Министерство образования Республики Беларусь Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Факультет информационных технологий и управления

Кафедра интеллектуальных информационных технологий

**Факультет: ФИТУ**

**Специальность: ИИ**

**Отчет по лабораторной работе №2 по курсу «СИМОИБ»**

Выполнил студент Ахроров М. Д. группы 921731

Проверил Захаров В. В.

.

Минск 2021

**Лабораторная работа № 2.**

# Режимы применения блочных шифров

**3.1. Теоретические сведения**

**DES – Data Encryption Standard.** Первым официальным стандартом симметричного блочного шифра, принятым правительством США в 1977 году, стал алгоритм DES.

Размер блока равен 64 битам, размер ключа 64 бита, из них собственно ключом, используемым для шифрования, являются только 56 бит, а оставшиеся восемь бит используются для проверки целостности ключа методом контроля четности. Архитектура шифра – классическая сеть Фейстеля.

Алгоритм зашифрования DES включает в себя начальную перестановку, 16 раундов шифрования (циклов преобразования Фейстеля) и конечную перестановку.

**AES – Advanced Encryption Standard.** AES – стандарт шифрования, основанный на алгоритме Rijndael, разработанном двумя бельгийскими криптографами разработанного двумя Бельгийскими криптографами Винсентом Рейменом и Джоаном Дейменом.

Алгоритм Rijndael представляет собой итеративный блочный шифр с возможностью выбора длины блока и длины ключа 128, 192 или 256 бит. Для стандарта AES длина блока только 128 бит, а длина ключа 128, 192 или 256 бит.

Архитектура алгоритма называется square – квадрат. Название алгоритма связано с тем, что блок данных (Block) представляется в виде прямоугольного массива из четырех строк и Nb столбцов. Операции производятся над отдельными байтами и над независимыми строками и столбцами.

Операция SubBytes выполняет табличную замену байтов массива. Каждый байт в State заменяют соответствующим элементом в фиксированной 8-битной таблице поиска, S; .

Операция ShiftRows выполняет циклический сдвиг влево строк массива. Причем каждая строка сдвигается на свое количество байт. Нулевая строка сдвигается на 0 байт, первая на 1 байт, вторая на 2 и третья на 3 байта.

Операция MixColumns выполняет умножение по модулю каждого столбца на физический полином :

.

Вместе с ShiftRows, MixColumns вносит диффузию в шифр.

Операция AddRoundKey выполняет добавление к массиву данных материала ключа. Для этого выполняют побитовую операцию XOR (сложение по модулю 2) каждого байта State с каждым битом RoundKey.

В последнем раунде, в отличие от предыдущих, не выполняют операцию MixColumns.

Ключи шифрования раундов RoundKeys получают из CipherKey использованием процедуры KeyExpansion. Алгоритму шифрования требуется Nr+1 наборов по Nb слов ключа. Один набор требуется перед первым раундом шифрования и по одному набору на каждом из Nr раундов шифрования. Полученный массив обозначается как .

В 2003 году Агентство национальной безопасности США признало шифр AES достаточно надежным для защиты сведений, составляющих государственную тайну (classified information). Для защиты информации до уровня SECRET включительно разрешено использовать ключи длиной 128 бит, а для уровня TOP SECRET – ключи длиной 192 и 256 бит.

Все блочные шифры обладают одним неприятным для защищающих свою информацию свойством, а именно – при зашифровании одинаковых блоков исходного текста получают одинаковые блоки криптотекста, поэтому существует потенциальная возможность утечки информации о повторяющихся блоках данных, шифруемых на одинаковом ключе. Этот факт в некоторых случаях может привести к получению существенной информации о содержании исходного текста при наблюдении криптограммы без ее расшифрования.

Для устранения этой проблемы используют различные режимы шифрования.

**Режимы шифрования.** Режимом шифрования называют способ применения алгоритма блочного шифра для преобразования последовательности блоков исходного текста в последовательность блоков шифртекста.

– **ECB** (Electronic Code Book) – режим электронной кодовой книги, или режим простой замены;

– **CBC** (Cipher Block Changing) – режим сцепления блоков шифра;

– **CTR** (Counter Mode) – режим счетчика.

– **ECB** (Electronic Code Book) – режим электронной кодовой книги, или режим простой замены. Зашифрование/расшифрование i-го блока исходного текста/шифртекста выполняется независимо от остальных блоков:

Недостатком режима ECB является то, что одинаковые блоки исходного текста преобразуются в одинаковые блоки шифротекста при использовании одинакового ключа.

Достоинства режима ECB:

– простота реализации;

– возможность распараллеливания шифрования.

Зашифрование/расшифрование i-го блока исходного текста/шифртекста выполняется независимо от остальных блоков:

,

,

где – блок исходного текста;

– блок шифротекста;

i – номер блока;

– блочная функция зашифрования;

– блочная функция расшифрования;

k – ключ.

**CBC** (Cipher Block Changing) – режим сцепления блоков шифра. Каждый блок открытого текста перед зашифрованием суммируется по модулю 2 с предыдущим блоком шифртекста.

Недостатки режима CBC:

– распространение ошибки с i-го на i+1-й блок;

– невозможность параллельной обработки блоков при зашифровании и расшифровании.

Достоинства режима CBC:

– одинаковые блоки исходного текста после зашифрования дают разные блоки криптотекста;

– невозможна независимая манипуляция с каждым блоком криптотекста отдельно.

,

,

,

где IV – вектор инициализации (случайное число).

**CTR** (Counter mode) – режим счетчика. Режим CTR делает из блочного шифра поточный. Он генерирует ключевую последовательность путем зашифрования значения счетчика которую затем суммирует по модулю два с исходным текстом:

Алгоритмы зашифрования и расшифрования в режиме CTR могут выполняться параллельно. Вычисления, связанные с зашифрованием значений счетчика могут быть выполнены до появления исходного или зашифрованного текстов.

Для режима CTR один бит ошибки в значении счетчика приводит к тому, что любой бит в расшифрованном сообщении может быть искаженным с вероятностью близкой к 50 %.

;

,

где значение счетчика для i-го блока.

Режимы ECB, CBC, CFB и OFB обрабатывают входной текст, длина которого должна быть кратна длине одного блока. Если это свойство не выполняется, то к сообщению необходимо добавить недостающее количество произвольных битов, называемых дополнением (padding). В стандарте ISO/IEC 9797-1 предложено добавлять в конец сообщения один единичный бит, а оставшиеся заполнять нулями.

При использовании этого метода для правильного расшифрования получатель должен точно знать, что в сообщении содержится дополнение. Это можно обеспечить, прикрепляя дополнение к каждому сообщению, даже если оно не требуется (в этом случае его посылают отдельным блоком) или посылать с каждым сообщением служебную информацию о его длине.

Кроме возникновения бита ошибки (инверсии бита) в блоке шифртекста может произойти удаление или вставка бита. Такое искажение приводит к нарушению границ всех последующих блоков шифртекста, и результаты их расшифрования будут полностью искаженными, пока не восстановится синхронизация границ блоков. При использовании режима 1-битного CFB синхронизация восстанавливается автоматически спустя b+1 позиций после вставленного или удаленного бита. В остальных режимах автоматического восстановления синхронизации не происходит.

Выбор режима шифрования зависит от поставленной цели и требований системы, в которую встраивают шифрование.

**ECB** (Electronic Code Book) – режим электронной кодовой книги, или режим простой замены;

**CBC** (Cipher Block Changing) – режим сцепления блоков шифра;

**CTR** (Counter mode) – режим счетчика.