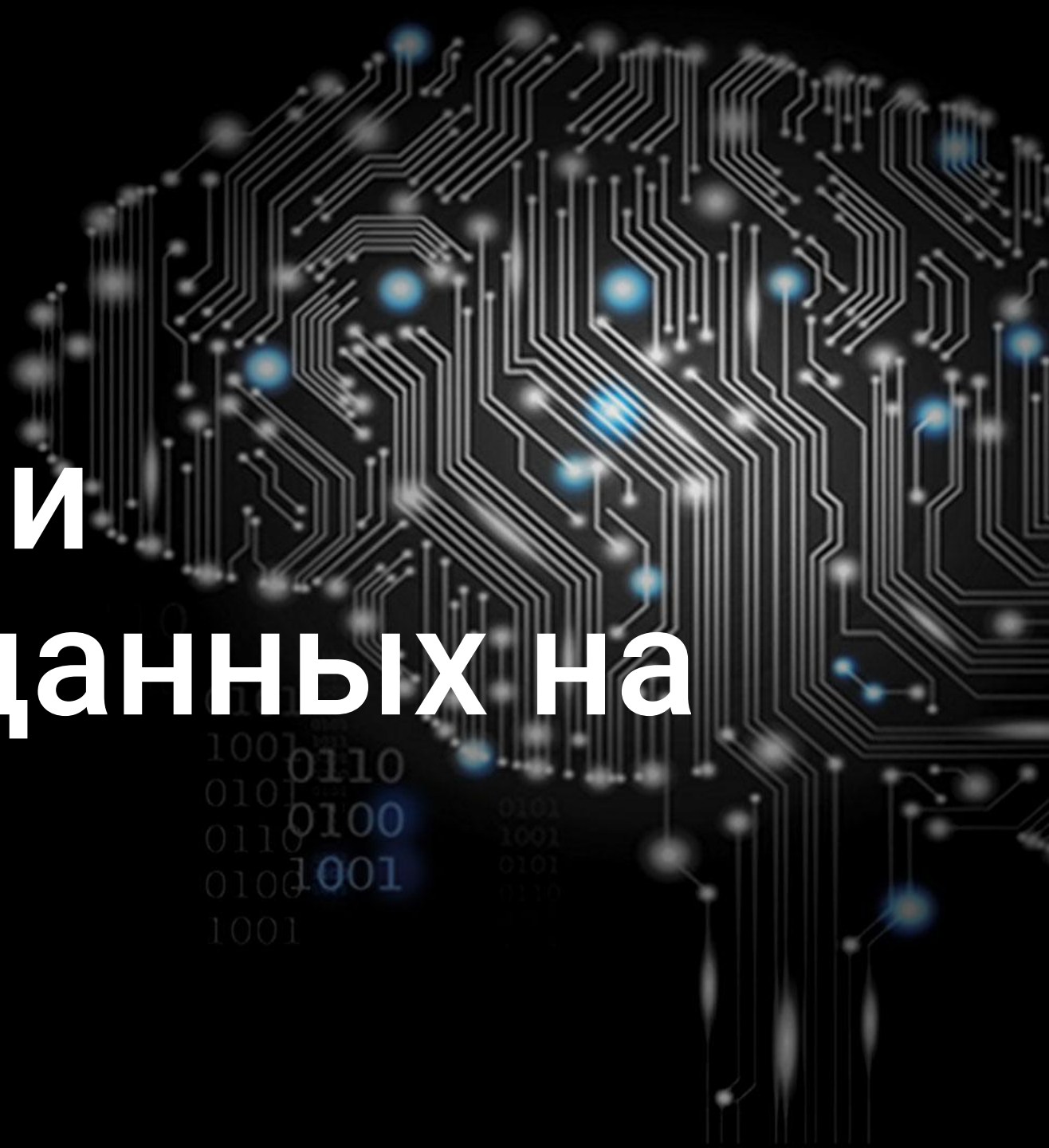
GeekBrains



Алгоритмы и структуры данных на языке C

Блочные шифры

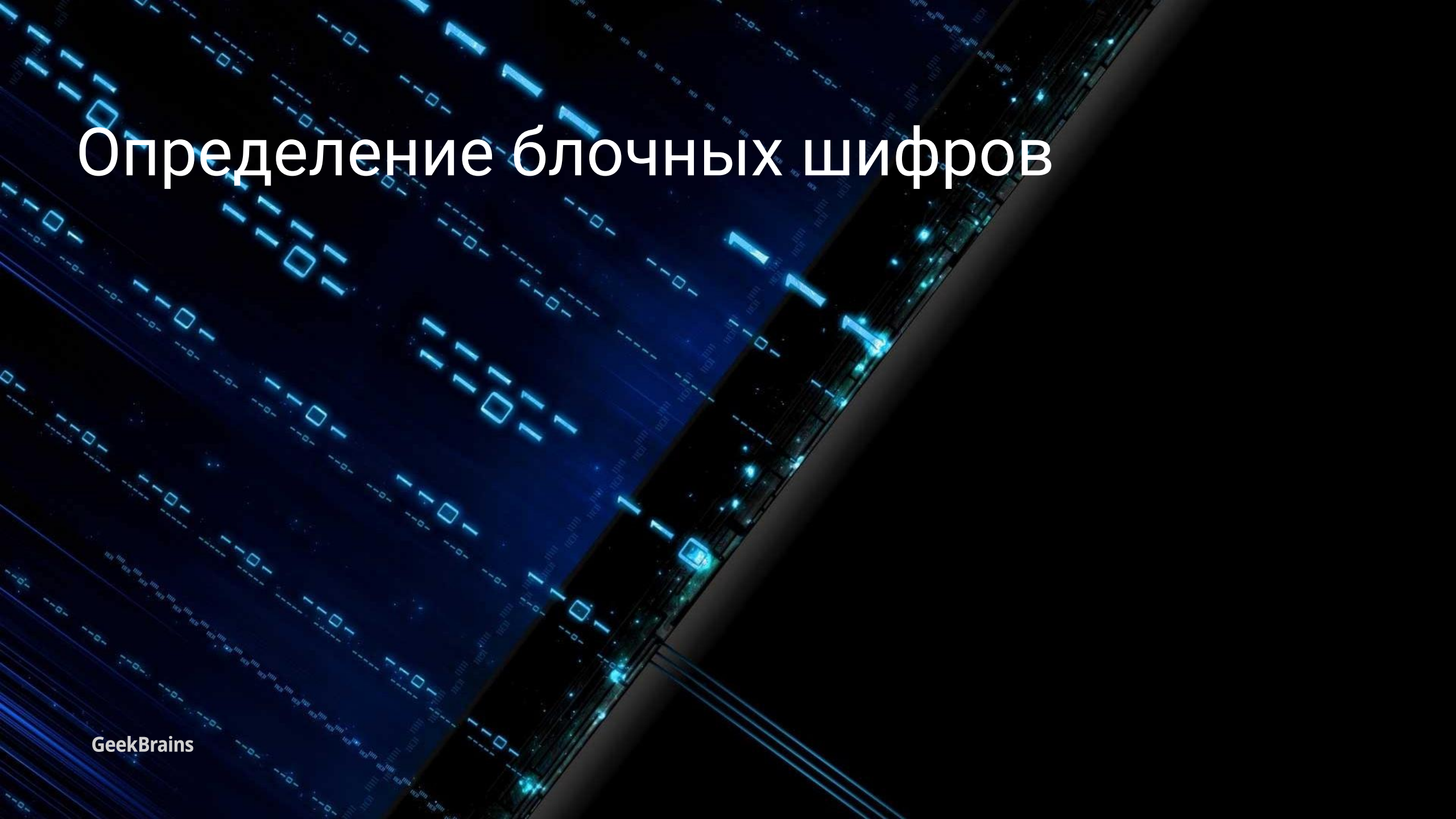
GeekBrains

Блочные шифры

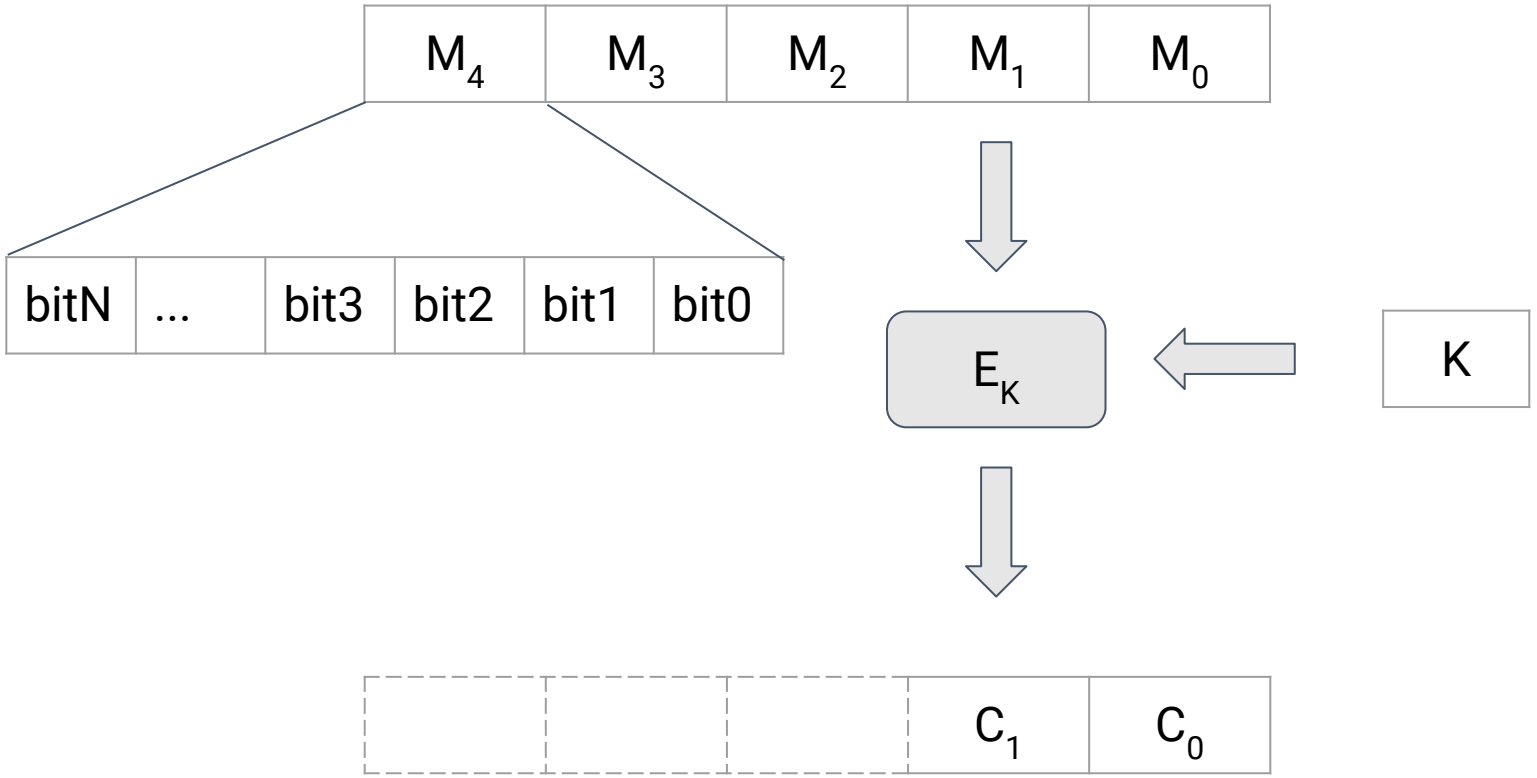
В этом видео

