困难一：如果 ucore 的缺页服务例程在执行过程中访问内存，出现了页访问异常，请问硬件要做哪些事情？

对于这个问题，我一开始的想法就是：缺页服务例程出现页访问异常，那么就会再次执行缺页服务例程，然后又会出现页访问异常.....然后就会进入死循环，一直陷入在缺页服务例程与页访问异常这个死循环里面，然后我就不知道硬件应该做什么事。

后来发现我弄错了，我把缺页的处理与页访问异常的处理弄混了，虽然页访问异常的处理函数里面也有缺页的处理，但只是其中的一种情况，这两种处理机制是不一样的。

这道题的正确做法应该是，硬件的处理与正常的页访问异常处理相一致：

- 将发生错误的线性地址保存在 cr2 寄存器中;
- 在中断栈中依次压入 EFLAGS，CS, EIP，以及页访问异常码 error code，由于 ISR 一定是运行在内核态下的，因此不需要压入 ss 和 esp 以及进行栈的切换；
- 根据中断描述符表查询到对应页访问异常的 ISR，跳转到对应的 ISR 处执行，接下来将由软件进行处理

困难二：页面异常的原因

·目标页面不存在（页表项全为 0，即该线性地址与物理地址尚未建立映射或者已经撤销）;

• 相应的物理页面不在内存中（页表项非空，但 Present 标志位=0，比如在 swap 分区或磁盘文件上）

• 访问权限不符合（此时页表项 P 标志=1，比如企图写只读页面）

吐槽一：这个实验比上一个实验简单一点，逻辑容易理解，代码量也比较小。