1. **Какие простейшие операции применяются в блочных алгоритмах шифрования?**

опера- ция суммирования 2-х (*А* + *В*) *n*-разрядных чисел – XOR: *А* + *В* (mod *n*). По- мимо этой операции некоторые алгоритмы (Blowfish, IDEA, ГОСТ и др.) предусматривают выполнение операций сложения чисел по модулю более вы- соких порядков: XOR: *А* + *В* (mod 2*n*). Понятно, что числа *А* и *В* также являются *n*-разрядных.

**(2) замена бит по таблице замен**

**(3)**нахождение остатка от деления на большое простое число

**(4) перестановка бит**

**(5) сложение по модулю 2**

1. **В чем отличие блочных алгоритмов шифрования от потоковых**?

§ важнейшим достоинством поточных шифров перед блочными является высокая скорость шифрования, соизмеримая со скоростью поступления входной информации; поэтому, обеспечивается шифрование практически в реальном масштабе времени вне зависимости от объема и разрядности потока преобразуемых данных.

§ в синхронных поточных шифрах (в отличие от блочных) отсутствует эффект размножения ошибок, то есть число искаженных элементов в расшифрованной последовательности равно числу искаженных элементов зашифрованной последовательности, пришедшей из канала связи.

§ структура поточного ключа может иметь уязвимые места, которые дают возможность криптоаналитику получить дополнительную информацию о ключе (например, при малом периоде ключа криптоаналитик может использовать найденные части поточного ключа для дешифрования последующего закрытого текста).

ПШ в отличие от БШ часто могут быть атакованы при помощи линейной алгебры (так как выходы отдельных регистров сдвига с обратной линейной связью могут иметь корреляцию с гаммой). Также для взлома поточных шифров весьма успешно применяется линейный и дифференциальный анализ.

1. **Что понимается под "раундом" алгоритма шифрования?**

**Раундом (или циклом)** в [криптографии](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) называют один из последовательных шагов обработки данных в алгоритме [блочного шифрования](https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D1%87%D0%BD%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5).[[1]](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%83%D0%BD%D0%B4_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)#cite_note-nom1-1) В шифрах [Фейстеля](https://ru.wikipedia.org/wiki/%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8C,_%D0%A5%D0%BE%D1%80%D1%81%D1%82" \o "Фейстель, Хорст) (построенных в соответствии с архитектурой [сети Фейстеля](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D1%8C_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F)) и близких ему по архитектуре шифрах — один шаг [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации путём применения круговой функции

Архитектура построения блочных шифров, доминирующая в настоящее время в традиционной [криптографии](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F), в которой весь процесс шифрования блока выполняется за серию шагов (раундов). На каждом раунде блок делится на изменяемую и постоянную части. С помощью функции шифрования из постоянной части и раундового ключа вырабатывается модифицирующий код, который используется для модификации изменяемой части посредством операции [гаммирования](https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5).[[2]](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%83%D0%BD%D0%B4_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)#cite_note-nom2-2)

Широкое распространение [сети Фейстеля](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D1%8C_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F) получили потому, что они удовлетворяют всем требованиям к алгоритмам [симметричного шифрования](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и в то же время достаточно просты и компактны.

