



INSTITUTO POLITÉCNICO
NACIONAL



ESCUELA SUPERIOR
DE CÓMPUTO

ARQUITECTURA DE COMPUTADORAS

Práctica 2

Alumna: SÁNCHEZ SANDOVAL YERALDI LIZETH
Profesora: VEGA GARCIA NAYELI

CÓDIGO ESCRITO EN C

```
1. #include<stdio.h>
2. #include<stdlib.h>
3. #include<time.h> //Libreria para obtener números random

4. int NElementos(void);
5. void LlenarArreglo(int*, int );
6. void MostrarArregloS(int*, int);
7. void OrdenarArreglo(int*, int);
8. int main(){
9.     int n=NElementos(), A1[n];
10.     LlenarArreglo(A1,n);
11.     MostrarArregloS(A1,n);
12.     OrdenarArreglo(A1,n);
13.     return 0;
14. }
15. int NElementos(){
16.     int n;
17.     printf("Ingrese cuántos elementos contiene su
Arreglo: ");
18.     scanf("%d", &n);
19.     return n;
20. }
21.
22. void LlenarArreglo(int* A1,int n){
23.     int i;
24.     srand(time(NULL)); //Para que te de los números
random usas este
25.     for(i=0; i<n; i++){
26.         A1[i]=1+rand()%9;// Significa que te va a g
enerar números random de 1 al 9
27.         //Inicio+rand()%Hasta dónde
28.     }
29. }
```

CÓDIGO ESCRITO EN C TRADUCIDO A ENSAMBLADOR

a.exe: file format pei-i386

Disassembly of section .text:

