

Tema de hoje: trabalho prático

message digest

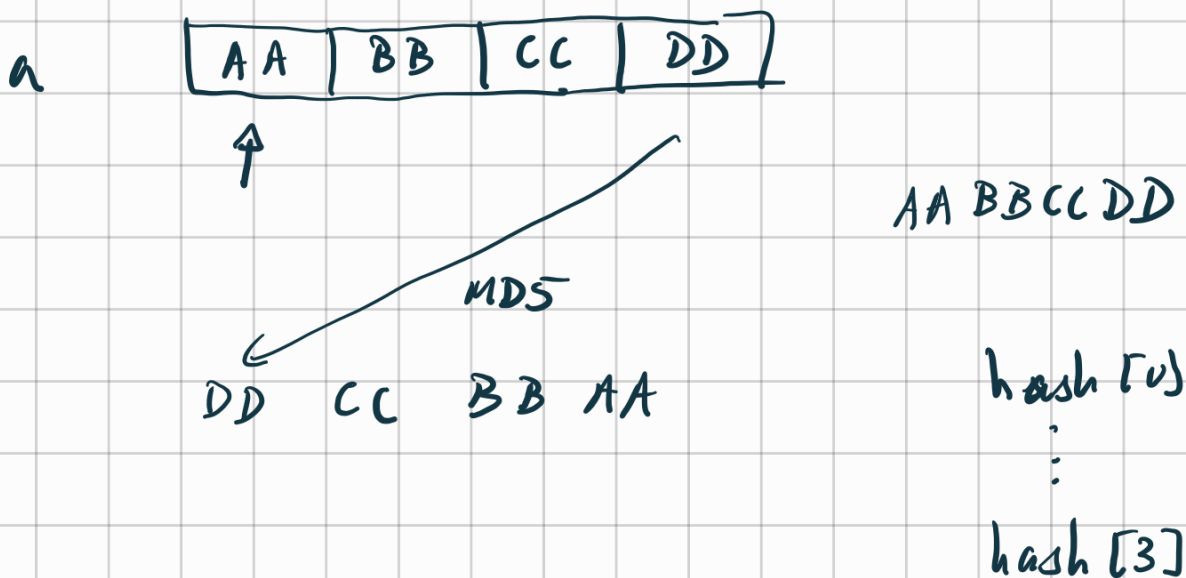
Ficheiro →  
hash

"Assinatura"

MD5

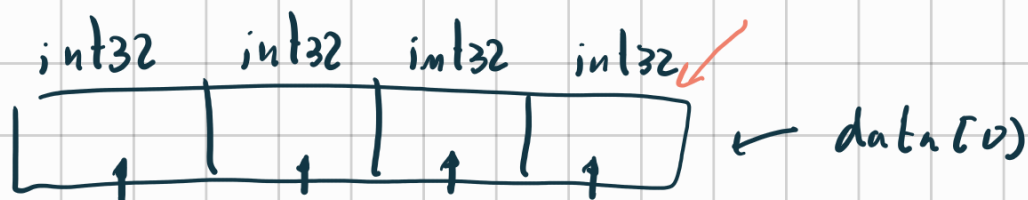
DETIL coins

```
fprintf(stdout, "%08X", a);
```