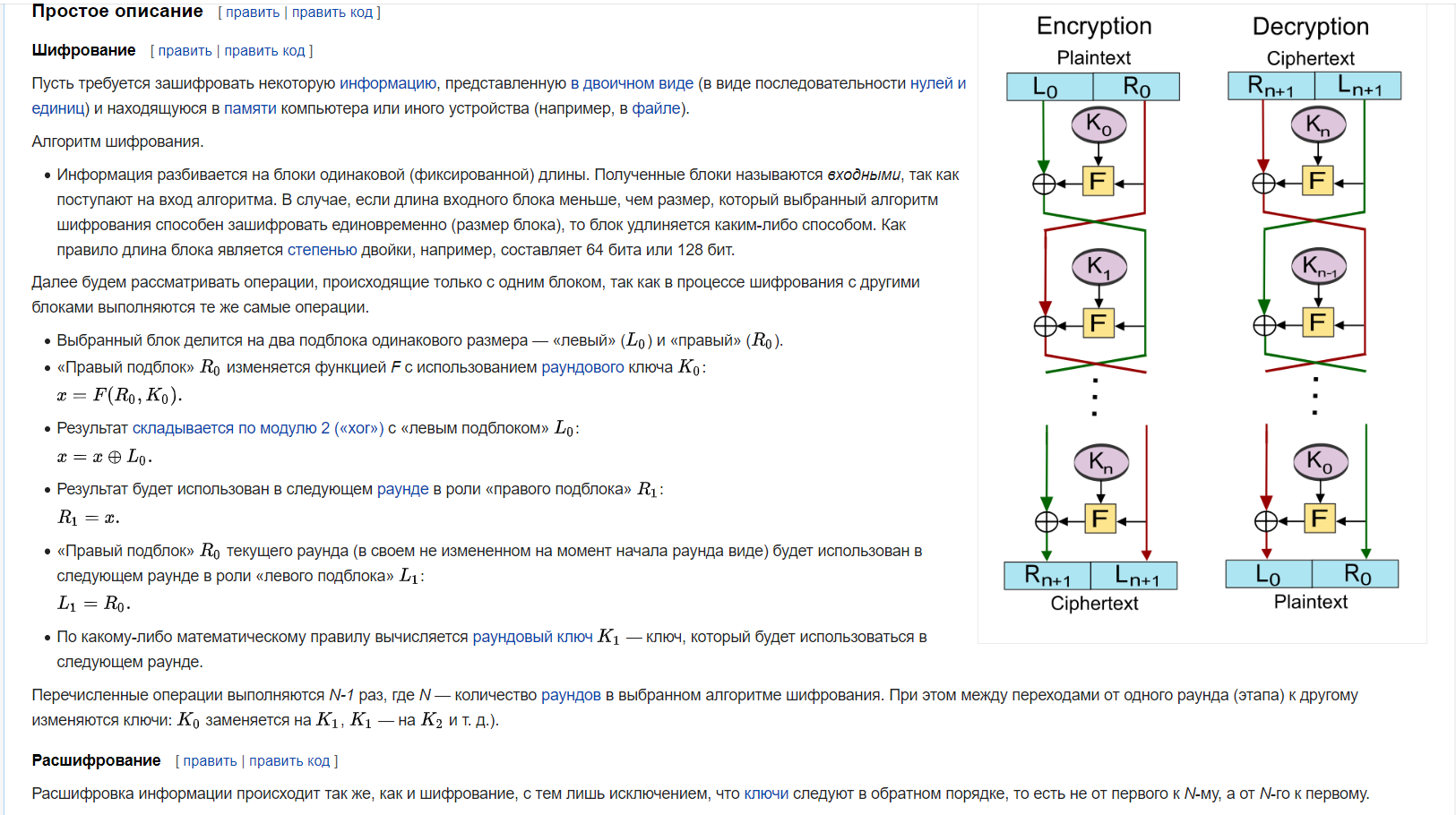
В ходе шифрации используется функция F, называемая образующей. Каждый раунд состоит из вычисления функции F для одной ветви и побитового выполнения операции [XOR](https://ru.wikipedia.org/wiki/XOR) результата F с другой ветвью. После этого ветви меняются местами.

Считается, что оптимальное число раундов — от 8 до 32. Важно то, что увеличение количества раундов значительно увеличивает [криптостойкость](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D1%82%D0%BE%D0%B9%D0%BA%D0%BE%D1%81%D1%82%D1%8C) [алгоритма](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC).[[3]](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%83%D0%BD%D0%B4_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)#cite_note-3)[[4]](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%83%D0%BD%D0%B4_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)#cite_note-nom3-4)

Возможно, эта особенность и повлияла на активное распространение [сети Фейстеля](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D1%8C_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F), так как для большей [криптостойкости](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D1%82%D0%BE%D0%B9%D0%BA%D0%BE%D1%81%D1%82%D1%8C) достаточно увеличивать количество раундов, не изменяя сам [алгоритм](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC). В последнее время количество раундов не фиксируется, а лишь указываются допустимые пределы.

