

Блочные шифры. Сети Фейстеля

Криптология

```
graph TD; A[Криптология] --> B[Криптография]; A --> C[Криптоанализ]; B --> D[Поиск и исследование мат. методов преобразования информации]; C --> E[Исследование возможности расшифрования информации без знания ключа];
```

Криптография

Поиск и
исследование мат.
методов
преобразования
информации

Криптоанализ

Исследование
возможности
расшифрования
информации без
знания ключа

Использование криптографических методов

```
graph TD; A[Использование криптографических методов] --> B[Хранение конфиденциальной и секретной информации]; A --> C[Установление подлинности сообщений]; A --> D[Передача конфиденциальной и секретной информации];
```

Хранение
конфиденциальной и
секретной информации


Установление
подлинности
сообщений

Передача
конфиденциальной и
секретной информации

Криптографическая система с секретным ключом (Симметричная криптография)



Криптографические системы



```
graph TD; A[Криптографические системы] --> B[Ограниченного использования]; A --> C[Общего использования]; B --> D[Стойкость основывается на сохранении в секрете алгоритма шифрования]; C --> E[Стойкость – основывается на секретности ключа, Алгоритм шифрования открыт];
```

Ограниченного
ИСПОЛЬЗОВАНИЯ

Стойкость
основывается на
сохранении в секрете
алгоритма
шифрования

Общего
ИСПОЛЬЗОВАНИЯ

Стойкость –
основывается на
секретности ключа,
Алгоритм
шифрования открыт

Симметричный шифр

```
graph TD; A[Симметричный шифр] --> B[Поточный]; A --> C[Блочный]; B --> D[Обработка информации побитно]; C --> E[Обработка информации поблочно];
```

The diagram is a hierarchical flowchart. At the top is a blue rounded rectangle containing the text 'Симметричный шифр'. Two arrows point downwards from this box to two light blue rounded rectangles: 'Поточный' on the left and 'Блочный' on the right. From 'Поточный', an arrow points down to an orange-to-blue gradient rounded rectangle containing 'Обработка информации побитно'. From 'Блочный', an arrow points down to another orange-to-blue gradient rounded rectangle containing 'Обработка информации поблочно'.

Поточный

Обработка
информации побитно

Блочный

Обработка
информации поблочно

Требования к современным криптографическим системам ЗИ

зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

число операций для определения использованного ключа шифрования по фрагменту шифросообщения и соответствующего ему открытому тексту, д. б. не меньше общего числа возможных ключей;

число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей соврем. компьютеров (с учетом возможности использования сетевых вычислений);

знание алгоритма шифрования не должно влиять на надежность защиты;

незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

структурные элементы алгоритма шифрования д. б. неизменными;

Доп. биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифротексте;

длина шифротекста д. б. равной длине исходного текста;

не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемых в процессе шифрования;

любой ключ из множества возможных должен обеспечивать надежную ЗИ;

алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Криптографические сети



состоят из многократных повторений, называемых *циклами* (*раундами, проходами*), состоящих из нескольких видов операций, называемых *слоями*.

Достоинства криптографических сетей

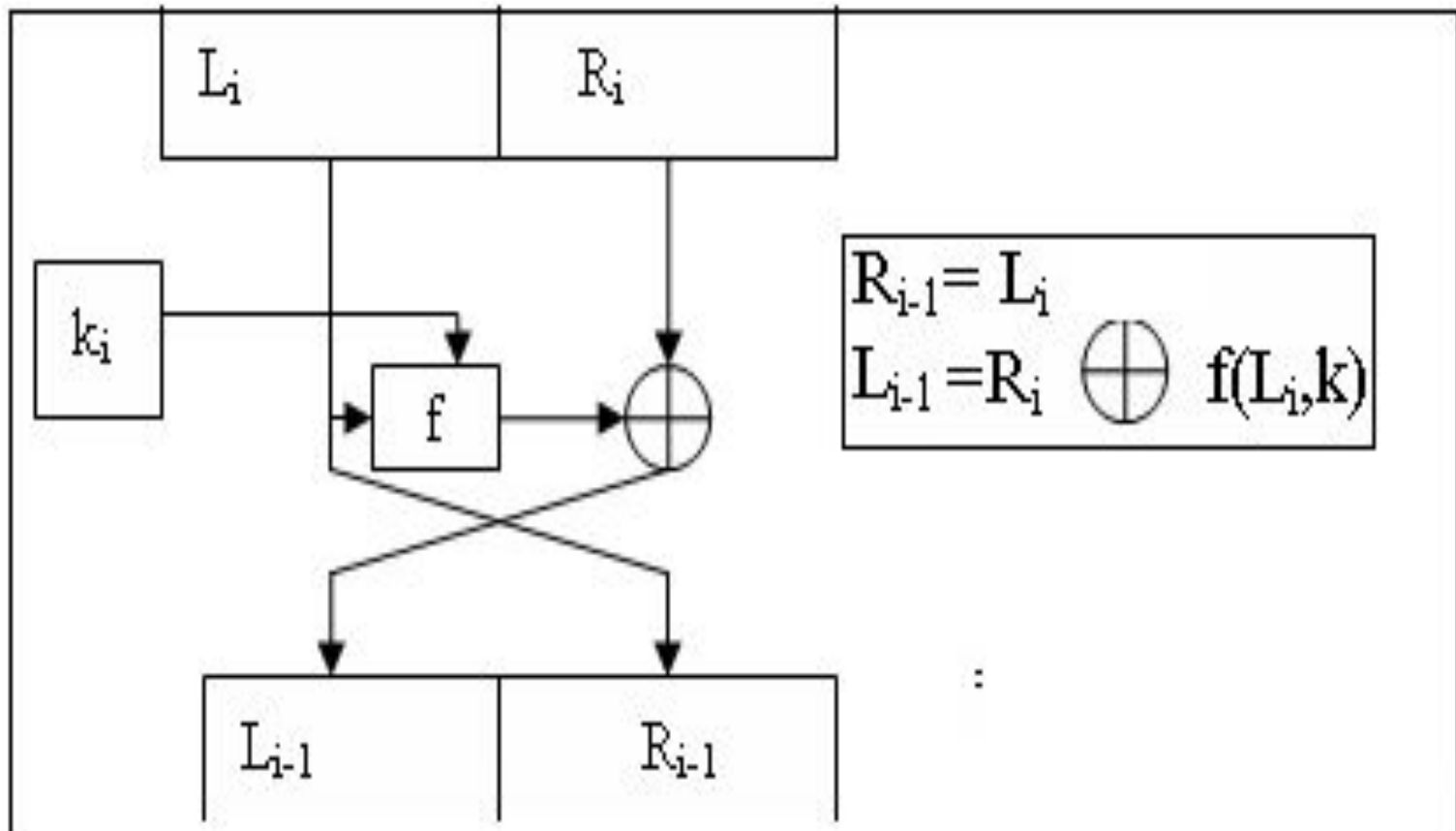
Уменьшение размера
программного кода за
счет использования
ЦИКЛОВ

