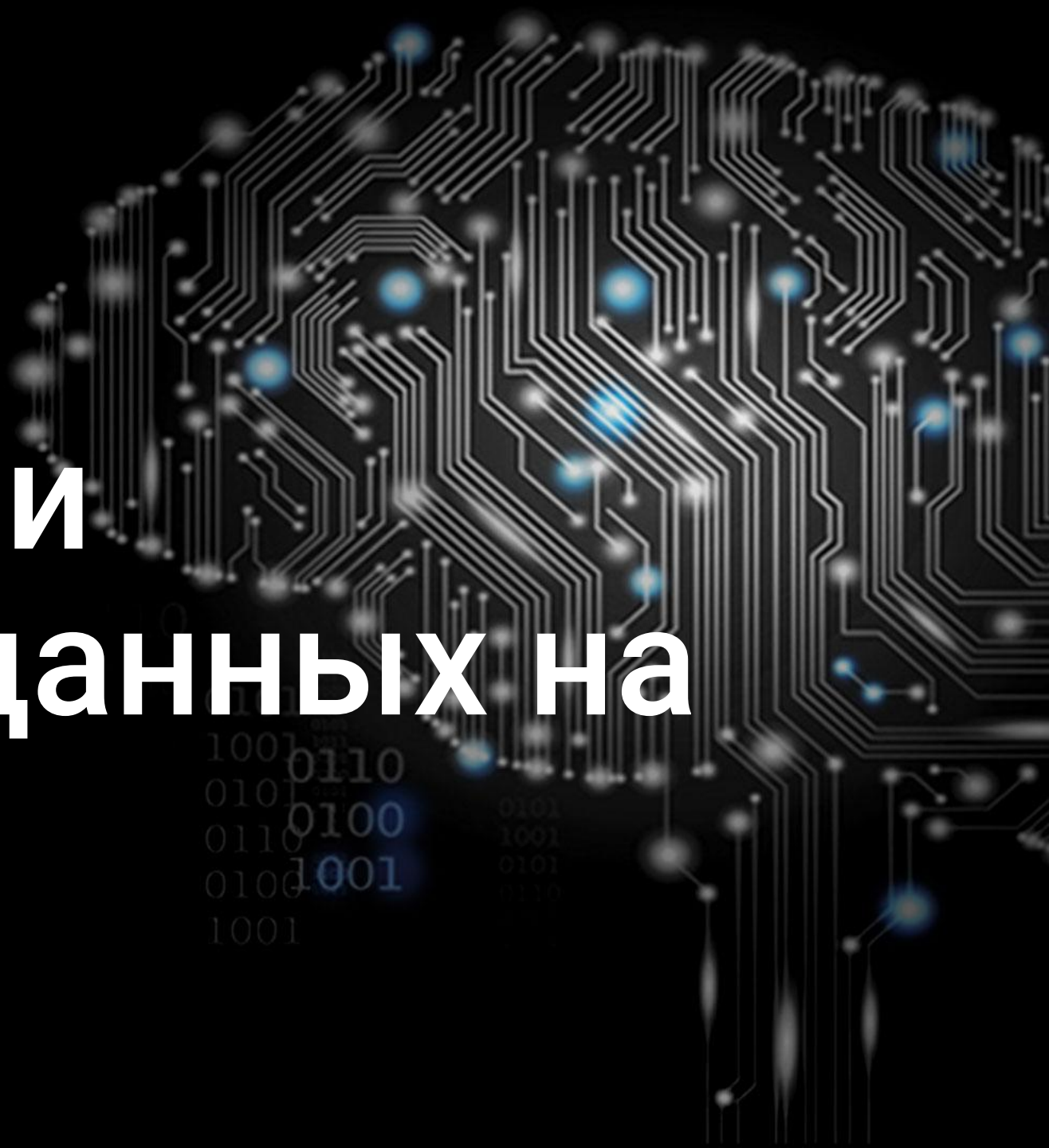
GeekBrains



Алгоритмы и структуры данных на языке C

MD5

GeekBrains

MD5

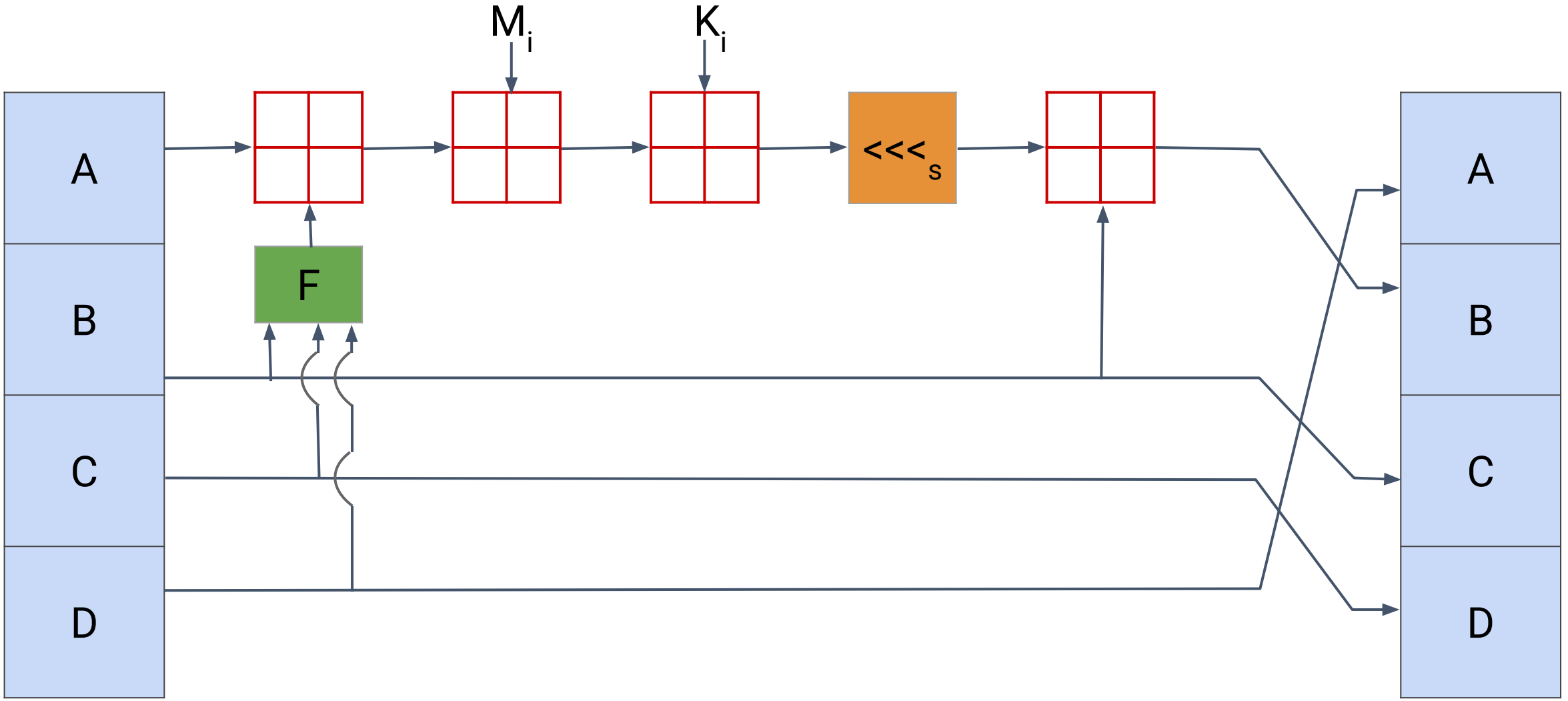
В этом видео

1. Применение MD5
2. Устройство MD5

Алгоритм MD5

GeekBrains

MD5 по RFC 6151



Алгоритм MD5

Этап 1. Добавление битов заполнения

Этап 2. Добавление размера сообщения

Этап 3. Инициализация буфера MD

Этап 4. Обработка сообщения блоками по 16 слов

Этап 5. Вывод

Работа алгоритма

Этап 1. Добавление битов заполнения или выравнивание потока

$$L' = 512 \times N + 448$$

где L это новая длина, а N старая

Этап 2. Добавление длины сообщения

M [0 ... N-1]

