Cryptography in decentralized systems

Practice 3

“Дослідження S-блоку та P-блоку”

1. **Дослідження S-блоку**

S-блок (блок підстановки) є одним з компонентів алгоритмів симетричних криптографічних перетворень, головний принцип якого полягає у заміні блоків даних відповідно до значень таблиць заміни. У блочних шифрах він зазвичай використовуються для приховування зв’язку між ключем і зашифрованим текстом — властивість Шеннона.

S-блок приймає деяку кількість вхідних бітів, m, і перетворює їх у деяку кількість вихідних бітів, n (4/6/8): S-блок m×n може бути реалізований як таблиця пошуку з 2m слів по n бітів кожне. Зазвичай у вигляді S-блоку використовуються фіксовані таблиці, як у стандарті шифрування даних (DES), але в деяких шифрах таблиці можуть генеруватися динамічно (випадково) або генеруватися на основі ключа.

Властивості S-блоку:

1. Нелінійність - функція S-блоку полягає в тому, щоб внести властивості нелінійності в алгоритм шифрування.

2. Високий алгебраїчний ступінь (AD) — це властивість безпечного S-блоку, де чим вищий алгебраїчний ступінь, тим кращий S-блок. Чим вищий ступінь функції, тим більша складність її обчислення та можливість протистояти атаці наближення.

3. Диференціальна рівномірність - таблиця S-box надає безпеку блокового шифру від диференціального криптоаналізу.

4. Повнота - функція повна тоді і тільки тоді, коли кожен вихідний біт залежить від усіх вхідних бітів. Таким чином, якщо можливо знайти вихідний біт найпростішого булевого виразу через вхідні біти, кожен із цих виразів повинен містити всі вхідні біти, якщо функція завершена.

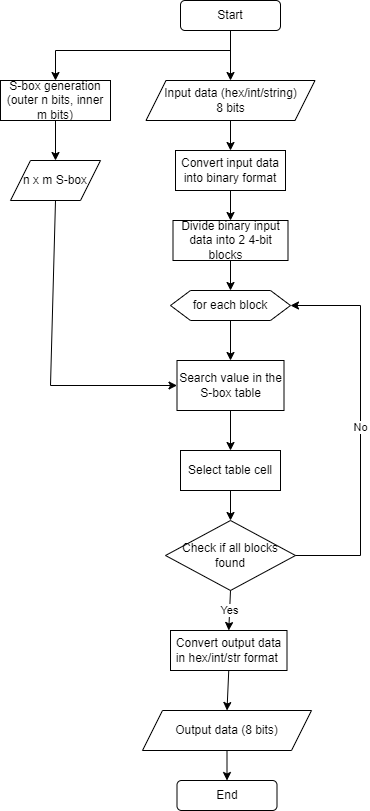
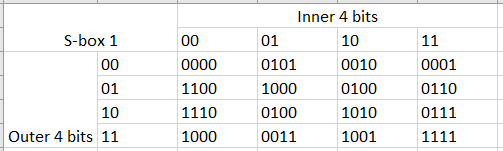


Рисунок 1 - Блок схема алгоритму прямого та зворотного симетричного криптографічного перетворення з використанням S-блоку

Пояснення алгоритму прямого симетричного криптографічного перетворення з використанням S-блоку на прикладі числа 200 десяткової системи числення. Для обчислень значень підстановки буде використано власну згенеровану таблицю S-блоку заміни S1 4х4 - 4 біти на вхід та 4 біти на вихід (по 2 біти на рядок та стовпець та 4 біти на комірку).

Таблиця 1 - S-блок заміни S1



Крок 1:

Конвертуємо число 200 з десяткової системи числення у двійкову систему (бітову):

200 -> 11001000

Крок 2:

Розбиваємо вхідний блок даних на дві тетради по чотири біти:

11001000 -> [1100, 1000]

Крок 3:

Виконуємо пошук значення за першою тетрадою у таблиці підстановки. За рядки відповідають перші два біта, за стовпці - наступні два. Відповідно на перетині значень 11 та 00 отримаємо значення: 1000.

