AAD 2024-11-04

Tema de hoje: trabalho prático

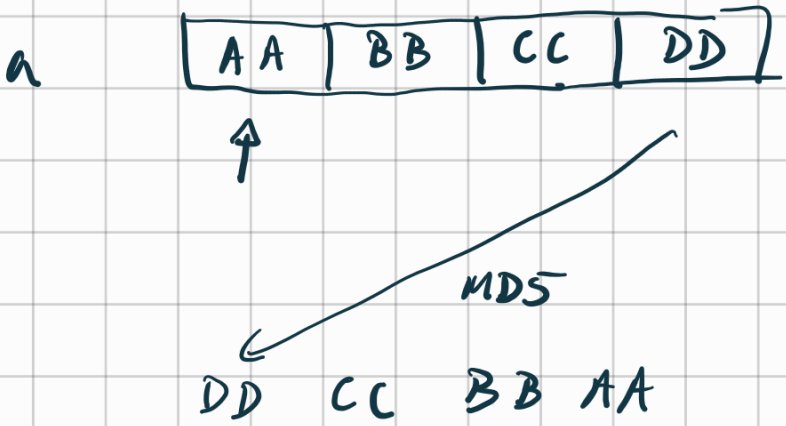
message digest

Ficheiro → hash → "Assinatura"

