```
lea.
        edx. [ebx+13h]
add
        [esp+4Ch+var_20], edx
mov
        [esp+4Ch+dest], edx
mov
        [esp+4Ch+n], 0A14h
mov
        [esp+4Ch+src], offset aT1_lib_c; "t1_lib.c"
mov
        CRYPTO malloc
call.
        byte ptr [eax], 2
mov
mov
        ebp, eax
        eax, ebx
mov
shr
        eax, 8
        [ebp+2], b1
mov
        edx, [ebp+3]
lea
        [ebp+1], al
mov
mov
        [esp+4Ch+n], ebx; n
        [esp+4Ch+dest], edx; dest
mov
        [esp+4Ch+var_24], edx
mov
        [esp+4Ch+src], edi; src
mov
                                call memcpy
call
        edx, [esp+4Ch+var_24]
mov
        [esp+4Ch+src], 10h
mov
add
        ebx, edx
mov
        [esp+4Ch+dest], ebx
call.
        RAND_pseudo_bvtes
        edx, [esp+4Ch+var_20]
mov
        [esp+4Ch+n], ebp
mov
        [esp+4Ch+src], 18h
mov
        [esp+4Ch+dest], esi
mov
        [esp+4Ch+var_40], edx
mov
call
        ssl3_write_bytes
test
        eax. eax
js,
        short loc_80B7920
```

```
eax, [ebx+13h]
                                             [esp+4Ch+var_20], eax
                                    mov
                                             [esp+4Ch+var_44], 0A14h
[esp+4Ch+var_48], offset aT1_lib_c; "t1_lib.c"
                                             [esp+4Ch+var_4C], eax
                                    mov
                                    call
                                             _CRYPTO_malloc
                                    mov
                                             ed×, ea×
                                    mov
                                             byte ptr [eax], 2
                                    mov
                                             eax, ebx
                                    shr
                                             eax, 8
                                             [edx+1], al
                                             [edx+2]́, b1
                                     MOV
                                             eax, [edx+3]
                                             [esp+4Ch+var_24], eax
[esp+4Ch+var_2C], ebx
                                             [esp+4Ch+var_28], eax
                                     MOV
                                             esi', [edi+3]
                                             еЬх, 4
                                             1oc_4856E0
             хог
                     byté ptr [esp+4Ch+var_2C], 2
             test
                                                                                              short loc_48571A
             jz
                     short loc_485642
                                                                        al, [edi+3]
                                                               moν
                                                                        [edx+3], a1
                                                               mov
                                     cx, [esi]
                                                                        eax, [edx+4]
                                                               1ea
                                     eax, [esp+4Ch+var_28]
                                                                                                           byte ptr [esp+4Ch+var_28], 2
                             mov
                                                               mov
                                                                        [esp+4Ch+var_28], eax
                                                                                                 test
                                     [eax], cx
                             mov
                                                               1ea
                                                                        esi', [edi+4]
                                                                                                           short' loc_485701
                                     есх, 2
                                                                        eax, [ebx-1]
                                                               1ea
                                                                        [esp+4Ch+var_2C], eax
                                                               moν
                                                                        short loc_4856E4
                                                               jmp
                                                                                                  cx, [esi]
                                                                ecx, [esp+4Ch+var_2C]
                                                       moν
                                                                                                  eax, [esp+4Ch+var_28]
[eax], cx
                                                        shr
                      byte ptr [esp+4Ch+var_2C], 1
                                                                edi, [esp+4Ch+var_28]
                                                       moν
                                                                                                   [esp+4Ch+var_28], 2
                      short loc_485657
                                                       rep movsd
                                                                                                  esi', 2
                                                                [esp+4Ch+var_28], edi
                                                        moν
                                                                                                   [esp+4Ch+var_2C], 2
                                                                1oc_48562A
                                                                                                   short loc_4856EB
          al, [esi+ecx]
 mov
          byte ptr [esp+4Ch+var_2C], al
mov
                                                               Inlined memcpy function
ı mav
          eďi, [esp+4Ch+var_28]
 mov
          [edi+ecx], al
                          [esp+4Ch+var_2C], edx
[esp+4Ch+var_48], 10h
                 mov
                 mov.
                 add
                          ebx, [esp+4Ch+var_24]
                 mov
                          [esp+4Ch+var_4C], ebx
```

call _RAND_pseudo_bytes eb×, [esp+4Ch+var_20] mov [esp+4Ch+var_40], ebx mov. edx, [esp+4Ch+var_2C] mov. lmov. [esp+4Ch+var_44], ed× [esp+4Ch+var_48], 18h [esp+4Ch+var_4C], ebp mov. mov _ss13_write_bytes call test eax, eax edx, [esp+4Ch+var_2C] 1oc_485740

(b)