1. **Охарактеризовать и привести формальное описание сети Фейстеля.**

**Сеть Фе́йстеля**, или конструкция [Фейстеля](https://ru.wikipedia.org/wiki/%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8C,_%D0%A5%D0%BE%D1%80%D1%81%D1%82" \o "Фейстель, Хорст) ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Feistel network, Feistel cipher*), — один из методов построения [блочных шифров](https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D1%87%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80). Сеть состоит из ячеек, называемых **ячейками Фейстеля**. На вход каждой ячейки поступают данные и ключ. На выходе каждой ячейки получают изменённые данные и изменённый ключ. Все ячейки однотипны, и говорят, что сеть представляет собой определённую многократно повторяющуюся ([итерированную](https://ru.wikipedia.org/wiki/%D0%98%D1%82%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D1%8F_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0))) структуру. [Ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) выбирается в зависимости от алгоритма шифрования/расшифрования и меняется при переходе от одной ячейки к другой. При [шифровании](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и расшифровании выполняются одни и те же операции; отличается только порядок [ключей](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)). Ввиду простоты операций сеть Фейстеля легко реализовать как программно, так и аппаратно. Большинство современных [блочных шифров](https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D1%87%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80) ([DES](https://ru.wikipedia.org/wiki/DES), [RC2](https://ru.wikipedia.org/wiki/RC2), [RC5](https://ru.wikipedia.org/wiki/RC5), [RC6](https://ru.wikipedia.org/wiki/RC6), [Blowfish](https://ru.wikipedia.org/wiki/Blowfish), [FEAL](https://ru.wikipedia.org/wiki/FEAL), [CAST-128](https://ru.wikipedia.org/wiki/CAST-128), [TEA](https://ru.wikipedia.org/wiki/TEA), [XTEA](https://ru.wikipedia.org/wiki/XTEA), [XXTEA](https://ru.wikipedia.org/wiki/XXTEA) и др.) использует сеть Фейстеля в качестве основы. Альтернативой сети Фейстеля является [подстановочно-перестановочная сеть](https://ru.wikipedia.org/wiki/SP-%D1%81%D0%B5%D1%82%D1%8C) ([AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) и др.).



1. **Какие стандартные операции используются в блочных алгоритмах шифрования?**

Все перечисленные стандарты и алгоритмы *блочных шифров* (БШ) строятся на основе подстановочных и перестановочных, т. е. являются комбинационными. БШ относятся также к классу симметричных.

в *алгоритмах симметричного шифрования* часто используются *операции* сложения по модулю 2, сложения по модулю 216 или 232, циклического сдвига, замены и перестановки.



1. **В чем состоит особенность сложения чисел по модулю 2n?**

. Самое большое слагаемое меньше 2*n*. Например, при *n=*3 са мое большое слагаемое в двоичном виде – это 111 (или 7), а 2*n* = 8.

Во-вторых. Результатом сложения также должно быть *n*-разрядное число.

В-третьих. Побитовое сложение предусматривает известную взаимосвязь между соседними символами (порядками).

В-пятых. В силу известных правил модулярной1 арифметики результат вычисления *А* + *В* (mod 2*n*) – это остаток от деления: (*А* + *В*)/ 2*n*.

1. Сложить по модулю 102 пары чисел: 55 и 14; 76 и 24; 99 и 99.
2. Сложить по модулю 28:

двоичные числа 10101100 и 11001010; 01111111 и 01101101; шестнадцатеричные числа 0В5 и 37.

1. **Дать пояснение принципам реализации «лавинного» эффекта.**

Важное криптографическое свойство для шифрования, которое означает, что изменение значения малого количества битов во входном тексте или в ключе ведет к «лавинному» изменению значений выходных битов шифротекста. Другими словами, это зависимость всех выходных битов от каждого входного бита.

Выбрать два произвольных блочных алгоритма. В чем состоят отличия между ними?

<https://techdifferences.com/difference-between-des-and-aes.html>

1. Представить графически и пояснить функционал одного раунда блочного алгоритма DES (АES, ГОСТ 28147-89, Blowfish).
2. **Сколько можно реализовать (теоретически) разновидностей алгоритма 3DES**?

Cуществуют несколько реализаций алгоритма 3DES. Вот некоторые из них:

* + DES-EEE3: шифруется 3 раза с 3 разными ключами (операции шифро

вание-шифрование-шифрование);

* + DES-EDE3: 3DES операции шифрование-расшифрование-шифрование с разными ключами:
  + DES-EEE2 и DES-EDE2: как и предыдущие, однако, на первом и третьем шаге используется одинаковый ключ.