MD5

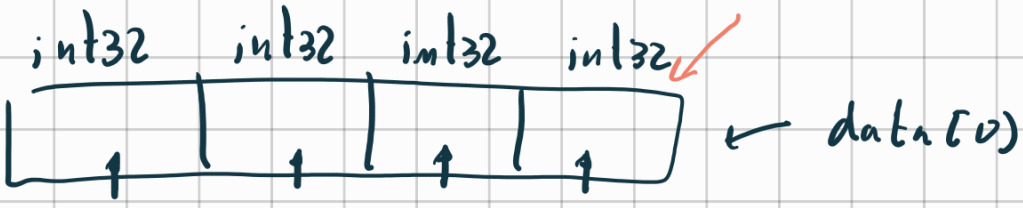
DETI coins

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

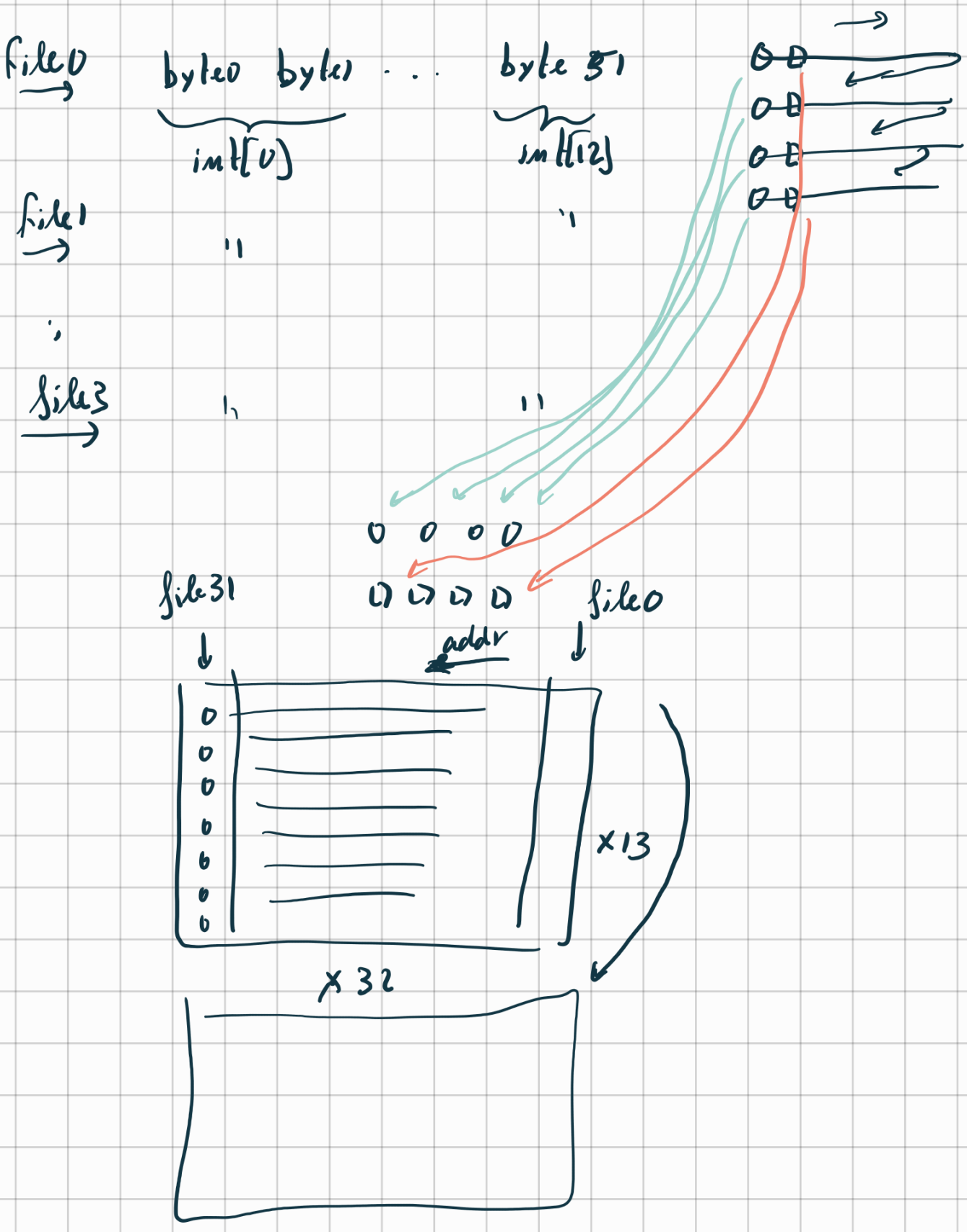


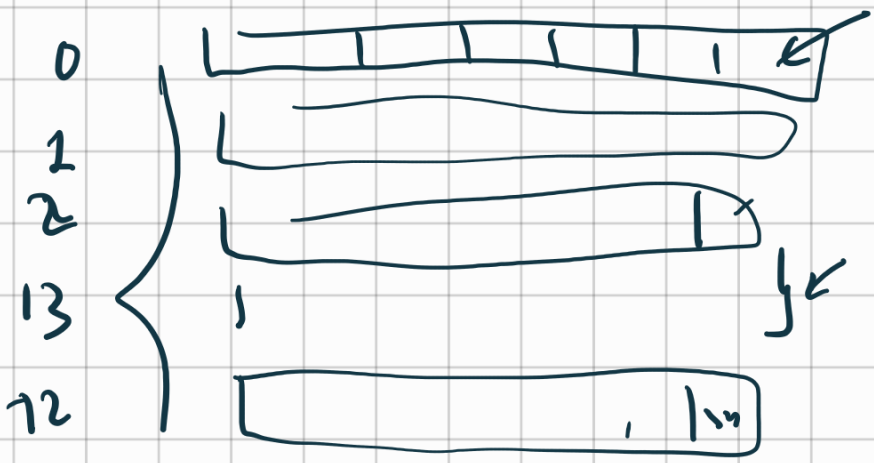
AVX

Registos SIMD (128-bits), AVX, NEON



Inicial mente





DETI

coin 'D' + ('E'<<8) +

(('T'<<16) + ('I'<<24)

data[2]

0x206E + ( ) << 16

'0'
'1'
'2'
'13'

↔ 0x7E

' ' ↔ 0x20

' ' + (n%32)

n = ' ' + (n/64)

64 x 64 x 64 x 64

2^{24}

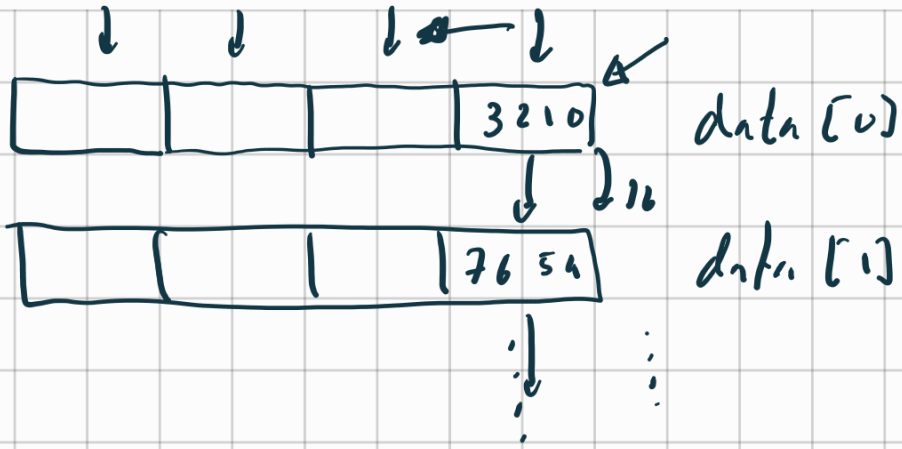
n /= 64;

n += (' ' + (n/64)) << 8;

