Практичне завдання:

**«S-блок та P-блок»**

**Мета практичного завдання:** опрацювати симетричне криптографічне перетворення на прикладі S-блоку та P-блоку, отримати практичний досвід з програмної реалізації цих перетворень або з створення інфографіки, що пояснює принципи роботи цих перетворень.

# 1 Теоретичні відомості

Симетричні криптографічні перетворення включають в себе використання S-блоку та P-блоку. S-блок використовується для заміни блоків даних з метою підвищення криптографічної стійкості і запобігання криптоаналізу. Він замінює вхідні значення на вихідні за певними правилами заміни. P-блок використовується для перемішування блоків даних з метою додаткового запобігання криптоаналізу і покращення розкиду даних. Він переставляє біти у визначений спосіб, що забезпечує нелінійність і дифузію даних. Використання S-блоку та P-блоку в симетричних криптографічних алгоритмах допомагає досягти ефективного шифрування з високим рівнем стійкості.

Алгоритм роботи S-блоку включає в себе заміну блоків даних згідно таблиці заміни, що визначається конкретним криптографічним алгоритмом. Кожному вхідному блоку відповідає вихідний блок, що встановлюється таблицею заміни. Цей процес забезпечує необоротну заміну значень, ускладнюючи зв'язок між вхідними і вихідними значеннями.

Зворотне перетворення S-блоку включає в себе обернену заміну значень згідно таблиці заміни. Тобто, замість використання вхідного блоку, таблиця заміни використовується для відновлення початкових значень. Цей процес є оберненим до заміни, яка була виконана на етапі шифрування або дешифрування.

Алгоритм роботи P-блоку включає в себе перестановку бітів вхідного блоку відповідно до заданої формули перестановки. Кожен біт вхідного блоку змінює свою позицію у вихідному блоку згідно з формулою перестановки. Цей процес перемішує біти вхідного блоку, утворюючи блок з переставленими бітами.

Зворотне перетворення P-блоку включає в себе обернену перестановку бітів вихідного блоку відповідно до формули перестановки. Замість перемішування блоку, формула перестановки застосовується для відновлення початкових позицій бітів в блоці. Цей процес є оберненим до перестановки, яка була виконана на етапі шифрування.

2 Хід роботи

Для виконання практичного завдання вам треба дослідити алгоритми криптографічних перетворень з S-блоком і P-блоком. Розібратися з відповідними деталями прямого та зворотного перетворення, що використовуються під час зашифрування та розшифрування в сучасних блокових симетричних шифрах. Визначитися з варіантом виконання практичного завдання, які наведені в наступній таблиці.

Варіанти виконання практичного завдання:

| Варіант | Стисле формулювання задачі | Формат відповіді | Максимальна кількість балів |
| --- | --- | --- | --- |
| 1 | Створення власної інфографіки у супроводі з текстовим розʼясненням щодо алгоритмів S-блоку та P-блоку (пряме та зворотне перетворення) | Google Document | 10 |
| 2 | Власна програмна реалізація алгоритмів S-блоку та P-блоку (пряме та зворотне перетворення) | GitHub repository | 10 |

Для обох варіантів завдання вимоги до S-блоку наступні:

* розмір вхідних даних 8 бітів
* розмір вихідних даних 8 бітів
* вхідний блок даних розбивається на дві тетради по 4 біти

Для обох варіантів завдання вимоги до P-блоку наступні:

* розмір вхідних даних 8 бітів
* розмір вихідних даних 8 бітів

## 2.1 Створення власної інфографіки

Створіть власну інфографіку, що з використанням ваших малюнків, схем та тексту покроково пояснює алгоритм S-блоку та P-блоку. Пояснення кожного алгоритму має складатись з прямого та зворотного перетворень. Для S-блоку алгоритмом зворотного перетворення може бути той самий алгоритм, але з застосуванням зворотної таблиці констант. Порядок обчислення зворотної таблиці констант також має бути розтлумачений інфографікою.

Головною метою цього варіанту завдання є створення документу з рисунками та текстовими коментарями до того, що зображено на цих рисунках. Інструменти для створення графіки оберіть на власний розсуд. Текст на рисунках і графічних елементах краще писати англійською мовою.

Результати своєї роботи треба оформити в Google Document. Посилання на документ з доступом на читання відправити у відповідь на це практичне завдання у Classroom.

## 2.2 Власна програмна реалізація

Реалізуйте свої власні функції для прямого і зворотного перетворення за алгоритмом S-блоку, а також за алгоритмом P-блоку. Мову програмування для реалізації оберіть на власний розсуд. Таблицю констант для реалізації S-блоку оберіть з рекомендованих, що доступні публічно або сгенеруйте самостійно. Формулу перестановки для реалізації P-блоку оберіть на власний розсуд.

Для S-блоку алгоритмом зворотного перетворення може бути той самий алгоритм, але з застосуванням функції обчислення зворотної таблиці констант. Фактично така функція має приймати таблицю констант для прямого перетворення і повертати таблицю констано для зворотного перетворення.

Важливо написати тести для власної реалізації алгоритмів S-блоку та P-блоку, з метою переконатися в правильності функціонування. Для певного набору даних, якщо виконати послідовно пряме та зворотне перетворення, то маємо отримати початковий набір даних.

Ваш репозиторій на GitHub має містити файли з прокоментованим вихідним кодом та README.md файл з описом завдання, інструкцією щодо запуска коду, приклад визову програми, приклад результату виконання програми. За потреби можете додати перелік залежностей вашої програми та зразки скріншотів.