00401000 <.text>:

```
401000: 83 ec 1c      sub $0x1c,%esp
401003: 8b 44 24 20   mov 0x20(%esp),%eax
401007: 8b 00         mov (%eax),%eax
401009: 8b 00         mov (%eax),%eax
40100b: 3d 91 00 00 c0      cmp $0xc0000091,%eax
401010: 77 4e         ja 0x401060
401012: 3d 8d 00 00 c0      cmp $0xc000008d,%eax
401017: 73 60         jae 0x401079
401019: 3d 05 00 00 c0      cmp $0xc0000005,%eax
40101e: 0f 85 cc 00 00 00   jne 0x4010f0
401024: c7 44 24 04 00 00 00 movl $0x0,0x4(%esp)
40102b: 00
40102c: c7 04 24 0b 00 00 00 movl $0xb,(%esp)
401033: e8 50 2c 00 00     call 0x403c88
401038: 83 f8 01         cmp $0x1,%eax
40103b: 0f 84 48 01 00 00   je 0x401189
401041: 85 c0           test %eax,%eax
401043: 0f 85 e7 00 00 00   jne 0x401130
401049: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi
401050: 31 c0           xor %eax,%eax
401052: 83 c4 1c         add $0x1c,%esp
401055: c2 04 00        ret $0x4
401058: 90              nop
401059: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi
401060: 3d 94 00 00 c0      cmp $0xc0000094,%eax
401065: 74 49           je 0x4010b0
401067: 3d 96 00 00 c0      cmp $0xc0000096,%eax
40106c: 0f 84 89 00 00 00   je 0x4010fb
401072: 3d 93 00 00 c0      cmp $0xc0000093,%eax
401077: 75 d7           jne 0x401050
401079: c7 44 24 04 00 00 00 movl $0x0,0x4(%esp)
401080: 00
401081: c7 04 24 08 00 00 00 movl $0x8,(%esp)
401088: e8 fb 2b 00 00     call 0x403c88
40108d: 83 f8 01         cmp $0x1,%eax
401090: 0f 84 ad 00 00 00   je 0x401143
401096: 85 c0           test %eax,%eax
401098: 74 b6           je 0x401050
40109a: c7 04 24 08 00 00 00 movl $0x8,(%esp)
4010a1: ff d0          call *%eax
4010a3: b8 ff ff ff ff     mov $0xffffffff,%eax
```

```

4010a8: eb a8          jmp 0x401052
4010aa: 8d b6 00 00 00 00 lea 0x0(%esi),%esi
4010b0: c7 44 24 04 00 00 00 movl $0x0,0x4(%esp)
4010b7: 00
4010b8: c7 04 24 08 00 00 00 movl $0x8,(%esp)
4010bf: e8 c4 2b 00 00 call 0x403c88
4010c4: 83 f8 01      cmp $0x1,%eax
4010c7: 75 cd          jne 0x401096
4010c9: c7 44 24 04 01 00 00 movl $0x1,0x4(%esp)
4010d0: 00
4010d1: c7 04 24 08 00 00 00 movl $0x8,(%esp)
4010d8: e8 ab 2b 00 00 call 0x403c88
4010dd: b8 ff ff ff ff mov $0xffffffff,%eax
4010e2: e9 6b ff ff ff jmp 0x401052
4010e7: 89 f6          mov %esi,%esi
4010e9: 8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
4010f0: 3d 1d 00 00 c0 cmp $0xc000001d,%eax
4010f5: 0f 85 55 ff ff ff jne 0x401050
4010fb: c7 44 24 04 00 00 00 movl $0x0,0x4(%esp)
401102: 00
401103: c7 04 24 04 00 00 00 movl $0x4,(%esp)
40110a: e8 79 2b 00 00 call 0x403c88
40110f: 83 f8 01      cmp $0x1,%eax
401112: 74 59          je 0x40116d
401114: 85 c0          test %eax,%eax
401116: 0f 84 34 ff ff ff je 0x401050
40111c: c7 04 24 04 00 00 00 movl $0x4,(%esp)
401123: ff d0          call *%eax
401125: b8 ff ff ff ff mov $0xffffffff,%eax
40112a: e9 23 ff ff ff jmp 0x401052
40112f: 90             nop
401130: c7 04 24 0b 00 00 00 movl $0xb,(%esp)
401137: ff d0          call *%eax
401139: b8 ff ff ff ff mov $0xffffffff,%eax
40113e: e9 0f ff ff ff jmp 0x401052
401143: c7 44 24 04 01 00 00 movl $0x1,0x4(%esp)
40114a: 00
40114b: c7 04 24 08 00 00 00 movl $0x8,(%esp)
401152: e8 31 2b 00 00 call 0x403c88
401157: c7 04 24 00 00 00 00 movl $0x0,(%esp)
40115e: e8 0d 11 00 00 call 0x402270
401163: b8 ff ff ff ff mov $0xffffffff,%eax
401168: e9 e5 fe ff ff jmp 0x401052
40116d: c7 44 24 04 01 00 00 movl $0x1,0x4(%esp)
401174: 00
401175: c7 04 24 04 00 00 00 movl $0x4,(%esp)
40117c: e8 07 2b 00 00 call 0x403c88
401181: 83 c8 ff      or $0xffffffff,%eax
401184: e9 c9 fe ff ff jmp 0x401052
401189: c7 44 24 04 01 00 00 movl $0x1,0x4(%esp)
401190: 00
401191: c7 04 24 0b 00 00 00 movl $0xb,(%esp)
401198: e8 eb 2a 00 00 call 0x403c88

