```
lea.
        edx. [ebx+13h]
add
        edi, 3
        [esp+4Ch+var_20], edx
mov
        [esp+4Ch+dest], edx
mov
mov
        [esp+4Ch+n], 0A14h
        [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], bl
mov
        edx, [ebp+3]
lea.
        [ebp+1], al
mov
mov
        [esp+4Ch+n], ebx; n
        [esp+4Ch+dest], edx; dest
mov
mov
        [esp+4Ch+var_24], edx
        [esp+4Ch+src], edi; src
mov
call.
        _memcpv
        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"
                                    moν
                                    mov
                                             [esp+4Ch+var_4C], eax
                                   mov
                                            _CRYPTO_malloc
                                   call
                                   mov
                                            ed×, ea×
                                   mov
                                            byte ptr [eax], 2
                                   mov
                                            eax, ebx
                                    shr
                                            eax. 8
                                            [edx+1], al
[edx+2], bl
                                    mov
                                    mov
                                    lea
                                            eax, [edx+3]
                                            [esp+4Ch+var_24], eax
[esp+4Ch+var_2C], ebx
                                    mov
                                    mov
                                             [esp+4Ch+var_28], eax
                                    MOV
                                            ēsi', [edi+3]
                                    lea
                                            еЬ×, 4
                                            loc_4856E0
                                    jnb
           хог
                    ecx, ecx
                                                                                      test
                                                                                               al, 1
                    byté ptr [esp+4Ch+var_2C], 2
           test
                                                                                      jnz
                                                                                               short loc_48571A
           jz
                    short loc_485642
                                                                         al, [edi+3]
                                                                mov
                                                                         [edx+3], a1
                                                                mov
                                     cx, [esi]
                                                                         eax, [edx+4]
                                                                1ea
                                     eax, [esp+4Ch+var_28]
                                                                         [esp+4Ch+var_28], eax
                                                                                                             byte ptr [esp+4Ch+var_28], 2
                            mov
                                                                mov
                                                                                                   test
                            mov
                                     [eax], cx
                                                                1ea
                                                                         esi', [edi+4]
                                                                                                             short' loc_485701
                                     есх, 2
                                                                         eax, [ebx-1]
                                                                1ea
                                                                         [esp+4Ch+var_2C], eax
                                                                mov
                                                                         short 1oc_4856E4
                                                                jmp
                                                                                                    cx, [esi]
                                                       mov
                                                                ecx, [esp+4Ch+var_2C]
                                                                                                    eax, [esp+4Ch+var_28]
[eax], cx
                                                        shr
                    byte ptr [esp+4Ch+var_2C], 1
                                                                edi, [esp+4Ch+var_28]
                                                       moν
            test
                                                                                                    [esp+4Ch+var_28], 2
                                                                                           add
                     short loc_485657
                                                       rep movsd
                                                                                                    esi', 2
                                                                 [esp+4Ch+var_28], edi
                                                        mov
                                                                                                    [esp+4Ch+var_2C], 2
                                                                                           sub
                                                        jmp
                                                                 1oc_48562A
                                                                                                    short loc_4856EB
        al, [esi+ecx]
mov
        byte ptr [esp+4Ch+var_2C], al
mov
        edi, [esp+4Ch+var_28]
moν
        [edi+ecx], al
                         [esp+4Ch+var_2C], ed×
                mov
                         [esp+4Ch+var_48], 10h
                mov.
                         ebx, [esp+4Ch+var_24]
                add
                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]
                                                                           (b)
                mov.
                        [esp+4Ch+var_44], edx
[esp+4Ch+var_48], 18h
[esp+4Ch+var_4C], ebp
                lmov.
                mov
                mov
                         _ss13_write_bytes
                call
                         eax, eax
                test
                         edx, [esp+4Ch+var_2C]
                         loc_485740
```