**Белорусский национальный технический университет**

**Кафедра «Программное обеспечение информационных систем и технологий»**

**Дисциплина «Основы информационной безопасности»**

**Лабораторная работа №3**

Выполнил: студент гр. 10702122 Тимощенко Н.В

Проверила Белова С.В.

Минск 2024

**Лабораторная работа 3**

**Цель работы:**

Познакомиться с основами симметричного шифрования. Изучить алгоритм шифрования DES на примере упрощенной версии S-DES**.**

**Задание:**

632 b

**Решение:**

632 = 1001111000

P10 = 0101101001

LS1 K1 = 1011010010

P8 = 11010001

LS2 K2 = 1101001010

P8 = 00110001

b = ‘98’ = 0110|0010

IP = 10100001; L1 = 1010, R1 = 0001

IP(^-1) = 00101100; L2 = 0010, R2 = 1100

E(P(R)) = 00010100

XOR(E(P,K1))= 0010100/11010010 = 0010|0101

S(L)[00;01] = [0,0] = 00

S(R)[01;01] = [1;1] = 01

-> 0001

P4 = 2431 = 0100

XOR(L,P4) = 0010/1010 = 0010

SW = 0001|0010

(E/R;R) = 00010100

S(L)[00;01] = [0;1] = 00

S(R)[01;01] = [1;1] = 01

-> 0001

P4 = 0100

XOR(L, P4) = 0100/0001 = 0101

L,R = 01010010

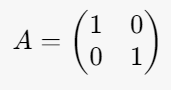
IP(^-1)() = 10001100

**Контрольные вопросы:**

1. Какие преобразования называются несингулярными? Приведите пример сингулярного и несингулярного преобразований.

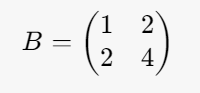
Несингулярные преобразования — это такие преобразования, которые сохраняют уникальность входных данных, т.е. каждое уникальное входное значение соответствует уникальному выходному значению. В криптографии это означает, что преобразование можно обратить, и исходные данные могут быть восстановлены.

**Пример**:  
Рассмотрим простое линейное преобразование, заданное матрицей:



Это единичная матрица, которая — несингулярная, поскольку ее определитель равен 1 (не равен нулю). Такое преобразование можно легко обратить, что делает его подходящим для шифрования, так как можно восстановить исходные данные.

Пример с сингулярным преобразованием: Рассмотрим матрицу:



Определитель этой матрицы равен 0. Эта матрица является сингулярной, и преобразование, заданное этой матрицей, не может быть обращено. Это означает, что исходные данные не могут быть восстановлены из зашифрованного текста, что делает его неподходящим для надежного шифрования.

2. Какова структура сети Файстеля?

Сеть Файстеля (Feistel network) — это структура, используемая в криптографии для создания симметричных блочных шифров. Она названа в честь криптографа Хорста Файстеля, который предложил эту концепцию. Основная идея сети Файстеля заключается в том, чтобы разбивать блок данных на две части и многократно применять преобразования к одной из частей с использованием ключа.

1. Какая сеть Файстеля называется классической? Гомогенной?

**Классическая сеть Файстеля** — это базовая версия структуры сети, которая была предложена Хорстом Файстелем. В классической сети:

* Блок данных разбивается на две равные части (L и R).
* В каждом раунде используется функция F, которая зависит от одной из половин блока и ключа раунда.
* Процесс включает несколько раундов, после чего левый и правый блоки могут быть объединены для получения зашифрованного текста.

Классические сети Файстеля используются в таких шифрах, как **DES (Data Encryption Standard).**

**Гомогенная сеть Файстеля** — это разновидность сети, в которой функция F применима к одной и той же структуре данных в каждом раунде. В гомогенной сети:

* Функция F может быть одной и той же для всех раундов, и ключи могут изменяться, но структура самой функции остается неизменной.
* Это позволяет сделать структуру более простой и понятной.

Гомогенные сети Файстеля обеспечивают гибкость при шифровании и могут быть адаптированы для различных уровней безопасности.

1. Как выполняется расшифрование в сетях Файстеля?

Расшифрование в сетях Файстеля выполняется с использованием той же структуры, что и шифрование, но с некоторыми изменениями в порядке применения ключей. Это обеспечивает обратимость процесса шифрования. Вот как это происходит:

### Основные шаги расшифрования в сетях Файстеля

**1.Инициализация**:

Зашифрованный блок данных представлен как **C = (L(n), R(n))**, где L(n) и R(n) — это левый и правый блоки зашифрованного текста.

**2.Ключи**:

Ключи для расшифрования используются в обратном порядке по сравнению с шифрованием. Если шифрование использовало ключи K1, K2, ..., Kn, то расшифрование будет использовать их в порядке Kn, K(n-1), ..., K1.

**3.Процесс расшифрования**:

Для каждого раунда i от n до 1 выполняются следующие шаги:

**R(i-1) = L(i)** (правый блок из предыдущего раунда становится левым блоком текущего раунда).

**L(i-1) = R(i) ⊕ F(L(i), K(i))** (левый блок текущего раунда вычисляется путем применения функции F к правому блоку и ключу).

**4.Финальный вывод**:

После завершения всех раундов, выходные данные комбинируются: **P = (L(0), R(0))**, где P — это расшифрованный текст.

5. От чего зависит криптоаналитическая стойкость шифра Файстеля?

6. Классифицируйте алгоритм DES. Является ли он сетью Файстеля? Почему?

7. Проведите сравнение алгоритмов DES и S-DES по основным параметрам (длина ключа, длина блока шифрования, количество раундов, количество подключей, размер и количество S-блоков).

8. Являются ли криптостойким алгоритм DES? Можно ли его применять на практике? Обоснуйте ответ.

9. Какие типы операций используются в большинстве современных блочных алгоритмах симметричного шифрования?