



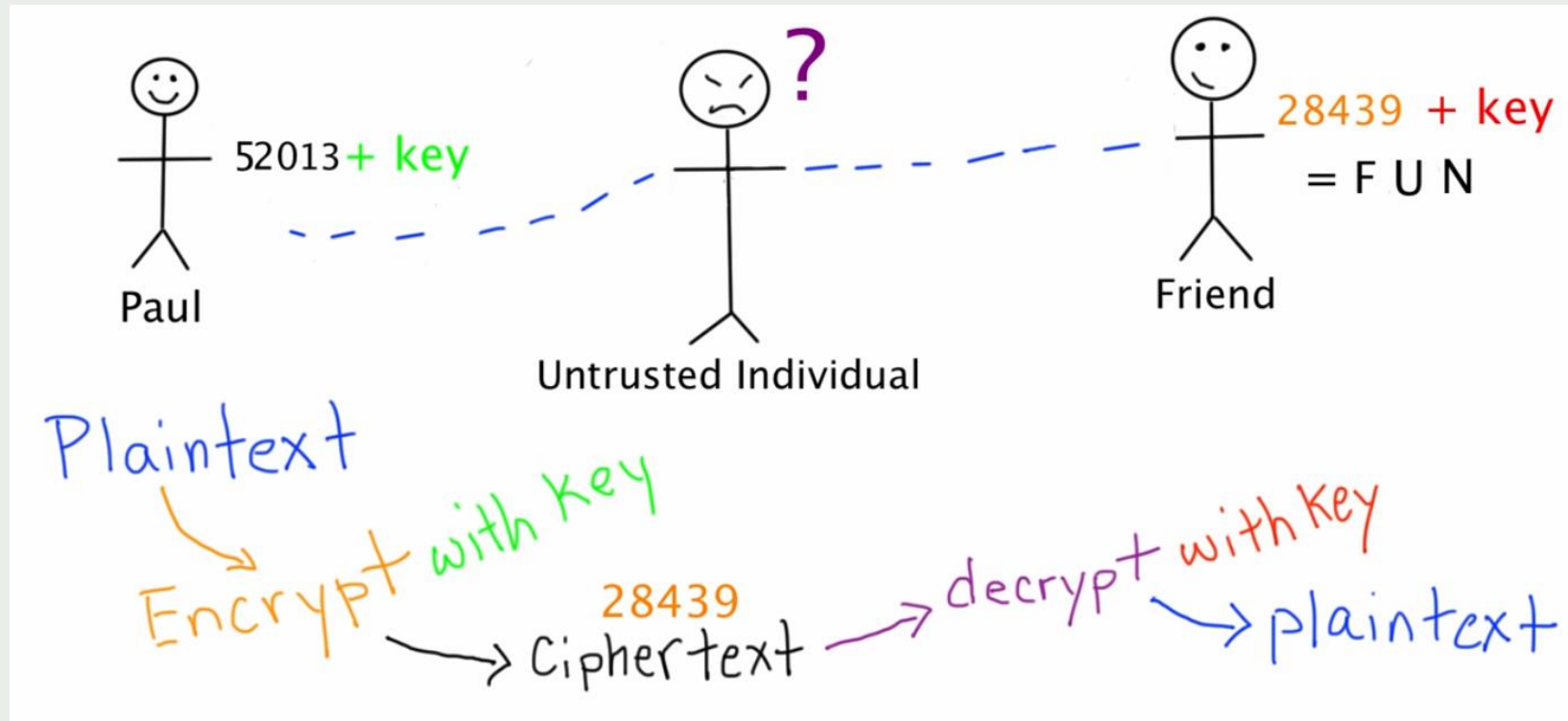
Комбінаторні множини в криптографічних алгоритмах шифрування