Виконуємо пошук за другою тетрадою. Відповідно на перетині значень 10 та 00 отримаємо значення: 1110.

Крок 4:

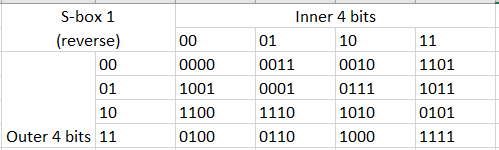
Поєднуємо отримані значення у один вихідний блок: 10001110

Конвертуємо вихідний блок даних 8 бітів у шістнадцяткову систему числення:

10001110 -> 8E

Алгоритм зворотного перетворення включає в себе обернену заміну значення 8Е згідно оберненої таблиці заміни S1 (reverse):

Таблиця 2 - Обернений S-блок заміни S1



Для створення оберненої таблиці необхідно значення комірки розділити по 2 біти, які будуть відповідати за рядки та стовпці, а вихідні значення рядка та стовпця об’єднати у 4 біти та розташувати у комірку.

Приклад: значення таблиці S1 [10, 00]->1110 у оберненій таблиці буде наступне: [11, 10] -> 1000.

Крок 1:  
 Конвертуємо шифр з шістнадцяткової системи у двійкову:

8Е -> 10001110

Крок 2:  
 Розбиваємо отримане значення на 2 тетради по 4 біти:  
 10001110 -> [1000, 1110]

Крок 3:

Для першої тетради шукаємо значення з оберненої таблиці заміни на перетині бітів 10 та 00: 1100

Для другої тетради шукаємо значення з оберненої таблиці заміни на перетині бітів 11 та 10: 1000

Крок 4:

Поєднуємо отримані значення у бітовий рядок: 1100 + 1000 = 11001000

Конвертуємо вихідний блок у десяткову систему числення:

11001000 -> 200

Отже, в результаті прямого симетричного криптографічного перетворення з використанням алгоритму S-блоку на прикладі числа 200 було отримано шифр 8E. В результаті зворотного перетворення з 8E було отримано 200.

Звичайно, як варіант для різних тетрад можна використовувати різні таблиці S-блоків, змінювати порядок значень бітів на вході (наприклад щоб за рядки відповідали не перші два біта, а 1 та 3 біти), тощо.

S-блоки використовуються в наступних шифрах:

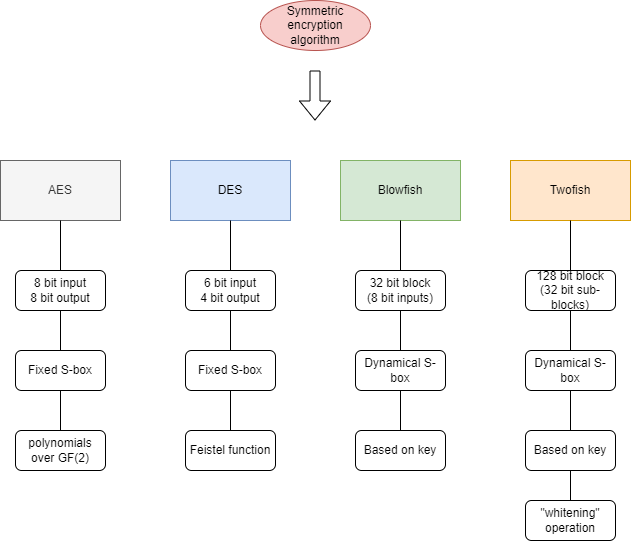


Рисунок 2 - Варіанти застосування S-блоків

Наразі S-блоки використовуються в наступних шифрах:

1. AES - Advanced Encryption Standard

2. DES - Data Encryption Standard

3. Blowfish

4. Twofish

Отже, блоки заміни мають сильні криптографічними можливості та широко використовуються для забезпечення властивості нелінійності в блокових шифрах. Це суттєво важливо для стійкості до стандартної атаки, у тому числі лінійного і диференціального криптоаналізу. Криптографічна стійкість S-блоку залежить від техніки та способів його побудови.

