Самостоятельная работа

**Тема:** "Принципы построения блочных шифров с закрытым ключом"

**Цель:** познакомиться с принципами построения современных блочных алгоритмов симметричного шифрования.

Контрольные вопросы

1. Какой шифр называют комбинированным или композиционным шифром?

Комбинированный (композиционный) шифр: Комбинированный или композиционный шифр - это шифр, который использует комбинацию различных методов шифрования. Это может включать в себя применение как симметричных (например, блочных или поточных) шифров, так и асимметричных (например, RSA). Часто комбинируют разные алгоритмы для повышения стойкости и безопасности шифрования.

1. Какие факторы влияют на стойкость блочного алгоритма шифрования?

Факторы, влияющие на стойкость блочного алгоритма шифрования:

Размер блока.

Размер ключа.

Качество ключевого расписания.

Сложность математических операций, используемых в алгоритме.

Эффективность алгоритма в сопротивлении различным видам атак.

1. Какие простейшие операции применяются в блочных алгоритмах шифрования?

Простейшие операции в блочных алгоритмах шифрования:

Перестановки битов (например, перестановки по таблице).

Подстановки (замены битов или байтов согласно заданной таблице подстановок).

Побитовые операции (например, XOR).

1. В чем отличие блочных алгоритмов шифрования от поточных?

Отличие блочных алгоритмов от поточных:

Блочные алгоритмы обрабатывают данные блоками фиксированного размера, в то время как поточные алгоритмы обрабатывают данные по одному биту или байту.

Блочные алгоритмы могут требовать заполнения данных, чтобы сделать их кратными размеру блока, в то время как поточные алгоритмы этого не требуют.

1. Что понимается под "раундом" алгоритма шифрования?

Понятие "раунд" в алгоритме шифрования: Раунд в алгоритме шифрования представляет собой последовательность преобразований (операций) над данными, ключами и промежуточными результатами, выполняемых для достижения шифрования или расшифрования. Раунды обычно включают в себя операции подстановки и перестановки, применяемые к блокам данных.

1. Каковы требования к блочному алгоритму шифрования?

Требования к блочному алгоритму шифрования:

Стойкость к криптоаналитическим атакам.

Эффективность (скорость работы).

Размер блока и ключа должны соответствовать стандартам безопасности.

Равномерное распределение вероятности для шифрования одинаковых блоков данных.

1. Почему блочный алгоритм шифрования должен иметь простую и понятную структуру?

Необходимость простой и понятной структуры блочного алгоритма: Простая и понятная структура упрощает анализ алгоритма для проверки его безопасности, облегчает разработку и обслуживание кода, а также уменьшает вероятность ошибок при его реализации.

1. Что понимается под требованием "высокой криптостойкости" алгоритма шифрования?

Требование "высокой криптостойкости" алгоритма шифрования: Высокая криптостойкость означает, что алгоритм обладает свойствами, делающими его устойчивым к различным криптоаналитическим атакам, включая методы анализа, перебора и другие.

1. Что представляет собой сеть Фейштеля?

Сеть Фейстеля: Сеть Фейстеля - это конструкция блочных шифров, где блок данных разделяется на две половины, которые проходят через серию раундов с использованием функций подстановки и перестановки. Эта конструкция позволяет легко расширять размер ключа и повышать безопасность алгоритма.

Упражнения для самостоятельной работы

1. Сложите по модулю 2:

1. двоичные числа 10101100 и 11001010 ;

Ответ: 10101100+11001010= 01100110

1. десятичные числа 15 и 10 ;

15=1111, 10=1010

Ответ:1111+1010=0101

1. шестнадцатеричные числа 0В5 и 37.

0В5=10110101, 37=110111

Ответ: 10110101+0110111= 11010010

Примечание: десятичные и шестнадцатеричные числа необходимо сначала перевести в двоичный вид.

2. Сложите по модулю :

1. двоичные числа 10101100 и 11001010 ;

Ответ: 10101100 + 11001010 = (1)01110110

1. десятичные числа 155 и 100;

155=0000000101010101 100=0000000100000000

Ответ:0000000101010101+0000000100000000= 1001010101

1. шестнадцатеричные числа 0В5 и 37.

0В5=10110101, 37=110111

Ответ: 10110101+ 00110111= 11101010

Примечание: десятичные числа необходимо сначала перевести в двоичный вид.

3. Выполните операцию циклического сдвига:

1. влево на 5 разрядов для двоичного числа 10101100;

ответ: 01100101

1. вправо на 4 разряда для шестнадцатеричного числа 9E ;

9Е=10011110

ответ: 11101001

1. вправо на 2 разряда для шестнадцатеричного числа 55.4

55=1010101

ответ: 0110101

Примечание: шестнадцатеричные числа необходимо сначала перевести в двоичный вид.

4. Пусть каждые три бита входного сообщения заменяются по следующей таблице замен:

Вход Выход

000 011

001 101

010 000

011 111

100 010

101 110

110 001

111 100

1) Исходное сообщение:

|  |  |  |  |
| --- | --- | --- | --- |
| 101 | 011 | 001 | 100 |
| 110 | 111 | 101 | 010 |

Ответ :

2) Исходное сообщение:

2356=

|  |  |  |  |
| --- | --- | --- | --- |
| 100 | 100 | 110 | 100 |
| 010 | 010 | 001 | 010 |

Ответ:

3) Исходное сообщение:

0B57=

|  |  |  |  |
| --- | --- | --- | --- |
| 101 | 101 | 010 | 111 |
| 110 | 110 | 000 | 100 |

Ответ:

5. Выполните разбиение исходного сообщения на блоки по три бита и произведите поблочную замену для следующих сообщений, представленных в цифровом виде:

o 1010 1100 1100(2)

o 2356(10)

o 0В57(16)

Решение: для поблочной замены будет использовать таблицу  
из задания 4:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Вход | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| Выход | 011 | 101 | 000 | 111 | 010 | 110 | 001 | 100 |

1) Исходное сообщение:

|  |  |  |  |
| --- | --- | --- | --- |
| 101 | 011 | 001 | 100 |
| 110 | 111 | 101 | 010 |

Ответ:

2) Исходное сообщение:

2356=

|  |  |  |  |
| --- | --- | --- | --- |
| 100 | 100 | 110 | 100 |
| 010 | 010 | 001 | 010 |

Результат:

3) Исходное сообщение:

0B57=

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ↓ | 101 | 101 | 010 | 111 |
| 110 | 110 | 000 | 100 |

Ответ:

Примечание: десятичные и шестнадцатеричные числа необходимо сначала перевести в двоичный вид.