простота усложнения
шифра увеличением
числа раундов

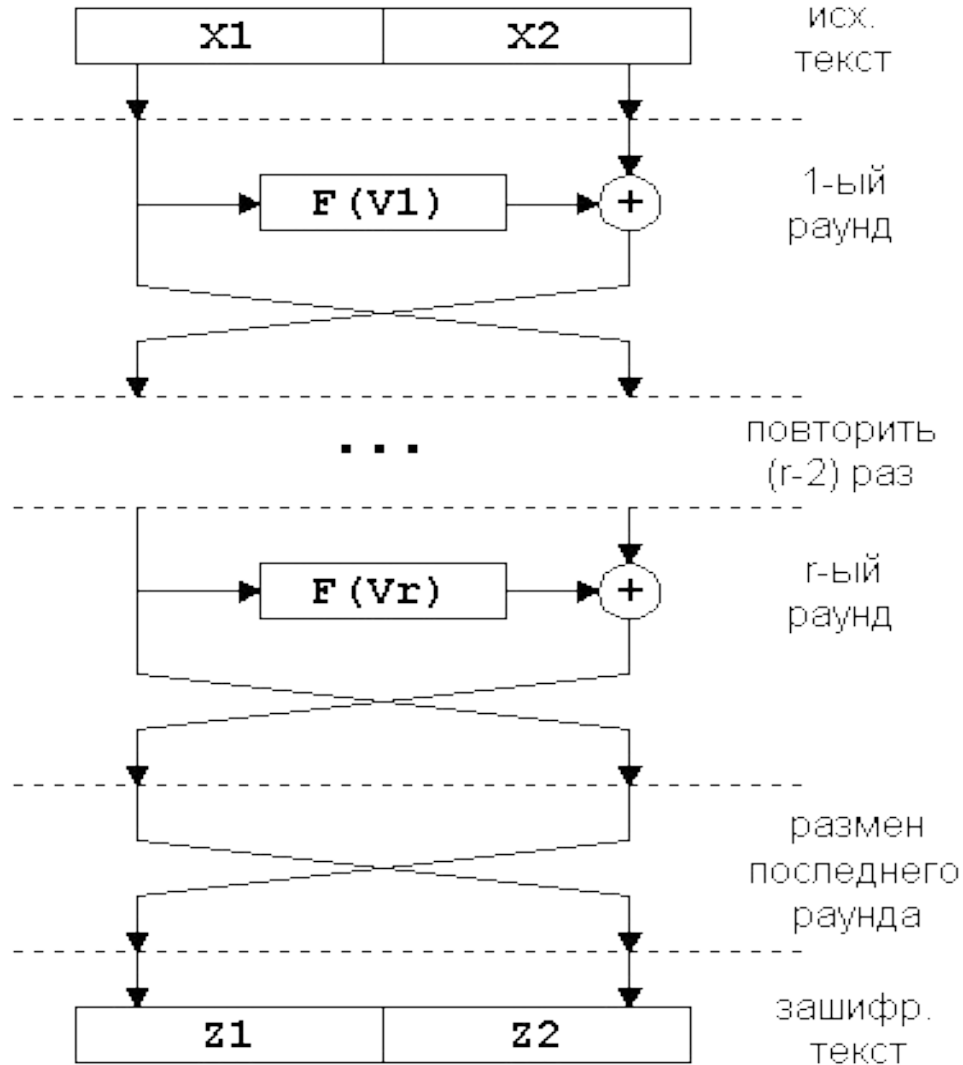
Унификация формулы
шифрования, упрощение
проверки
криптостойкости

Сети Фейстеля

Схема одного прохода :



Классическая сеть Фейстеля



Особенности сети Фейстеля

в каждом проходе - по одному слою (**преобразования однотипны**)

на какую-либо часть шифруемого блока **обратимая (необратимая) операция** накладывает значение, вычисленное от другой части

Входной блок делится на несколько одинаковых подблоков - ветвей

Сеть является обратимой (для дешифрации не нужно вычислять обратную функцию)

Для дешифрации используется тот же алгоритм, на вход подается тот же текст, **ключи** используются в **обратном порядке**

Алгоритмы на основе сети Фейстеля

Blowfish

TEA

XTEA

RC5

CAST-
128

DES

XXTEA

ГОСТ
28147-8
9

RC6