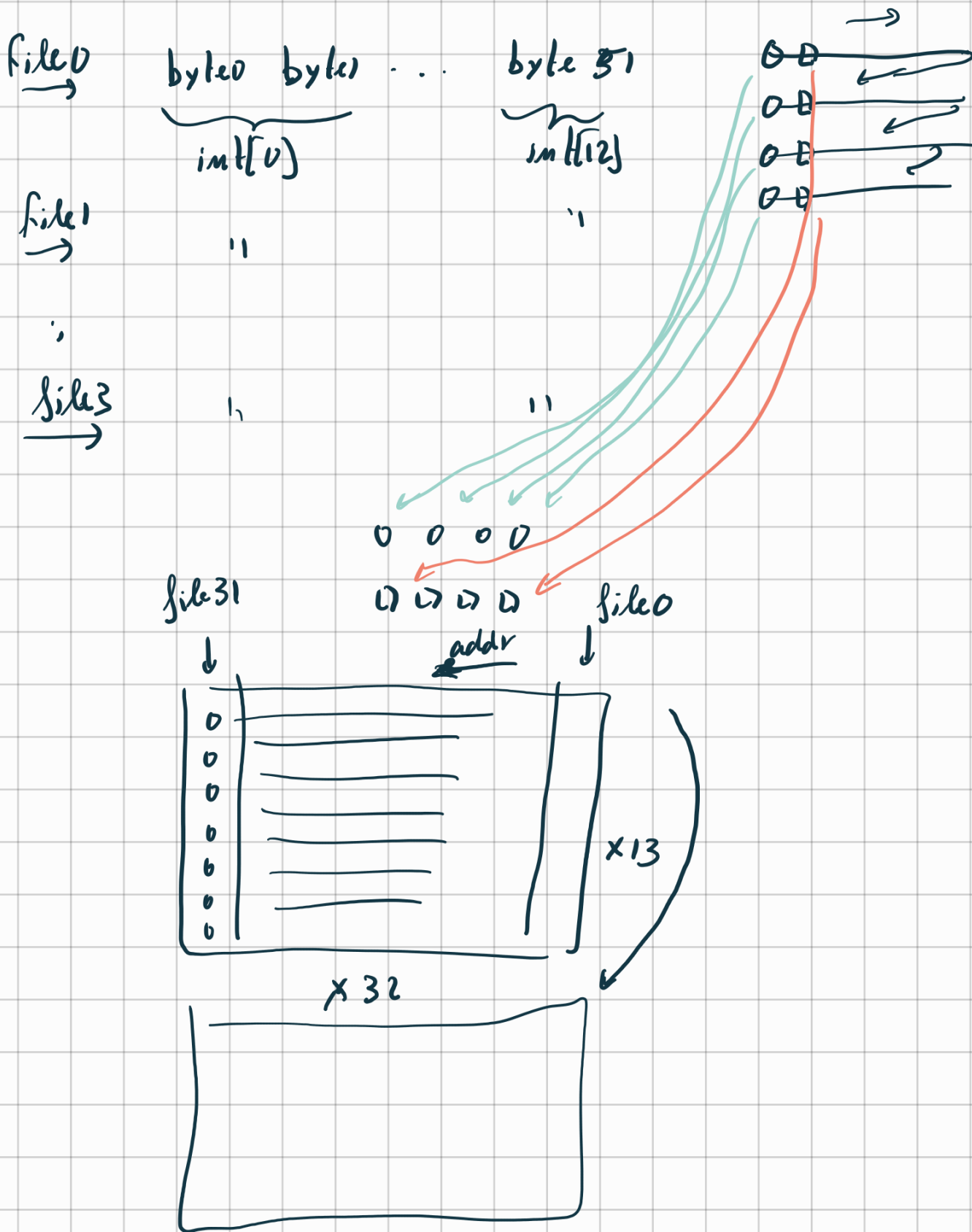


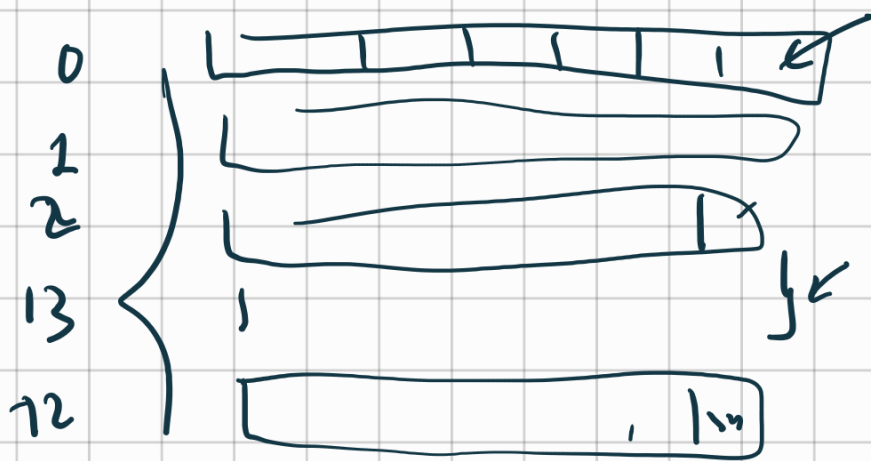
AVX

Registos SIMD (128-bits), AVX, NEON



## Inicialmente





$$DETI$$

$$coin$$

$$'D' + ('E' \ll 8) +$$

$$((T' \ll 16) + \dots) \ll 24$$

data[2]

$$0x206E + (\downarrow) \ll 16$$

$$\begin{matrix} '0' \\ '1' \\ '2' \\ '3' \end{matrix}$$

$$\Leftrightarrow 0x7E$$

$$'' \Leftrightarrow 0x20$$

$$'' + (n \% 32)$$



$$u = '' + (n).64)$$

$$n /= 64;$$

$$u += (('' + (n).64)) \ll 8;$$

