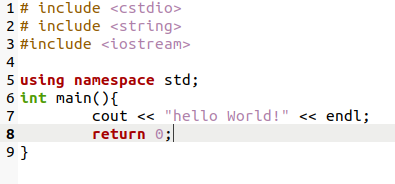
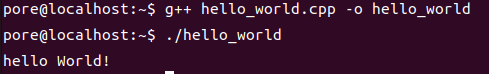
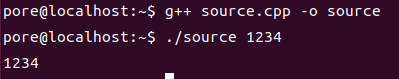
Task1

1.

2. 

Task2：



class A size(112):

+---

0 | {vfptr}

8 | var\_rXRrPQbtbJ

12 | var\_ntiaelLtXC

16 | var\_mWZZfdRLZn

18 | var\_WQCVKCxqgF

| <alignment member> (size=1)

20 | var\_fZvZmrpsfJ

22 | var\_YoHBbyVQiu

| <alignment member> (size=1)

24 | var\_oECYLSEMLd

26 | var\_QgbpAocnJh

28 | var\_nGHeasBnUL

| <alignment member> (size=2)

32 | var\_gBbaaDvuGS

36 | x

40 | var\_OyePZLDhlK

| <alignment member> (size=6)

48 | var\_UvpemeCyRD

56 | var\_mBlidswZEY

64 | var\_JEvkVfhgwT

68 | var\_CmhupsjQwq

72 | var\_EyHFNVrvvg

| <alignment member> (size=4)

80 | var\_xMMJjixEwj

88 | var\_aKPfmBFdkE

96 | var\_FYcQBDFevs

104 | var\_rRaUlSVyAL

| <alignment member> (size=4)

+---

最后A类中的成员变量占据的内存是112byte，因为虽然最后int是4byte，但是要满足整个类的大小必须是里面变量类型大小最大值的整数倍，所以会变成112byte

Task3:



|

0 | &A::func\_DqxjFyoCzy

1 | &A::func\_eRdyLXZKYB

2 | &A::func\_aTBVUZZAWS

3 | &A::func\_xcUDGNovun

4 | &A::func\_nwRMxvBlnI

5 | &A::getX

6 | &A::func\_YeSikHrcKV

7 | &A::func\_kjZmXOTDmO

8 | &A::func\_tldpOoZaYh

9 | &A::func\_VtxnllHbCy

getX()是第六个虚函数，所以偏移量是5

通过\*(long\*)&a强制转换成8个字节，取a对象的前八个地址，得到vptr虚表地址，虚表中每个元素是8个字节，\*（long\*）\*（long\*）&a就是表的第一个元素，考虑到getX（）的偏移量是5，所以最终get（）的虚函数地址就是\*(((long\*)\*(long\*)(&a))+5)