Хованова Маргарита



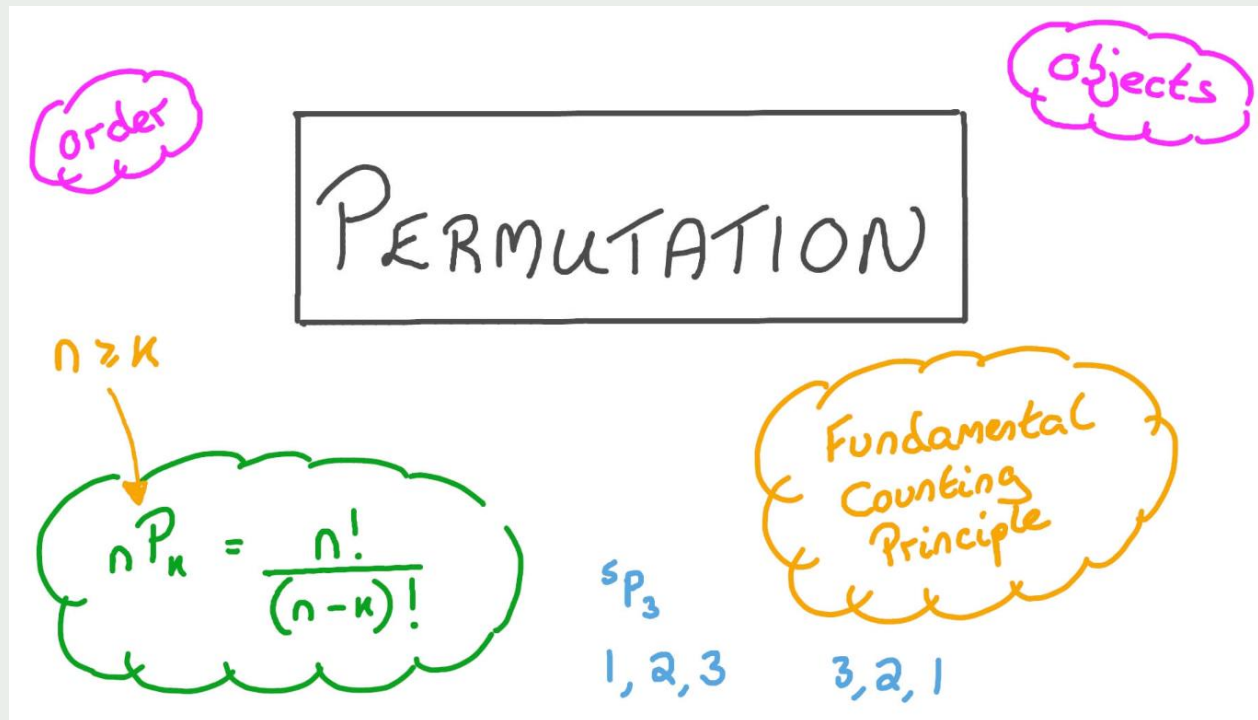
Вступ

- Криптографія – наука про математичні методи забезпечення конфіденційності



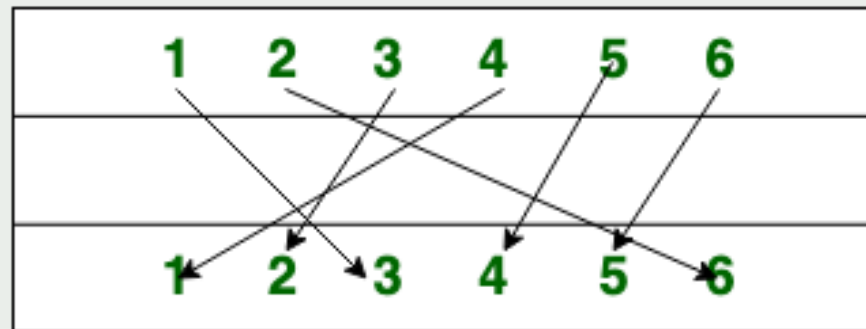
Перестановки...

... це один з безлічі математичних елементів, що використовує потужний математичний апарат криптографії



Класичні шифри перестановки

- Шифри перестановки – симетричні
- Суть: перестановка знаків за певними правилами
- Стійкість: розмір блоку, складність порядку перестановки



