МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

**Звіт до лабораторної роботи №1**

на тему “Застосування класичних симетричних систем шифрування  
для захисту даних ”

Виконав студент(ка) *Борщ Дмитро*

Варіант *№ 1*

Група КБ-01

Перевірила Лаврик Т.В

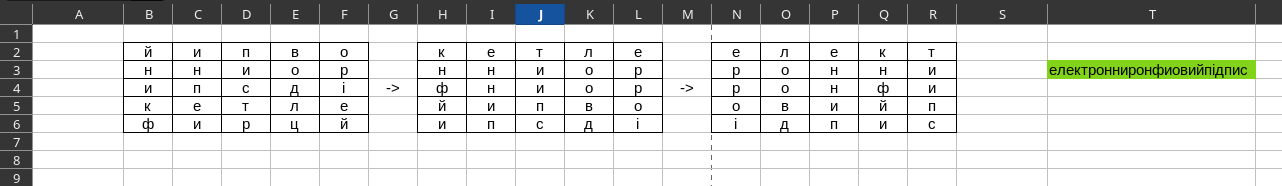
**Суми 2022**

**ЗВІТ 1**

Табличний шифр: подвійна перестановка

**Завдання 1 (4 б.)**

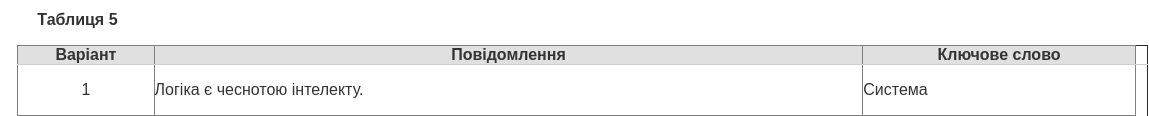
Розшифруйте шифротекст "ЙИПВО ННИОР ИПСДІ КЕТЛЕ ФИРЦЙ", отриманий методом подвійного перестановки, розмір таблиці 5×5, ключі 54213 (стовпці) і 42513 (рядки).

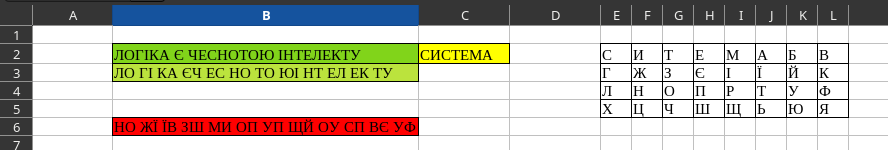


Біграмний шифр Плейфера

**Завдання 2 (5 б.)**

Зашифруйте повідомлення, використовуючи алгоритм Плейфера відповідно до Вашого варіанту (табл. 5). Розмір таблиці для шифрування 4 × 8.

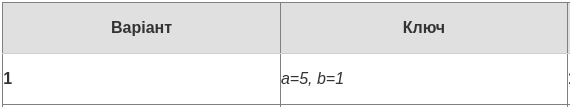




Аффінна система підстановок Цезаря

**Завдання 3 (5 б.)**

Зашифруйте повідомлення "МОВА РОСТЕ ЕЛЕМЕНТАРНО, РАЗОМ З ДУШЕЮ НАРОДУ (Іван Франко), використовуючи аффінну систему підстановок Цезаря з ключами відповідно до Вашого варіанту (табл. 8).





Система шифрування Віженера

**Завдання 4 (4 б.)**

Зашифруйте повідомлення, використовуючи шифр Віженера відповідно до Вашого варіанту (табл. 5).