```

```

40119d: 83 c8 ff      or  $0xffffffff,%eax
4011a0: e9 ad fe ff ff jmp 0x401052
4011a5: 8d 74 26 00   lea 0x0(%esi,%eiz,1),%esi
4011a9: 8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
4011b0: 55            push %ebp
4011b1: 89 e5         mov %esp,%ebp
4011b3: 53            push %ebx
4011b4: 83 ec 14      sub $0x14,%esp
4011b7: a1 cc 50 40 00 mov 0x4050cc,%eax
4011bc: 85 c0         test %eax,%eax
4011be: 74 1c         je 0x4011dc
4011c0: c7 44 24 08 00 00 00 movl $0x0,0x8(%esp)
4011c7: 00
4011c8: c7 44 24 04 02 00 00 movl $0x2,0x4(%esp)
4011cf:00
4011d0: c7 04 24 00 00 00 00 movl $0x0,(%esp)
4011d7: ff d0         call *%eax
4011d9: 83 ec 0c      sub $0xc,%esp
4011dc: c7 04 24 00 10 40 00 movl $0x401000,(%esp)
4011e3: e8 68 2b 00 00 call 0x403d50
4011e8: 83 ec 04      sub $0x4,%esp
4011eb: e8 70 08 00 00 call 0x401a60
4011f0: a1 08 40 40 00 mov 0x404008,%eax
4011f5: 89 04 24      mov %eax,(%esp)
4011f8: e8 73 10 00 00 call 0x402270
4011fd: e8 be 04 00 00 call 0x4016c0
401202: a1 20 70 40 00 mov 0x407020,%eax
401207: 85 c0         test %eax,%eax
401209: 74 42         je 0x40124d
40120b: 8b 1d b8 81 40 00 mov 0x4081b8,%ebx
401211: a3 0c 40 40 00 mov %eax,0x40400c
401216: 89 44 24 04   mov %eax,0x4(%esp)
40121a: 8b 43 10      mov 0x10(%ebx),%eax
40121d: 89 04 24      mov %eax,(%esp)
401220: e8 d3 2a 00 00 call 0x403cf8
401225: a1 20 70 40 00 mov 0x407020,%eax
40122a: 89 44 24 04   mov %eax,0x4(%esp)
40122e: 8b 43 30      mov 0x30(%ebx),%eax
401231: 89 04 24      mov %eax,(%esp)
401234: e8 bf 2a 00 00 call 0x403cf8
401239: a1 20 70 40 00 mov 0x407020,%eax
40123e: 89 44 24 04   mov %eax,0x4(%esp)
401242: 8b 43 50      mov 0x50(%ebx),%eax
401245: 89 04 24      mov %eax,(%esp)
401248: e8 ab 2a 00 00 call 0x403cf8
40124d: e8 ce 2a 00 00 call 0x403d20
401252: 8b 15 0c 40 40 00 mov 0x40400c,%edx
401258: 89 10         mov %edx,(%eax)
40125a: e8 11 0e 00 00 call 0x402070
40125f: 83 e4 f0      and $0xffffffff,%esp
401262: e8 89 09 00 00 call 0x401bf0
401267: e8 bc 2a 00 00 call 0x403d28
40126c: 8b 00         mov (%eax),%eax

```

```

40126e: 89 44 24 08    mov  %eax,0x8(%esp)
401272: a1 00 70 40 00    mov  0x407000,%eax
401277: 89 44 24 04    mov  %eax,0x4(%esp)
40127b: a1 04 70 40 00    mov  0x407004,%eax
401280: 89 04 24       mov  %eax,(%esp)
401283: e8 d8 01 00 00    call 0x401460
401288: 89 c3          mov  %eax,%ebx
40128a: e8 89 2a 00 00    call 0x403d18
40128f: 89 1c 24       mov  %ebx,(%esp)
401292: e8 19 2b 00 00    call 0x403db0
401297: 89 f6          mov  %esi,%esi
401299: 8d bc 27 00 00 00 00 lea  0x0(%edi,%eiz,1),%edi
4012a0: 83 ec 3c       sub  $0x3c,%esp
4012a3: 8d 44 24 2c    lea  0x2c(%esp),%eax
4012a7: c7 44 24 04 00 70 40 movl $0x407000,0x4(%esp)
4012ae: 00
4012af: c7 04 24 04 70 40 00 movl $0x407004,(%esp)
4012b6: c7 44 24 2c 00 00 00 movl $0x0,0x2c(%esp)
4012bd: 00
4012be: 89 44 24 10    mov  %eax,0x10(%esp)
4012c2: a1 04 40 40 00    mov  0x404004,%eax
4012c7: 83 e0 01       and  $0x1,%eax
4012ca: 89 44 24 0c    mov  %eax,0xc(%esp)
4012ce: 8d 44 24 28    lea  0x28(%esp),%eax
4012d2: 89 44 24 08    mov  %eax,0x8(%esp)
4012d6: e8 55 2a 00 00    call 0x403d30
4012db: 83 c4 3c       add  $0x3c,%esp
4012de: c3            ret
4012df: 90            nop
4012e0: 83 ec 1c       sub  $0x1c,%esp
4012e3: c7 04 24 01 00 00 00 movl $0x1,(%esp)
4012ea: ff 15 a4 81 40 00    call *0x4081a4
4012f0: e8 bb fe ff ff    call 0x4011b0
4012f5: 8d 74 26 00    lea  0x0(%esi,%eiz,1),%esi
4012f9: 8d bc 27 00 00 00 00 lea  0x0(%edi,%eiz,1),%edi
401300: 83 ec 1c       sub  $0x1c,%esp
401303: c7 04 24 02 00 00 00 movl $0x2,(%esp)
40130a: ff 15 a4 81 40 00    call *0x4081a4
401310: e8 9b fe ff ff    call 0x4011b0
401315: 8d 74 26 00    lea  0x0(%esi,%eiz,1),%esi
401319: 8d bc 27 00 00 00 00 lea  0x0(%edi,%eiz,1),%edi
401320: ff 25 d0 81 40 00    jmp  *0x4081d0
401326: 8d 76 00       lea  0x0(%esi),%esi
401329: 8d bc 27 00 00 00 00 lea  0x0(%edi,%eiz,1),%edi
401330: ff 25 c0 81 40 00    jmp  *0x4081c0
401336: 90            nop
401337: 90            nop
401338: 90            nop
401339: 90            nop
40133a: 90            nop
40133b: 90            nop
40133c: 90            nop
40133d: 90            nop