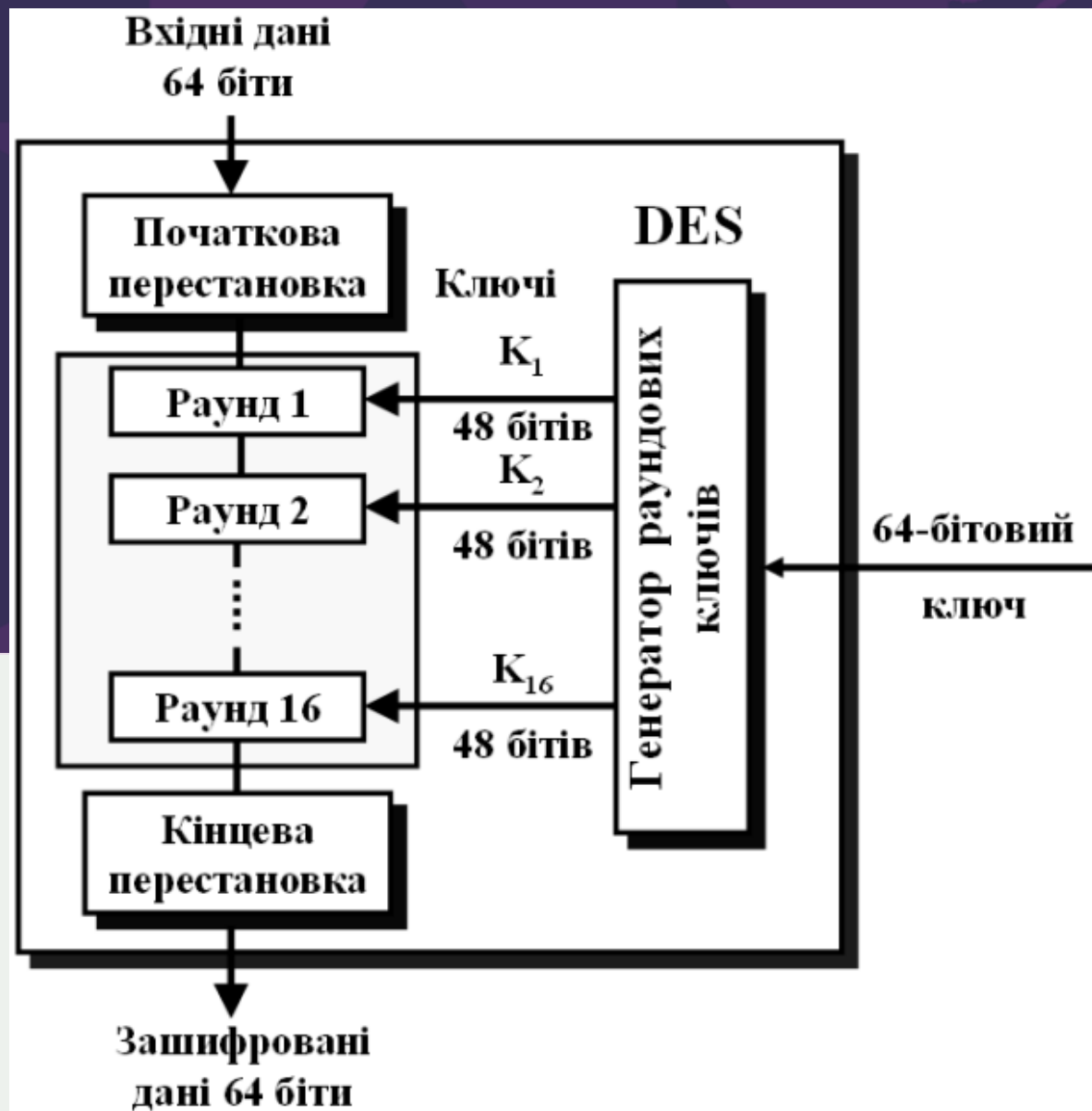
Приклади класичних шифрів перестановки

- Звичайна перестановка
- Звичайні рядково-стовпчикові табличні перестановки
- Рядково-стовпчикові табличні перестановки із застосуванням ключа стовпчиків
- Рядково-стовпчикові табличні перестановки з двома ключами
- Табличні перестановки з використанням трафарету

Сучасні системи шифрування

В чистому вигляді перестановки не використовуються, оскільки їх використання не надто посилює криптографічну стійкість алгоритму