1. Определение блочных шифров
2. Трехраундовый шифр
3. Шифр Фейстеля

Определение блочных шифров



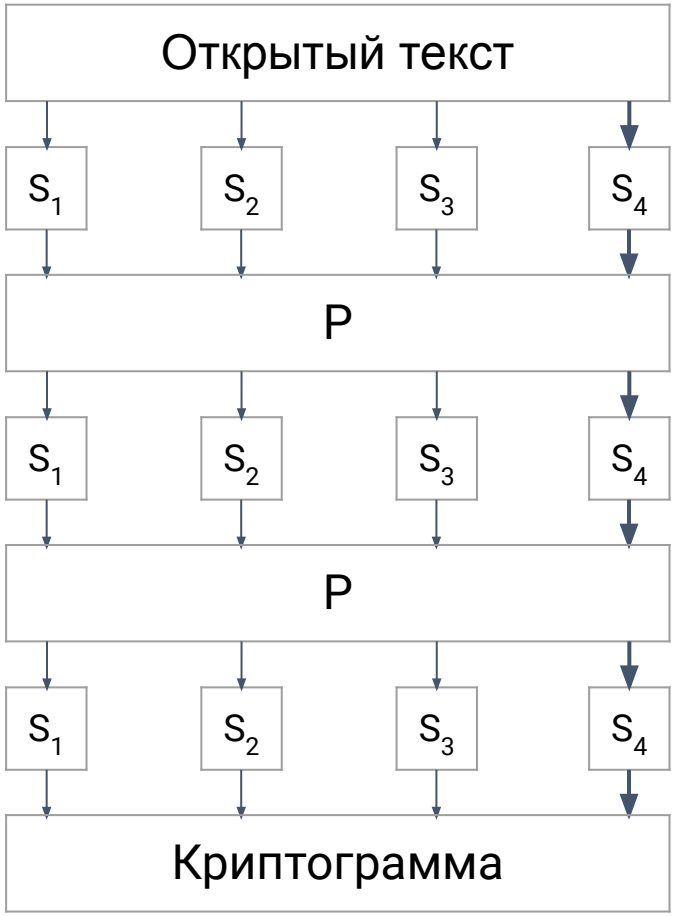
Общая схема блочных шифров

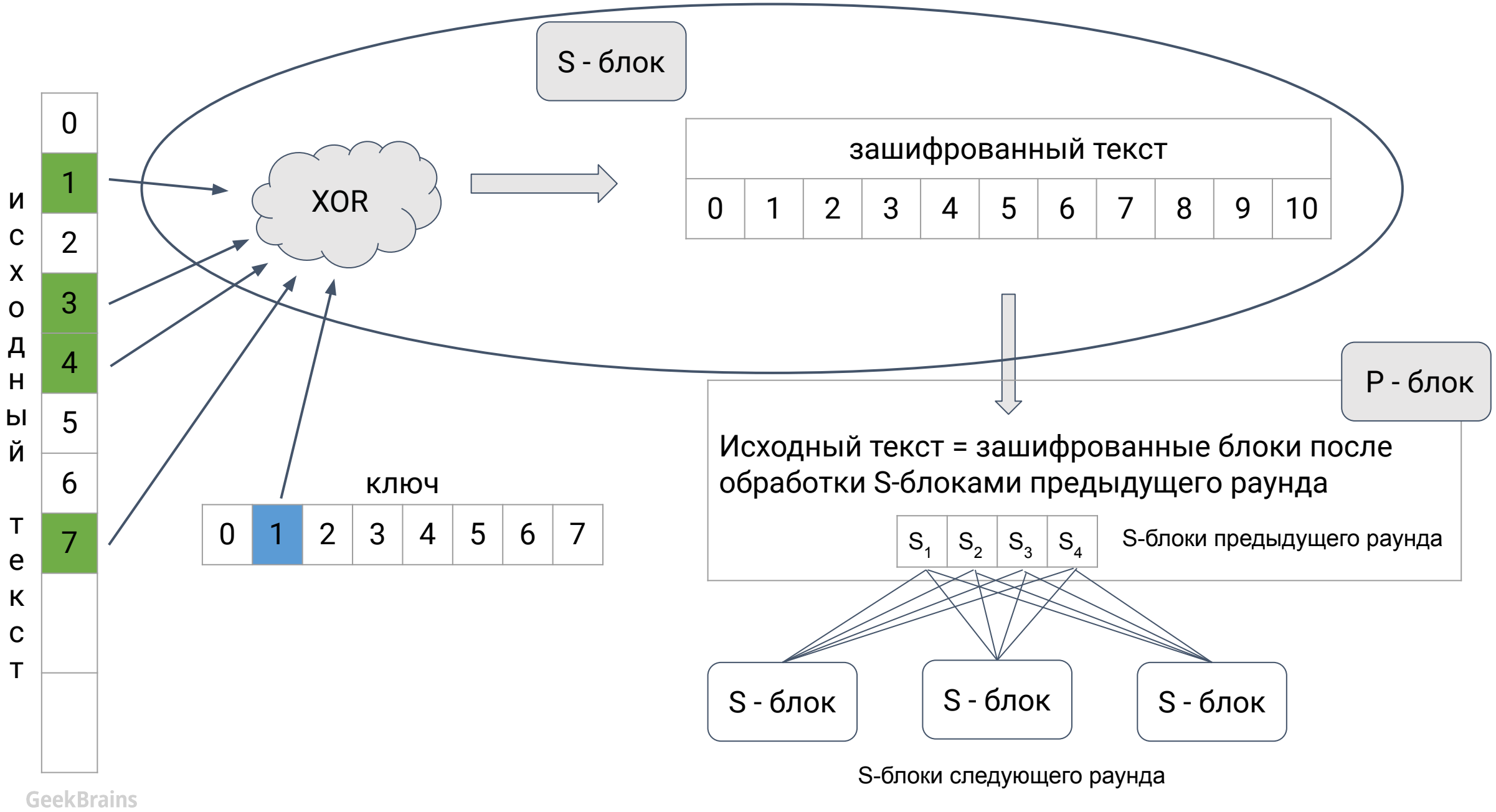


Трехраундовый шифр