```

```

40133e: 90          nop
40133f: 90          nop
401340: 55          push %ebp
401341: 89 e5       mov %esp,%ebp
401343: 56          push %esi
401344: 53          push %ebx
401345: 83 ec 10    sub $0x10,%esp
401348: c7 04 24 00 50 40 00    movl $0x405000,(%esp)
40134f: e8 24 2a 00 00    call 0x403d78
401354: 83 ec 04    sub $0x4,%esp
401357: 85 c0       test %eax,%eax
401359: 0f 84 b1 00 00 00    je 0x401410
40135f: c7 04 24 00 50 40 00    movl $0x405000,(%esp)
401366: 89 c3       mov %eax,%ebx
401368: e8 eb 29 00 00    call 0x403d58
40136d: 83 ec 04    sub $0x4,%esp
401370: a3 6c 70 40 00    mov %eax,0x40706c
401375: c7 44 24 04 13 50 40    movl $0x405013,0x4(%esp)
40137c: 00
40137d: 89 1c 24     mov %ebx,(%esp)
401380: e8 eb 29 00 00    call 0x403d70
401385: 83 ec 08    sub $0x8,%esp
401388: 89 c6       mov %eax,%esi
40138a: c7 44 24 04 29 50 40    movl $0x405029,0x4(%esp)
401391: 00
401392: 89 1c 24     mov %ebx,(%esp)
401395: e8 d6 29 00 00    call 0x403d70
40139a: 83 ec 08    sub $0x8,%esp
40139d: a3 00 40 40 00    mov %eax,0x404000
4013a2: 85 f6       test %esi,%esi
4013a4: 74 11       je 0x4013b7
4013a6: c7 44 24 04 08 70 40    movl $0x407008,0x4(%esp)
4013ad: 00
4013ae: c7 04 24 b8 60 40 00    movl $0x4060b8,(%esp)
4013b5: ff d6       call *%esi
4013b7: a1 18 40 40 00    mov 0x404018,%eax
4013bc: 85 c0       test %eax,%eax
4013be: 74 3a       je 0x4013fa
4013c0: c7 04 24 41 50 40 00    movl $0x405041,(%esp)
4013c7: e8 ac 29 00 00    call 0x403d78
4013cc: 83 ec 04    sub $0x4,%esp
4013cf: 85 c0       test %eax,%eax
4013d1: ba 00 00 00 00    mov $0x0,%edx
4013d6: 74 15       je 0x4013ed
4013d8: c7 44 24 04 4f 50 40    movl $0x40504f,0x4(%esp)
4013df: 00
4013e0: 89 04 24     mov %eax,(%esp)
4013e3: e8 88 29 00 00    call 0x403d70
4013e8: 83 ec 08    sub $0x8,%esp
4013eb: 89 c2       mov %eax,%edx
4013ed: 85 d2       test %edx,%edx
4013ef: 74 09       je 0x4013fa
4013f1: c7 04 24 18 40 40 00    movl $0x404018,(%esp)