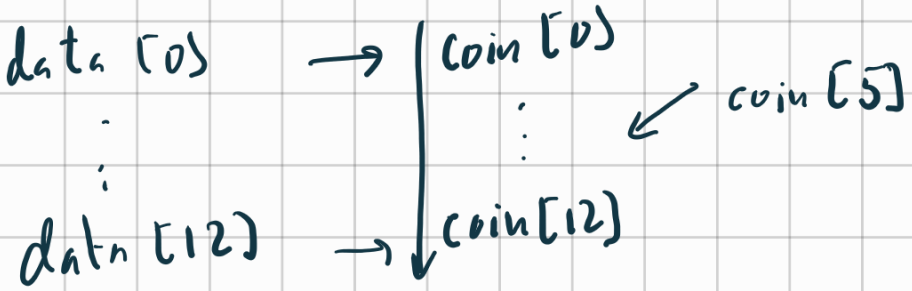
⋮

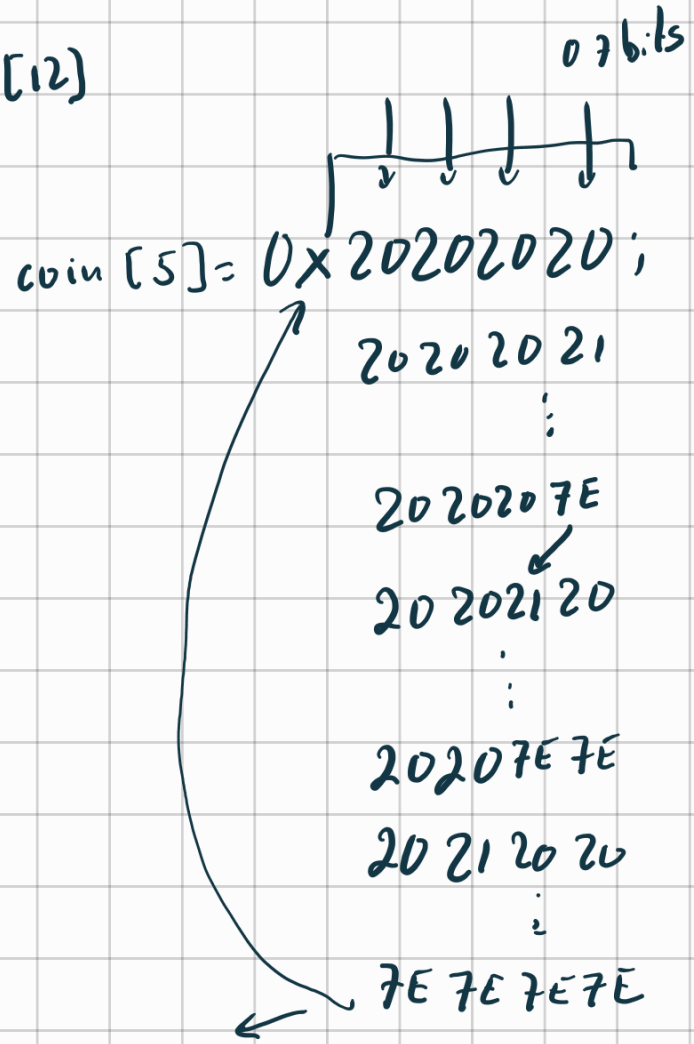
data[3] = n;

data[4] = ' ' + idx;



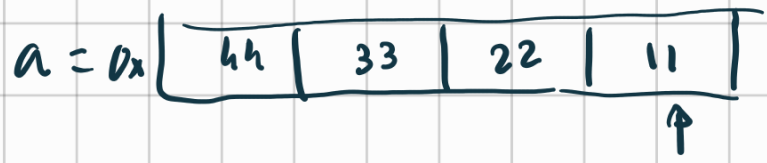

```
data[0]= c(0x49544544);
           ↑ ↑ ↑ 'D'
         'T' 'T' 'E'
{x,x,x,x};
```





02020202

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



11 22 33 44