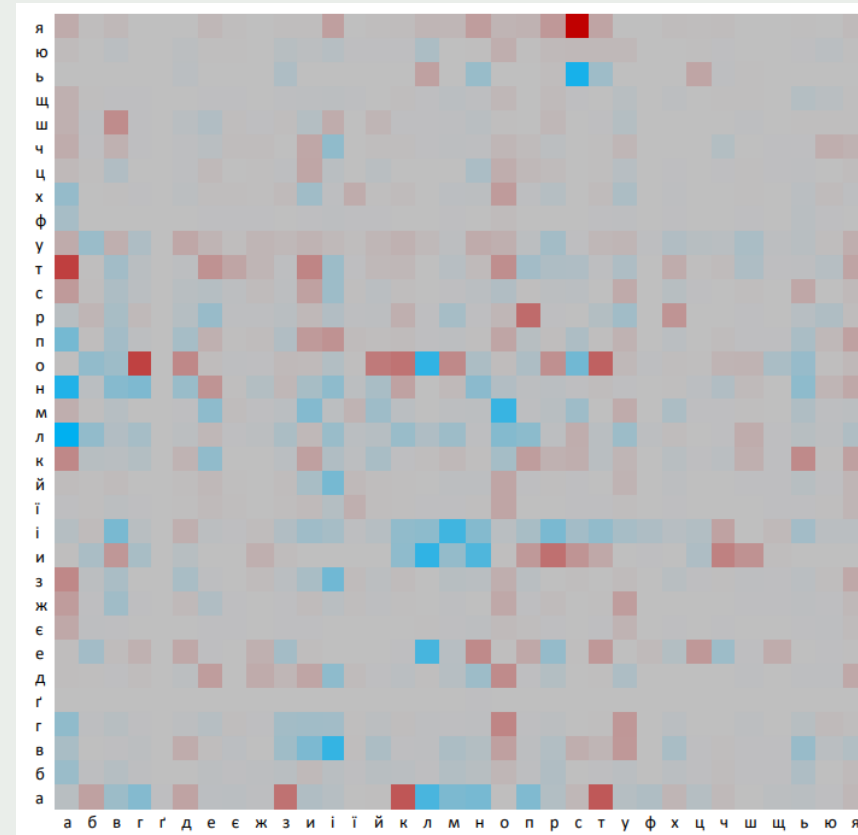
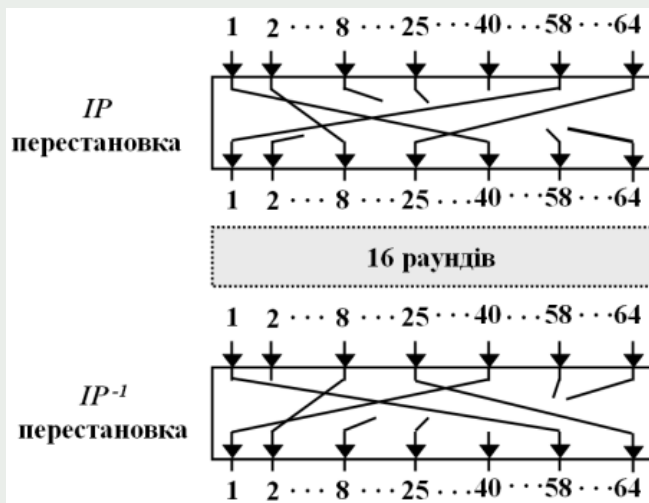




