МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ФАХОВИЙ КОЛЕДЖ ПРОМИСЛОВОЇ АВТОМАТИКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ОДЕСЬКОГО НАЦІОНАЛЬНОГО ТЕХНОЛОГІЧНОГО УНІВЕРСИТЕТУ»

Практична робота № 2

Тема: Шифри перестановки. Метод шифрування подвійною перестановкою
Мета: ознайомитися з алгоритмами шифрування та дешифрування у шифрі подвійної перестановки.

Виконав:
Студентка ФКПАІТ ОНТУ
групи КП-222
Пащенко Ангеліна
Оцінка:
_____

Одеса 2025

Завдання

1. Ознайомитися з особливостями шифрів перестановки.
2. Сформулювати алгоритм шифрування.
3. У відповідності з номером студентського квитка з таблиці 1 вибрати вихідні дані до виконання завдання
4. Зашифрувати відкрите повідомлення згідно свого варіанту
5. Обмінятися даними з сусідом по парті та виконати дешифрування
6. Визначити ефективність і криптостійкість шифру

Зашифрувала Варіант №16

16	Провідник пильно дивився	Батьківщина

ПРОВІДНИК ПИЛЬНО ДИВИВСЯ

Символів: 22 $k_{стовпців}$= 2 1 $k_{рядків}$ =7 3 9 5 6 8 1 11 2 4 10

	2	1
7	**П**	**Р**
3	**О**	**В**
9	**І**	**Д**
5	**Н**	**И**
6	**К**	**П**
8	**И**	**Л**
1	**Ь**	**Н**
11	**О**	**Д**
2	**И**	**В**
4	**И**	**В**
10	**С**	**Я**

До перестановки →

	1	2
7	**Р**	**П**
3	**В**	**О**
9	**Д**	**І**
5	**И**	**Н**
6	**П**	**К**
8	**Л**	**И**
1	**Н**	**Ь**
11	**Д**	**О**
2	**В**	**И**
4	**В**	**И**
10	**Я**	**С**

Перестановка стовпців →

	1	2
1	**Н**	**Ь**
2	**В**	**И**
3	**В**	**О**
4	**В**	**И**
5	**И**	**Н**
6	**П**	**К**
7	**Р**	**П**
8	**Л**	**И**
9	**Д**	**І**
10	**Я**	**С**
11	**Д**	**О**

Перестановка рядків

Шифр: НЬ ВИ ВО ВИ ИН ПК РП ЛИ ДІ ЯС ДО

Розшифровка 3го варіанту

Шифр: РОГЕ НИГЯ ТОРП ИРУБ НКАД ЯСАЛ ОЕНЯ

$k_{стовпців}$= 4321 $k_{рядків}$ =3152746

	1	2	3	4
1	**Р**	**О**	**Г**	**Е**
2	**Н**	**И**	**Г**	**Я**
3	**Т**	**О**	**Р**	**П**
4	**И**	**Р**	**У**	**Б**
5	**Н**	**К**	**А**	**Д**
6	**Я**	**С**	**А**	**Л**
7	**О**	**Е**	**Н**	**Я**

Готова табиця

	1	2	3	4
3	**Т**	**О**	**Р**	**П**
1	**Р**	**О**	**Г**	**Е**
5	**Н**	**К**	**А**	**Д**
2	**Н**	**И**	**Г**	**Я**
7	**О**	**Е**	**Н**	**Я**
4	**И**	**Р**	**У**	**Б**
6	**Я**	**С**	**А**	**Л**

Перестановка рядків

	4	3	2	1
3	**П**	**Р**	**О**	**Т**
1	**Е**	**Г**	**О**	**Р**
5	**Д**	**А**	**К**	**Н**
2	**Я**	**Г**	**И**	**Н**
7	**Я**	**Н**	**Е**	**О**
4	**Б**	**У**	**Р**	**И**
6	**Л**	**А**	**С**	**Я**

Перестановка стовпців

Розшифровка: ПРОТЕ ГОРДА КНЯГИНЯ НЕ ОБУРИЛАСЯ

Контрольні питання:

1. Шифр перестановки це метод симетричного шифрування, при якому символи відкритого тексту не замінюються іншими, а лише переставляються згідно з певним алгоритмом або ключем
2. Алгоритм перестановки використаний у практичній роботі:
    1. Порахувати кількість стовпців і строк за формулами
    2. Записати ключ і під ним цифри використовуючи натуральний порядок їх у алфавіті
    3. Записати фразу у таблицю використовуючи один зі способів
    4. Переставити стовпці по порядку зростання цифр ключа