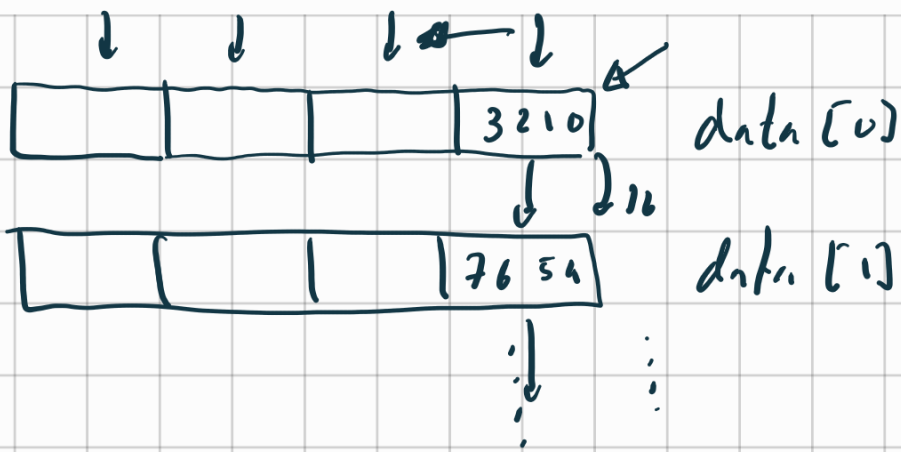
⋮

$$data[3] = u;$$

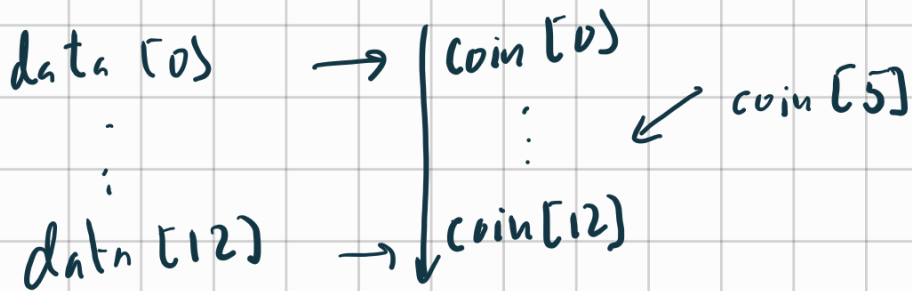
$$data[4] = '' + idx;$$

$$64 \times 64 \times 64 \times 64$$

$$\underline{\underline{2^{24}}}$$



data[0] = c(0x49544544);  
 ↑ ↑ ↑ ↑  
 'T' 'T' 'E' 'D'  
 { x, x, x, x };



coin[5] = 0x20202020;  
 20202021  
 ...  
 2020207E  
 20202120  
 ...  
 20207E7E  
 20212020  
 ...  
 7E7E7E7E

07 bits

02020202

`printf("%.08X", a);`

`a = 0x`

44	33	22	11
----	----	----	----

↑

11      22      33      44