1. **Дослідження P-блоку**

P-блок (блок перестановки) є одним з компонентів алгоритмів симетричних криптографічних перетворень, головний принцип якого полягає у перестановці бітів вхідного блоку відповідно до заданої формули перестановки. В загалом визначається метод перестановки бітів, який використовується для перестановки або транспонування бітів між входами S-блоків, зберігаючи дифузію під час транспонування.

Основна мета блоку перестановок полягає в тому, щоб внести плутанину та дифузію в дані, при цьому підвищуючи безпеку шифру. Переставляючи біти нелінійним чином, це допомагає усунути шаблони або кореляції, які можуть існувати у вихідних даних.

У блокових шифрах S-блоки та P-блоки використовуються, щоб зробити зв'язок між відкритим текстом і зашифрованим текстом складним для розуміння.

P-блок працює з блоком даних фіксованого розміру та переставляє біти на основі визначеної формули перестановки. Відповідно сама формула буде являтися ключем для подібного симетричного криптографічного перетворення. Розмір таблиці перестановок залежить від розміру блоку шифру.

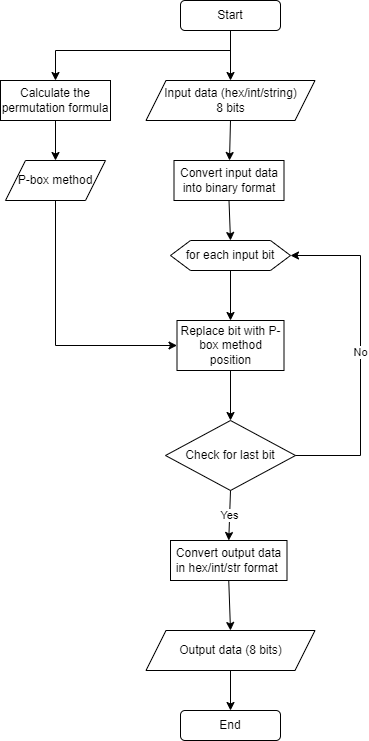
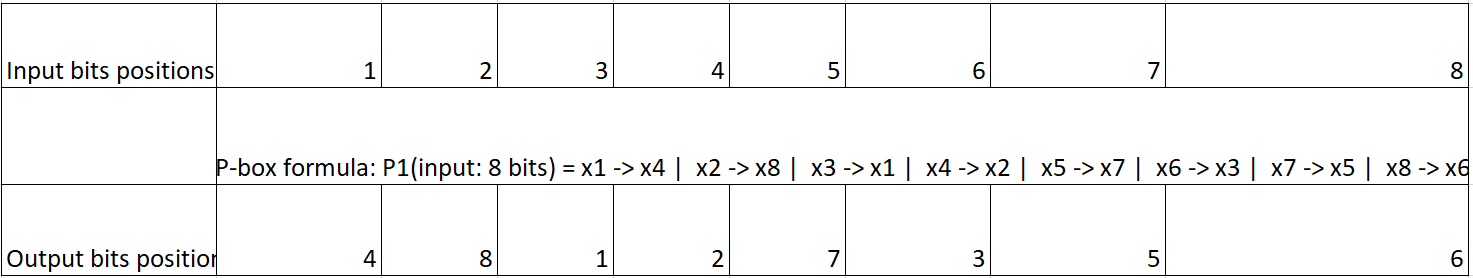


Рисунок 3 - Блок схема алгоритму прямого та зворотного симетричного криптографічного перетворення з використанням S-блоку

Пояснення алгоритму прямого симетричного криптографічного перетворення з використанням P-блоку на прикладі числа 200 десяткової системи числення. Для обчислень значень підстановки буде використано власну згенеровану формулу P-блоку P1, яка приймає на вхід 8 бітів та повертає вихідні дані у розмірі 8 бітів.

Таблиця 3 - P1-блок перестановки для прямого перетворення



Крок 1:

Конвертуємо число 200 з десяткової системи числення у двійкову систему (бітову):

200 -> 11001000

Крок 2:

Для кожного вхідного біта робимо транспонування відповідно до формули перестановки та ставимо на позицію відповідно до P1-блоку.

Для першого біта (1) замість позиції 1 ставимо на позицію 4. Таку операцію робимо з кожним бітом вхідних даних.