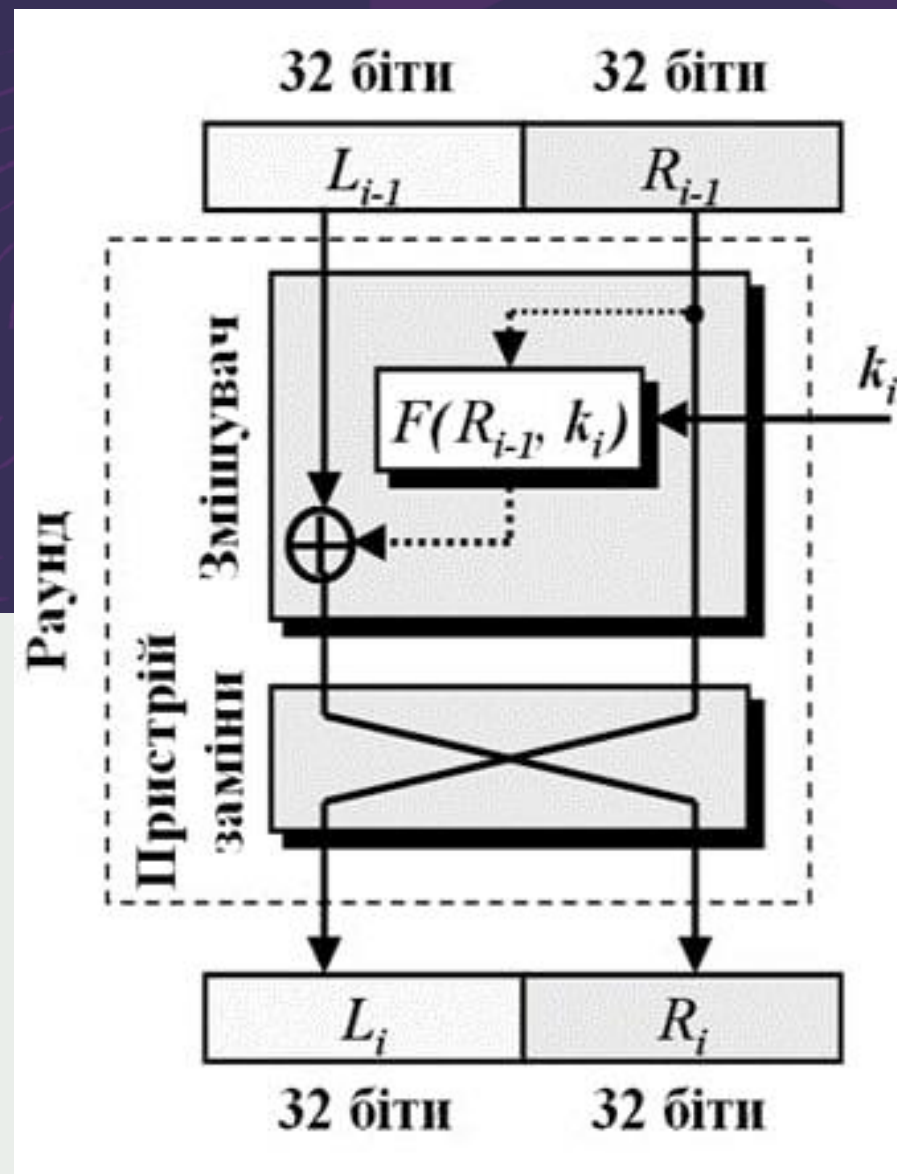
Алгоритм DES

Початкова та кінцева перестановки алгоритму DES

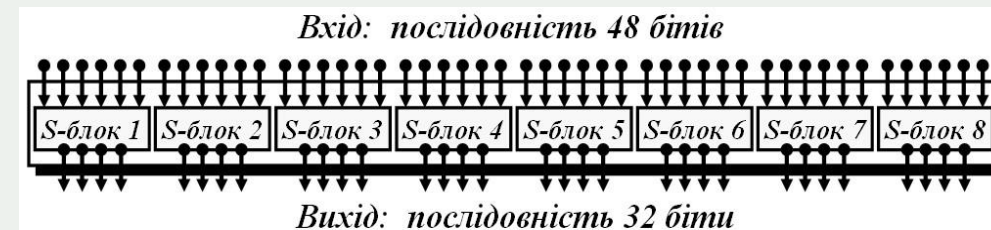
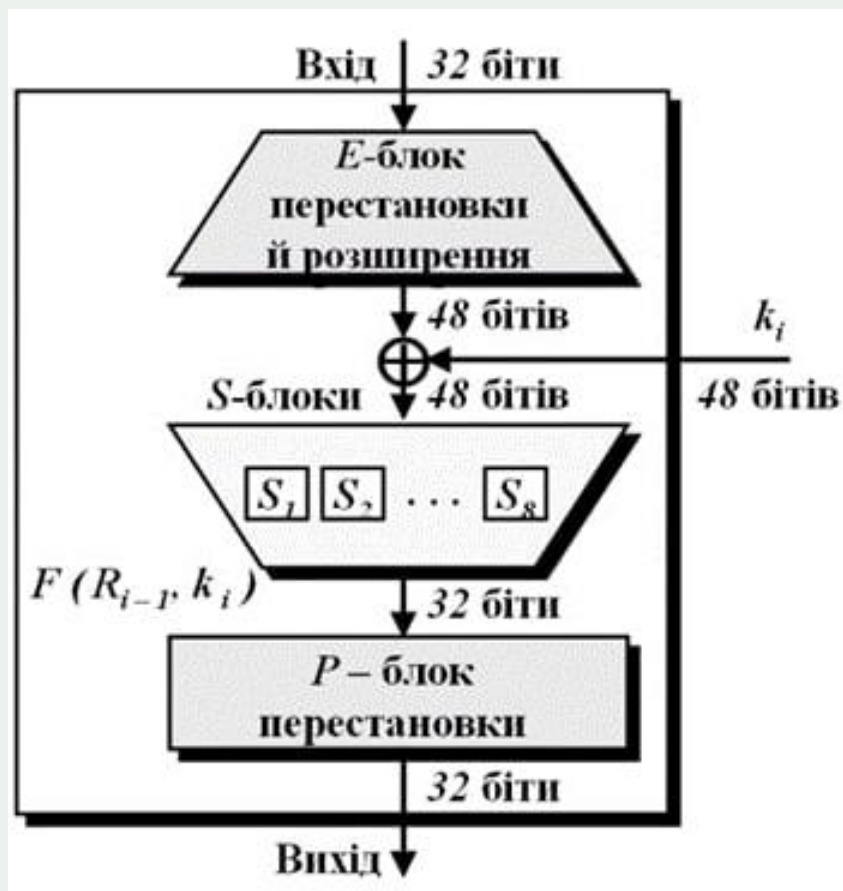
- Початкове розсіювання статистичної структури повідомлення
- При використанні початкової перестановки (Initial Permutation – IP) після завершення всіх раундів застосовується обернена перестановка IP^{-1}



