ЛАБОРАТОРНА РОБОТА № 1.

ТЕМА: МЕТОД ШИФРУВАННЯ ДАНИХ «ШИФР ЦЕЗАРЯ».

МЕТА: ОЗНАЙОМИТИСЬ З МЕТОДОМ ШИФРУВАННЯ ДАНИХ «ШИФР ЦЕЗАРЯ» І НАДАТИ ЙОГО ПРОГРАМНУ РЕАЛІЗАЦІЮ

ТЕОРЕТИЧНІ ВІДОМОСТІ

Шифр Цезаря (Caezar, 100-44 рр. до н.е.) реалізує кодування фрази шляхом «зрушення» усіх букв фрази на певне число kk (у оригінальному шифрі Цезаря це число kk дорівнювало 3). Якщо буква шифрованої фрази має в алфавіті позицію jj, то вона в «шифровці» замінюватиметься буквою, що знаходиться в алфавіті на позиції jj + kk.

Нехай kk = 3 і фразою для шифрування буде «i remember that september». Використовуватимемо латинські букви із стандартним проходженням букв в алфавіті. Результати шифрування вказаної вище фрази показані нижче в таблиці:

1	**i**		**r**	**e**	**m**	**e**	**m**	**b**	**e**	**r**		**t**	**h**	**a**	**t**	
2	**9**	**0**	**18**	**5**	**13**	**5**	**13**	**2**	**5**	**18**	**0**	**20**	**8**	**1**	**20**	**0**
3	**12**	**3**	**21**	**8**	**16**	**8**	**16**	**5**	**8**	**21**	**3**	**23**	**11**	**4**	**23**	**3**
4	**12**	**3**	**21**	**8**	**16**	**8**	**16**	**5**	**8**	**21**	**3**	**23**	**11**	**4**	**23**	**3**
5	**l**	**c**	**u**	**h**	**p**	**h**	**p**	**e**	**h**	**u**	**c**	**w**	**k**	**d**	**w**	**c**

1	**s**	**e**	**p**	**t**	**e**	**m**	**b**	**e**	**r**
2	**19**	**5**	**16**	**20**	**5**	**13**	**2**	**5**	**18**
3	**22**	**8**	**19**	**23**	**8**	**16**	**5**	**8**	**21**
4	**22**	**8**	**19**	**23**	**8**	**16**	**5**	**8**	**21**
5	**v**	**h**	**s**	**w**	**h**	**p**	**e**	**h**	**u**

Пояснення до таблиці:

1-й рядок - фраза для шифрування;
2-й рядок - номери букв фрази для шифрування в латинському алфавіті;
3-й рядок - номери букв фрази для шифрування, збільшені на 3;

4-й рядок - результат «ділення по модулю 27» чисел 3-го рядка;
5-й рядок - зашифрована фраза.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Ознайомитись з методом шифрування даних «Шифр Цезаря».
2. Написати програму для шифрування та розшифрування за допомогою метода «Шифр Цезаря», передбачивши в ній можливості вибору:
    a. Файлу.
    b. Алфавіту (наприклад, англійський та український).
3. Написати програму для дешифрування повідомлення шляхом перебору всіх можливих значень зсуву .
4. Підготувати звіт про виконання роботи. Звіт оформлюється у вигляді документу Word з такою структурою:
    a. титульний лист,
    b. тема і мета роботи,
    c. опис алгоритму роботи програми у вигляді блок-схеми або UML- діаграм (класів, діяльності тощо),
    d. функціональні можливості програми (основні і додаткові),
    e. фрагмент програмного коду, що реалізує базову функціональність,
    f. особливості програмної реалізації окремих функцій.
5. Електронну копію звіту відправити на адресу: George@aprodos.kpi.ua.