```

```

4013f8:      ff d2      call  *%edx
4013fa:c7 04 24 30 14 40 00    movl  $0x401430,(%esp)
401401:      e8 1a ff ff ff    call  0x401320
401406:      8d 65 f8      lea   -0x8(%ebp),%esp
401409:      5b            pop   %ebx
40140a:      5e            pop   %esi
40140b:      5d            pop   %ebp
40140c:      c3            ret
40140d:      8d 76 00      lea   0x0(%esi),%esi
401410:      c7 05 00 40 40 00 00    movl  $0x0,0x404000
401417:      00 00 00
40141a:      be 00 00 00 00      mov  $0x0,%esi
40141f:      eb 81          jmp  0x4013a2
401421:      eb 0d          jmp  0x401430
401423:      90            nop
401424:      90            nop
401425:      90            nop
401426:      90            nop
401427:      90            nop
401428:      90            nop
401429:      90            nop
40142a:      90            nop
40142b:      90            nop
40142c:      90            nop
40142d:      90            nop
40142e:      90            nop
40142f:      90            nop
401430:      55            push  %ebp
401431:      89 e5          mov  %esp,%ebp
401433:      83 ec 18       sub  $0x18,%esp
401436:      a1 00 40 40 00      mov  0x404000,%eax
40143b:      85 c0          test %eax,%eax
40143d:      74 09          je   0x401448
40143f:      c7 04 24 b8 60 40 00    movl  $0x4060b8,(%esp)
401446:      ff d0          call *%eax
401448:      a1 6c 70 40 00      mov  0x40706c,%eax
40144d:      85 c0          test %eax,%eax
40144f:      74 0b          je   0x40145c
401451:      89 04 24       mov  %eax,(%esp)
401454:      e8 37 29 00 00      call 0x403d90
401459:      83 ec 04       sub  $0x4,%esp
40145c:      c9            leave
40145d:      c3            ret
40145e:      90            nop
40145f:      90            nop
401460:      8d 4c 24 04      lea   0x4(%esp),%ecx
401464:      83 e4 f0        and  $0xffffffff,%esp
401467:      ff 71 fc        pushl -0x4(%ecx)
40146a:      55            push  %ebp
40146b:      89 e5          mov  %esp,%ebp
40146d:      53            push  %ebx
40146e:      51            push  %ecx
40146f:      83 ec 20       sub  $0x20,%esp

```



```

401472:    e8 79 07 00 00        call 0x401bf0
401477:    89 e0                mov  %esp,%eax
401479:    89 c3                mov  %eax,%ebx
40147b:    e8 85 00 00 00        call 0x401505
401480:    89 45 f4            mov  %eax,-0xc(%ebp)
401483:    8b 45 f4            mov  -0xc(%ebp),%eax
401486:    8d 50 ff            lea  -0x1(%eax),%edx
401489:    89 55 f0            mov  %edx,-0x10(%ebp)
40148c:    c1 e0 02            shl  $0x2,%eax
40148f:    8d 50 03            lea  0x3(%eax),%edx
401492:    b8 10 00 00 00        mov  $0x10,%eax
401497:    83 e8 01            sub  $0x1,%eax
40149a:    01 d0                add  %edx,%eax
40149c:    b9 10 00 00 00        mov  $0x10,%ecx
4014a1:    ba 00 00 00 00        mov  $0x0,%edx
4014a6:    f7 f1                div  %ecx
4014a8:    6b c0 10            imul $0x10,%eax,%eax
4014ab:    e8 90 0d 00 00        call 0x402240
4014b0:    29 c4                sub  %eax,%esp
4014b2:    8d 44 24 08        lea  0x8(%esp),%eax
4014b6:    83 c0 03            add  $0x3,%eax
4014b9:    c1 e8 02            shr  $0x2,%eax
4014bc:    c1 e0 02            shl  $0x2,%eax
4014bf:    89 45 ec            mov  %eax,-0x14(%ebp)
4014c2:    8b 45 ec            mov  -0x14(%ebp),%eax
4014c5:    8b 55 f4            mov  -0xc(%ebp),%edx
4014c8:    89 54 24 04        mov  %edx,0x4(%esp)
4014cc:    89 04 24            mov  %eax,(%esp)
4014cf: e8 5b 00 00 00        call 0x40152f
4014d4:    8b 45 ec            mov  -0x14(%ebp),%eax
4014d7:    8b 55 f4            mov  -0xc(%ebp),%edx
4014da:    89 54 24 04        mov  %edx,0x4(%esp)
4014de:    89 04 24            mov  %eax,(%esp)
4014e1:    e8 b9 00 00 00        call 0x40159f
4014e6:    8b 45 ec            mov  -0x14(%ebp),%eax
4014e9:    8b 55 f4            mov  -0xc(%ebp),%edx
4014ec:    89 54 24 04        mov  %edx,0x4(%esp)
4014f0:    89 04 24            mov  %eax,(%esp)
4014f3:    e8 e6 00 00 00        call 0x4015de
4014f8:    89 dc                mov  %ebx,%esp
4014fa:90                nop
4014fb:    8d 65 f8            lea  -0x8(%ebp),%esp
4014fe:    59                  pop  %ecx
4014ff: 5b                pop  %ebx
401500:    5d                  pop  %ebp
401501:    8d 61 fc            lea  -0x4(%ecx),%esp
401504:    c3                  ret
401505:    55                  push %ebp
401506:    89 e5                mov  %esp,%ebp
401508:    83 ec 28            sub  $0x28,%esp
40150b:    c7 04 24 64 50 40 00 movl $0x405064,(%esp)
401512:    e8 a1 27 00 00        call 0x403cb8
401517:    8d 45 f4            lea  -0xc(%ebp),%eax