Крок 3:

Поєднуємо отримані значення бітів за новими позиціями у один вихідний блок: 00010011

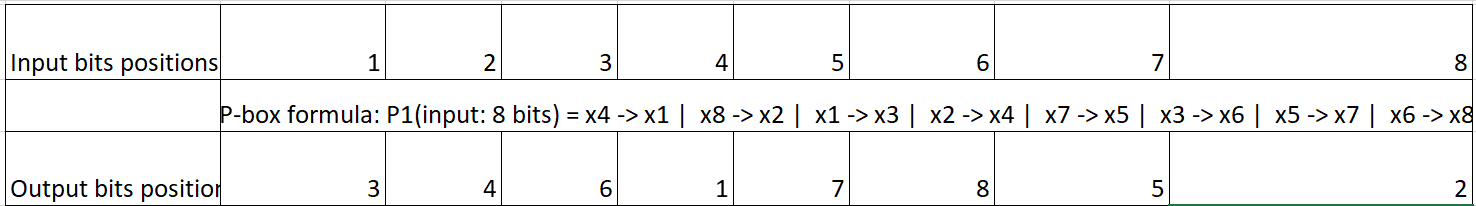
Крок 4:

Конвертуємо вихідний блок даних 8 бітів у шістнадцяткову систему числення:

00010011-> 13

Процес перестановки для P-блоку може бути зворотнім, тобто існує відповідна зворотна перестановка, яку можна застосувати для відновлення вихідних даних. 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. Це дозволяє здійснювати дешифрування (зворотні перетворення) в криптографічних алгоритмах.

Таблиця 4 - P2-блок перестановки для зворотного перетворення



Формулу перестановки для оберненого перетворення було зроблено шляхом заміни позицій для вхідних та вихідних бітів відповідно (тепер перший біт вхідних даних має бути третім у вихідному блоці, тощо).

Крок 1:

Конвертуємо шифр 13 у бітовий рядок:

13 -> 00010011

Крок 2:

Для кожного вхідного біта робимо транспонування відповідно до формули перестановки та ставимо на позицію відповідно до P2-блоку.

Для першого біта (1) замість позиції 1 ставимо на позицію 3. Таку операцію робимо з кожним бітом вхідних даних.

Крок 3:

Поєднуємо отримані значення бітів за новими позиціями у один вихідний блок: 11001000

Крок 4:

Конвертуємо вихідний блок даних 8 бітів у десяткову систему числення:

11001000 -> 200

Отже, в результаті прямого симетричного криптографічного перетворення з використанням алгоритму P-блоку на прикладі числа 200 було отримано шифр 13. В результаті зворотного перетворення з 13 було отримано 200.

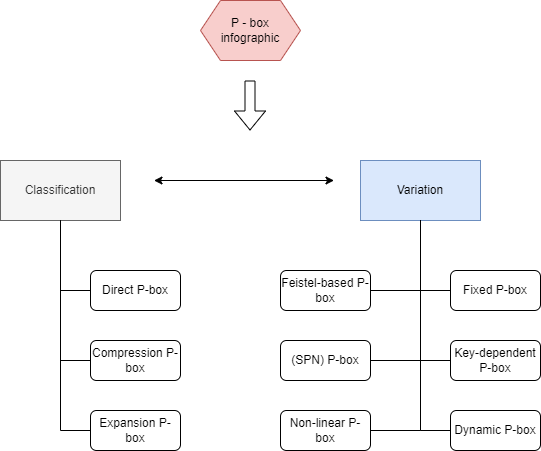


Рисунок 4 - Інфографіка P-блоків перестановки

P-блоки зазвичай класифікуються за стисненням, розширенням та можуть бути прямі залежно від того, чи кількість вихідних бітів менше/більше або дорівнює кількості вхідних бітів відповідно. Тільки прямі P-блоки є інверсними (зворотніми).

Отже, блок перестановки відіграє важливу роль у забезпеченні властивостей нелінійності та дифузії блокових шифрів, сприяючи їх стійкості проти різних криптографічних атак. Ретельний вибір формули перестановки забезпечує збалансоване та безпечне транспонування даних.