Расшифрование происходит, как и в простом DES, в обратном порядке по отношению к процедуре зашифрования.

1. **Какие факторы влияют на стойкость блочного алгоритма шифрования?**

**(1) используемые операции**

**(2) длина ключа**

**(3) количество раундов**

1. **В чем состоит сущность дифференциального криптоанализа?**

*Дифференциальный криптоанализ* базируется на таблице неоднородных дифференциальных распределений *S*-блоков в блоч- ном шифре. Криптоанализ шифртекстов на основе рассматриваемого стан- дарта «работает» с парами шифртекстов, открытые тексты которых имеют определенные разности, как это отмечалось в материалах к лабораторной ра- боте № 2. Метод анализирует эволюцию этих разностей в процессе прохожде- ния открытых текстов раундов DES при шифровании одним и тем же ключом.

1. **В чем состоит сущность линейного криптоанализа?**

*Линейный криптоанализ*. Для того, чтобы найти линейное приближение для DES нужно найти «хорошие» однораундовые линейные приближения и объединить их. Обратим внимание на *S*-блоки. У них 6 входных битов и 4 вы- ходных. Входные биты можно объединить с помощью операции XOR 63 спо- собами (26 - 1), а выходные биты – 15 способами. Теперь для каждого *S*-блока можно оценить вероятность того, что для случайно выбранного входа входная комбинация XOR равна некоторой выходной комбинации XOR. И т.д.

1. **Какие ключевые комбинации относятся к слабым (к полуслабым) и по- чему?**
2. ***Слабые и полуслабые ключи***. Из-за того, что первоначальный ключ изменяется при получении подключа для каждого раунда алгоритма, определенныепервоначальные ключи являются *слабыми* [4]. Вспомним, что первоначальное значение разделяется на две половины, каждая из которых сдвигается незави- симо. Если все биты каждой половины равны 0 или 1, то для всех раундов ал- горитма используется один и тот же ключ. Это может произойти, если ключ состоит из одних 1, из одних 0, или если одна половина ключа состоит из од- них 1, а другая – из одних 0.
3. Четыре слабых ключа показаны в шестнадцатеричном виде в табл. 5.3 (каждый восьмой бит – это бит четности).
4. **Слабые ключи DES**

|  |  |  |  |
| --- | --- | --- | --- |
| 0101 | 0101 | 0101 | 0101 |
| 1F1F | 1F1F | 0E0E | 0E0E |
| E0E0 | E0E0 | F1F1 | F1F1 |
| FEFE | FEFE | FEFE | FEFE |

Кроме того, некоторые пары ключей при зашифровании переводят откры- тый текст в идентичный шифртекст. Иными словами, один из ключей пары может расшифровать сообщения, зашифрованные другим ключом пары. Это происходит из-за метода, используемого DES для генерации подключей: вме- сто 16 различных подключей эти ключи генерируют только два различных подключа. В алгоритме каждый из этих подключей используется восемь раз. Эти ключи, называемые *полуслабыми*, в шестнадцатеричном виде приведены в табл. 5.4.

**Полуслабые ключи DES**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 01FE | 01FE | 01FE | 01FE | и | FE01 | FE01 | FE01 | FE01 |
| 1FE0 | 1FE0 | 0EF1 | 0EF1 | и | E01F | E01F | F10E | F10E |
| 01E0 | 01E0 | 01F1 | 01F1 | и | E001 | E001 | F101 | F101 |
| 1FFE | 1EEE | 0EFE | 0EFE | и | FE1F | FE1F | FE0E | FE0E |
| 011F | 011F | 010E | 010E | и | 1F01 | 1F01 | 0E01 | 0E01 |
| E0FE | E0FE | F1FE | F1FE | и | FEE0 | FEE0 | FEE1 | FEE1 |

1. Где **применяются блочные криптоалгоритмы**?

сообщений, файлов и другой информации, пред- ставленной в электронном виде, например, на жёстком диске ); в S/mime для обеспечения криптографической безопасности электронной почты.

3DES используется при управлении ключами в стандартах ANSI X9.17 (метод генерации 64-битных ключей) и ISO 8732 (управление ключами в бан- ковском деле), а также в PEM (Privacy Enhanced Mail).