где M - массив 32-битных слов конечной последовательности после первых двух этапов, а N это его длина, гарантированно кратная 16

Этап 3. Инициализация буфера MD

слово A: 01 23 45 67

слово B: 89 ab cd ef

слово C: fe dc ba 98

слово D: 76 54 32 10

Этап 4. Обработка сообщения блоками по 16 слов

1-й раунд: $FunF(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$,

2-й раунд: $FunG(X,Y,Z) = (X \wedge Z) \vee (\neg Z \wedge Y)$,

3-й раунд: $FunH(X,Y,Z) = X \oplus Y \oplus Z$,

4-й раунд: $FunI(X,Y,Z) = Y \oplus (\neg Z \vee X)$,

где $\oplus$, $\wedge$, $\vee$, $\neg$ побитовые логические операции **XOR**, **AND**, **OR** и **NOT** соответственно

$$\mathbf{T[n] = 2^{32} * |\sin n|}$$

Этап 4. Обработка сообщения блоками по 16 слов

Этап 1

```
/* [abcd k s i] a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s). */
[ABCD  0 7  1][DABC  1 12  2][CDAB  2 17  3][BCDA  3 22  4]
[ABCD  4 7  5][DABC  5 12  6][CDAB  6 17  7][BCDA  7 22  8]
[ABCD  8 7  9][DABC  9 12 10][CDAB 10 17 11][BCDA 11 22 12]
[ABCD 12 7 13][DABC 13 12 14][CDAB 14 17 15][BCDA 15 22 16]
```

Этап 2

```
/* [abcd k s i] a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s). */
[ABCD  1 5 17][DABC  6 9 18][CDAB 11 14 19][BCDA  0 20 20]
[ABCD  5 5 21][DABC 10 9 22][CDAB 15 14 23][BCDA  4 20 24]
[ABCD  9 5 25][DABC 14 9 26][CDAB  3 14 27][BCDA  8 20 28]
[ABCD 13 5 29][DABC  2 9 30][CDAB  7 14 31][BCDA 12 20 32]
```

Этап 3

```
/* [abcd k s i] a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s). */
[ABCD  5 4 33][DABC  8 11 34][CDAB 11 16 35][BCDA 14 23 36]
[ABCD  1 4 37][DABC  4 11 38][CDAB  7 16 39][BCDA 10 23 40]
[ABCD 13 4 41][DABC  0 11 42][CDAB  3 16 43][BCDA  6 23 44]
[ABCD  9 4 45][DABC 12 11 46][CDAB 15 16 47][BCDA  2 23 48]
```

Этап 4

```
/* [abcd k s i] a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s). */
[ABCD  0 6 49][DABC  7 10 50][CDAB 14 15 51][BCDA  5 21 52]
[ABCD 12 6 53][DABC  3 10 54][CDAB 10 15 55][BCDA  1 21 56]
[ABCD  8 6 57][DABC 15 10 58][CDAB  6 15 59][BCDA 13 21 60]
[ABCD  4 6 61][DABC 11 10 62][CDAB  2 15 63][BCDA  9 21 64]
```

Этап 5. Вывод

MD5:

младший A ...

A9990CD6D22117C1D4E3 ...

C5E9CF2FC5AA20305143 ...

... старший D

Итоги

Рассмотрели:

- Применение MD5
- Устройство MD5