Раунд шифрування в DES



Функція DES



пряма перестановка за таблицею, на вхід якій подаються 32 біти та отримуються 32 біти на виході

Практична реалізація



Шифр перестановки стовпців за ключем

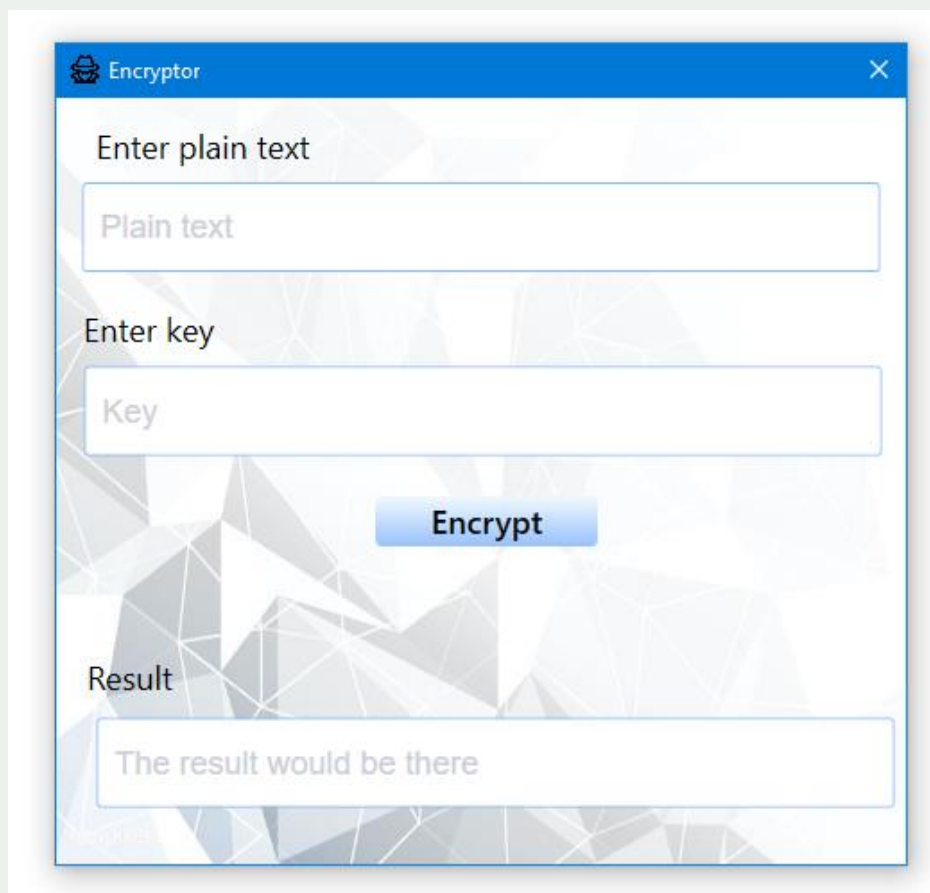
Row Column Transposition

Plaintext : "Kill Corona Virus at twelve am tomorrow"



