**Алгоритм RC4** лаб2 крипто

Алгоритм RC4 (Rivest Cipher 4) - це симетричний потоковий шифр, використовується для шифрування та розшифрування даних із застосуванням одного ключа, має дуже просту структуру.

Основна ідея роботи алгоритму RC4 полягає у генерації псевдовипадкової послідовності байтів (потоку ключів), яка потім використовується для змішування з вхідними даними (або їх бітами) за допомогою операції XOR. Ключом для генерації цієї послідовності є секретний ключ, який обмінюється між відправником і отримувачем повідомлення.

Оскільки алгоритм RC4 є потоковим шифром, він підходить для шифрування великих об'ємів даних без додаткових зусиль зі зберіганням великих ключів чи ініціалізацією. Однак з технічної точки зору, він має певні слабкі сторони, особливо коли використовується для довгих повідомлень без регенерації ключа.

Основні кроки роботи алгоритму RC4:

* **Ініціалізація стану S-Box**: Алгоритм починається з ініціалізації S-Box - це масив з 256 байтів, який містить послідовність чисел від 0 до 255.
* **Перетворення ключа в початковий стан S-Box**: Ключ, який використовується для шифрування або дешифрування, використовується для перестановки S-Box. Це виконується за допомогою алгоритму Key Scheduling Algorithm (KSA).
* **Генерація потоку ключів**: Після ініціалізації S-Box використовується алгоритм Pseudo-Random Generation Algorithm (PRGA) для генерації потоку псевдовипадкових байтів, який буде використовуватися для змішування з вхідними даними.
* **Змішування з даними**: Потік ключів, згенерований PRGA, використовується для змішування з вхідними даними (або їх бітами) за допомогою операції XOR. Це забезпечує шифрування або дешифрування даних.
* **Вивід результату**: Зашифровані або розшифровані дані виводяться як результат роботи алгоритму.

**Опис програми**:

1. **KSA (Key Scheduling Algorithm)**: Ця функція виконує початкову ініціалізацію стану перестановок (S-box) на основі ключа.
2. **PRGA (Pseudo-Random Generation Algorithm)**: Ця функція генерує псевдовипадкову послідовність, яка буде використовуватися для змішування з вхідними даними для шифрування або дешифрування.
3. **RC4**: Ця функція об'єднує KSA та PRGA для створення RC4-потоку.
4. **encrypt**: Ця функція використовує RC4 для шифрування вхідного повідомлення за допомогою вказаного ключа.
5. **decrypt**: Ця функція використовує ту саму логіку шифрування для дешифрування зашифрованого тексту.