВЩІИЧВЩЗВЕИИЇЩБЗХКБЩЬЕХЇКВЧЩИЦЛКИЕЖЗИЯБЗБЗХЙЬЦЬЇХАВЧЗХАБЧХУКТЖЩЬЕХЇКИЧБЖХЦИІЇФЖБЖЙКЬІЬЗЬЖЖЗИЯБЗБ | | |
|  | | ИІЇБГІЧЮДЄЛІГПСГЛЯЗЧШЇИІЇБГІЧМЇСЇЖЖЇЇКЮГІЧМІЇЕЙКЦИЇЕМЇРЯИІЇБГІЧЙЧКЧШЇИІЇБГІЧМЇСЇЖЖЇЇКЮГІЧМІЇЕЙЗЇУГІГЖЇЇКЮГІЧМІЯВЇШКЧБЯІІЦМЇСЇЖЙЗЇУГІГЩЙЯКТЯШНЗЇВЧЙКЇЙЇІЇЩЧІЇОКЧІРНВФЖГИИЧМЯИЧМГЖЇИДОДЗЇЛЇОЇИКЯІЯЮЯЖЧКМЇИМЇИНЩЩЯЮЯІЧМЯЇКЯМГЖЇИІЇБГІІЧЇЙЯКЧРДЦДІЧВГЩЧАМФЛЦЮЯЖЧКМЇЩГИЮЇШНМЖЇИЇЙЯКЧРДЦЮЯЖЧКМЇЩЇЬЇЮЇШНМЖНІЯЧЛЇРДЧМГЩІЧДІЯЖЇИНМЧМГЩІЧМЇШМЇИІЇБГІГЛЖДІСЯІІЧИІЇБГІЧЯЗЯИЯІМЧИГЦЖЇЕАЛГИЩЇЗГЗДМЯКГРГОКГЛЙЯРДЧЗФІДВІЧЖГМЇУЇІЧВГЩЧАМФЛЦЧЗОЧЩДМЇИЯЗЯИЯІМГЮЯЖЧКМЇЩЇЬЇЛМЯЙЯІЦІЧВГЩЧХМФЛЦЛЗЇЩЧИГЮЇЩБГІГЩЧЗОЧЩДМД | | |
| Варіант | Сдвиг | | стат |
|  | 3 | | 510 |
|  | 7 | | 440 |
|  | 8 | | 452 |
|  | 5 | | 449 |
|  | 12 | | 639 |
|  | 4 | | 548 |
|  | 17 | | 633 |
|  | 20 | | 555 |
|  | 2 | | 473 |
|  | 15 | | 487 |
|  | 28 | | 459 |
|  | 9 | | 544 |
|  | 22 | | 466 |
|  | 24 | | 586 |
|  | 26 | | 479 |