clideo.com

Практична реалізація



The screenshot shows a window titled "Encryptor" with a blue header bar. Inside, there are three input fields and a button. The first field, labeled "Enter plain text", contains the placeholder text "Plain text". The second field, labeled "Enter key", contains the placeholder text "Key". Below these fields is a blue button labeled "Encrypt". At the bottom, there is a field labeled "Result" containing the placeholder text "The result would be there". The background of the window has a faint geometric pattern.

Encryptor

Enter plain text

Plain text

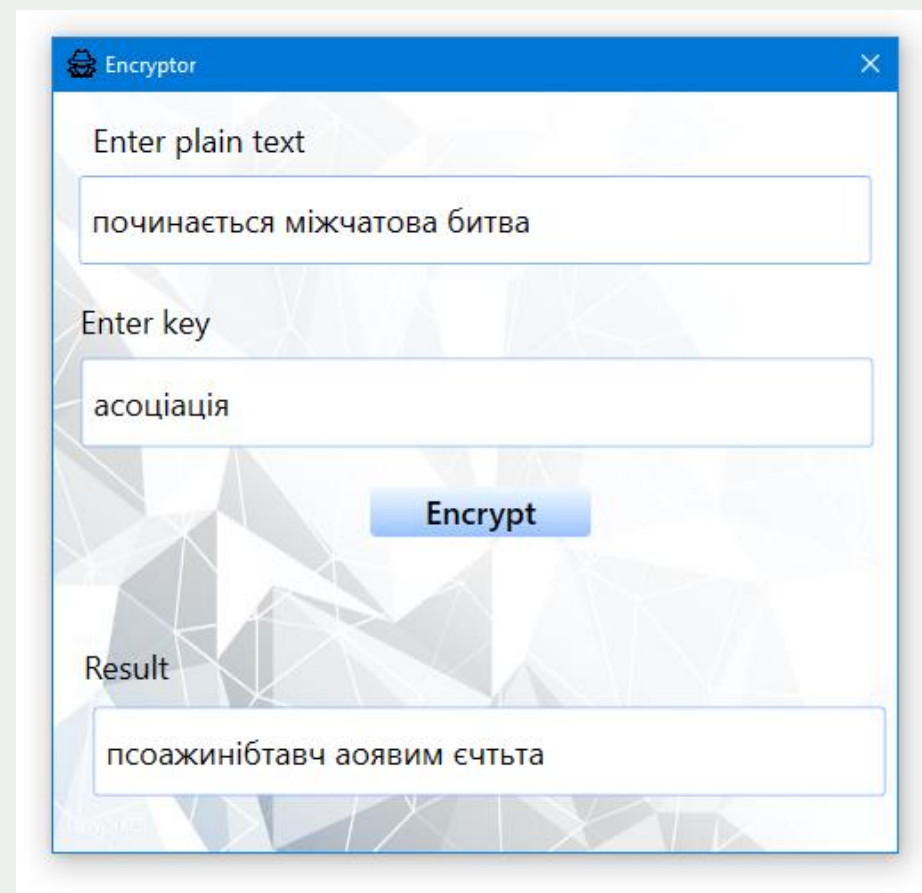
Enter key

Key

Encrypt

Result

The result would be there



This screenshot shows the same "Encryptor" window after an encryption operation. The "Enter plain text" field now contains the text "починається міжчатова битва". The "Enter key" field contains the text "асоціація". The "Result" field at the bottom now contains the encrypted text "псоажинібтавч аоявим єчтьта". The "Encrypt" button remains visible between the input fields.

