题目1

varialbe	start adress
d[1]	0x8049614
d[0].a	0x8049600
d[0].b[1]	0x8049604
d[0].c	0x8049608
d[0].p.y	0x804960c
d[0].p.z	0x804960c
d[0].d	0x8049610

题目2

输出：

do you want a midterm exam?

yes!

题目3

type	size	offset	Alignment
A	24	0,4,8,16	8
B	16	0,8,9,12	8
C	16	0,8	8
D	56	0,48	8
E	12	0,6	2

题目4

由sub $40 %esp，知道开辟了40个字节的空间用于存储，则只需要做到修改返回地址即可。

假设通过password的get来实现，那么得到的字符串会从%ebp的位置开始。距离ret addr 有32个字节，所以可以输入一个长度为32的字符串，后面加上`\xda\x13\x04\x08`来实现。

一个输入示例可以为:
`12345678901234567890123456\xda\x13\x04\x08`

前28个字符用于占位置，从而到达需要改变的返回地址位置。