GeekBrains

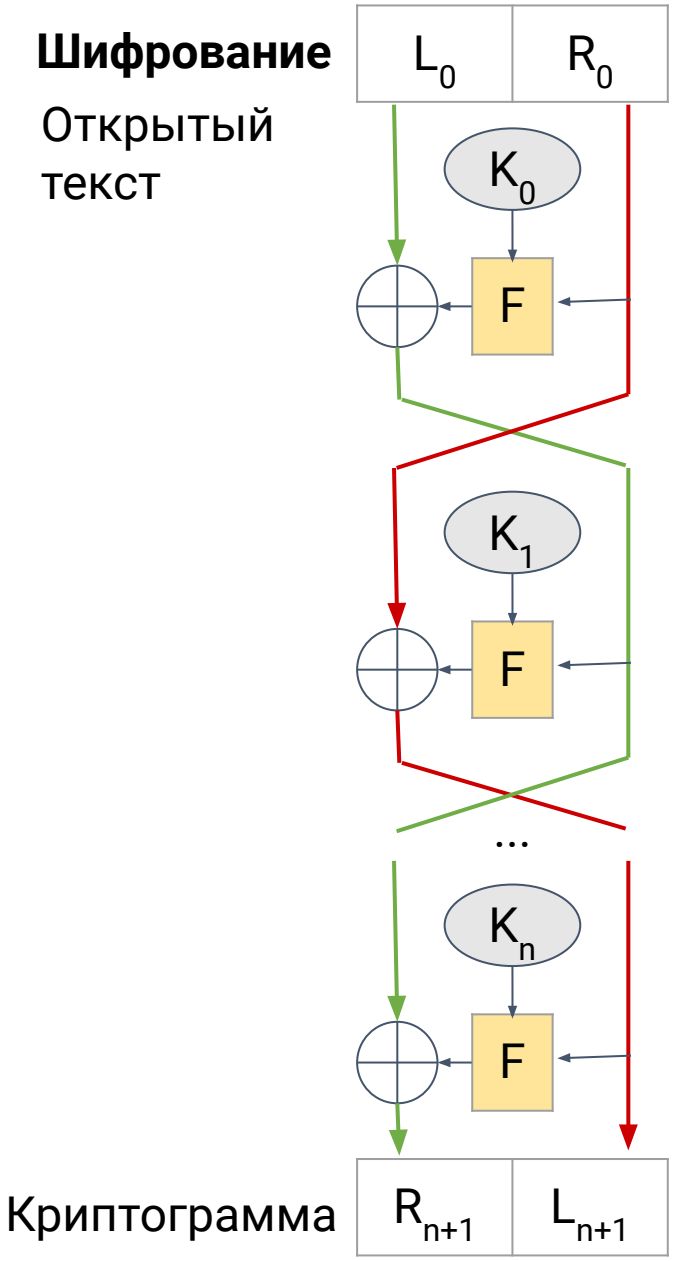
Трехраундовый шифр

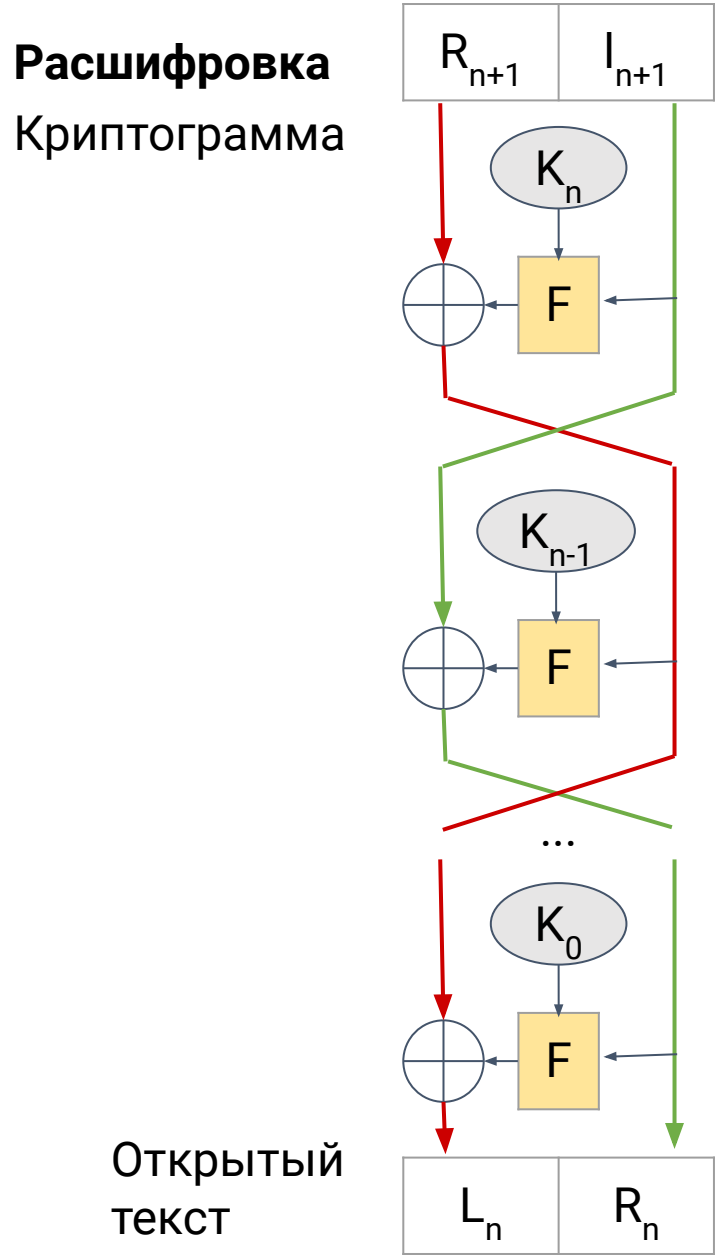



S - блок
исходный текст
0
1
2
3
4
5
6
7
XOR
ключ
0 1 2 3 4 5 6 7
зашифрованный текст
0 1 2 3 4 5 6 7 8 9 10
P - блок
Исходный текст = зашифрованные блоки после обработки S-блоками предыдущего раунда
S1 S2 S3 S4
S-блоки предыдущего раунда
S - блок
S - блок
S - блок
S-блоки следующего раунда

Шифр Фейстеля

Шифр Фейстеля





Высокоуровневое описание алгоритма Фейстеля

1. Разбиваем открытый текст пополам на блоки L_0 и R_0
2. Повторяем:
   a. присваиваем $L_{i+1} = R_i$;
   b. присваиваем $R_{i+1} = L_i$ XOR $F(R_i , K_i)$.

Алгоритм расшифровывания шифра Фейстеля

1. Разделяем криптограмму пополам на L_{i+1} и R_{i+1}
2. Повторяем:
   a. присваиваем $R_i = L_{i+1}$;
   b. присваиваем $L_i = R_{i+1}$ XOR $F(L_{i+1}, K_i)$.

Итоги

Рассмотрели:

- Определение блочных шифров
- Трехраундовый шифр
- Шифр Фейстеля