Encryptor

Enter plain text

починається міжчатова битва

Enter key

асоціація

Encrypt

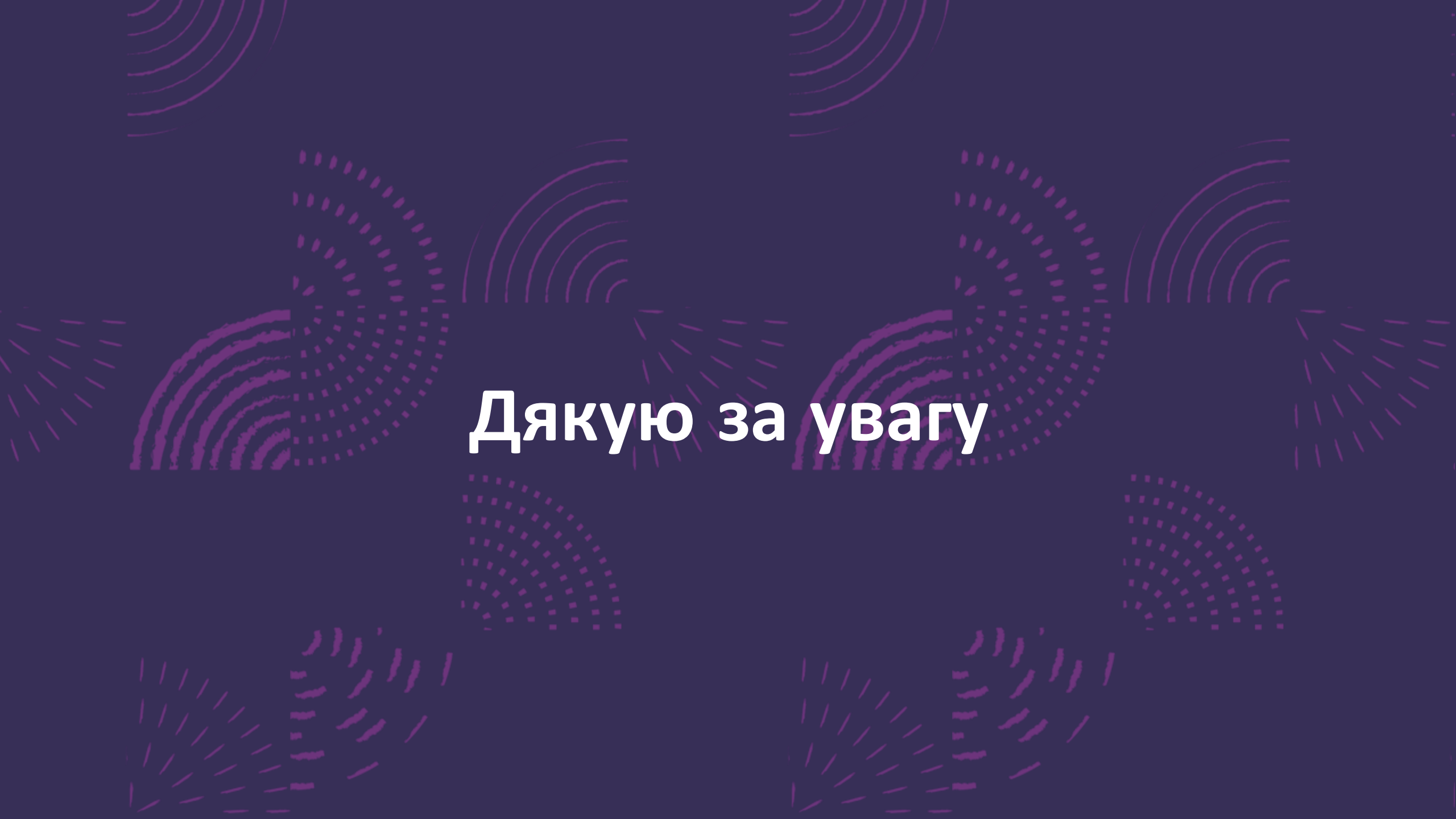
Result

псоажинібтавч аоявим єчтьта

Висновки

- Розглянуте використання комбінаторних множин
- Створено систему, яку можна використовувати для навчальних цілей та демонстрації класичних алгоритмів криптографії
- Основна мета застосування перестановок: полегшення апаратурної та програмної реалізації алгоритмів





Дякую за увагу