```

```

40151a: 89 44 24 04    mov  %eax,0x4(%esp)
40151e: c7 04 24 94 50 40 00    movl $0x405094,(%esp)
401525: e8 6e 27 00 00    call 0x403c98
40152a: 8b 45 f4        mov  -0xc(%ebp),%eax
40152d: c9             leave
40152e: c3            ret
40152f: 55            push %ebp
401530: 89 e5          mov  %esp,%ebp
401532: 53            push %ebx
401533: 83 ec 24       sub  $0x24,%esp
401536: c7 04 24 00 00 00 00    movl $0x0,(%esp)
40153d: e8 26 27 00 00    call 0x403c68
401542: 89 04 24       mov  %eax,(%esp)
401545: e8 36 27 00 00    call 0x403c80
40154a: c7 45 f4 00 00 00 00    movl $0x0,-0xc(%ebp)
401551: eb 3d          jmp  0x401590
401553: 8b 45 f4       mov  -0xc(%ebp),%eax
401556: 8d 14 85 00 00 00 00    lea  0x0(,%eax,4),%edx
40155d: 8b 45 08       mov  0x8(%ebp),%eax
401560: 8d 1c 02       lea  (%edx,%eax,1),%ebx
401563: e8 40 27 00 00    call 0x403ca8
401568: 89 c1          mov  %eax,%ecx
40156a: ba 39 8e e3 38    mov  $0x38e38e39,%edx
40156f: 89 c8          mov  %ecx,%eax
401571: f7 ea          imul %edx
401573: d1 fa          sar  %edx
401575: 89 c8          mov  %ecx,%eax
401577: c1 f8 1f       sar  $0x1f,%eax
40157a: 29 c2          sub  %eax,%edx
40157c: 89 d0          mov  %edx,%eax
40157e: c1 e0 03       shl  $0x3,%eax
401581: 01 d0          add  %edx,%eax
401583: 29 c1          sub  %eax,%ecx
401585: 89 ca          mov  %ecx,%edx
401587: 8d 42 01       lea  0x1(%edx),%eax
40158a: 89 03          mov  %eax,(%ebx)
40158c: 83 45 f4 01     addl $0x1,-0xc(%ebp)
401590: 8b 45 f4       mov  -0xc(%ebp),%eax
401593: 3b 45 0c       cmp  0xc(%ebp),%eax
401596: 7c bb          jl   0x401553
401598: 90            nop
401599: 83 c4 24       add  $0x24,%esp
40159c: 5b            pop  %ebx
40159d: 5d            pop  %ebp
40159e: c3            ret
40159f: 55            push %ebp
4015a0: 89 e5          mov  %esp,%ebp
4015a2: 83 ec 28       sub  $0x28,%esp
4015a5: c7 45 f4 00 00 00 00    movl $0x0,-0xc(%ebp)
4015ac: eb 25          jmp  0x4015d3
4015ae: 8b 45 f4       mov  -0xc(%ebp),%eax
4015b1: 8d 14 85 00 00 00 00    lea  0x0(,%eax,4),%edx
4015b8: 8b 45 08       mov  0x8(%ebp),%eax

```

```

4015bb:    01 d0      add  %edx,%eax
4015bd:    8b 00      mov  (%eax),%eax
4015bf:    89 44 24 04 mov  %eax,0x4(%esp)
4015c3:    c7 04 24 97 50 40 00 movl $0x405097,(%esp)
4015ca:    e8 e9 26 00 00 call 0x403cb8
4015cf:83 45 f4 01 addl $0x1,-0xc(%ebp)
4015d3:    8b 45 f4    mov  -0xc(%ebp),%eax
4015d6:    3b 45 0c    cmp  0xc(%ebp),%eax
4015d9:    7c d3      jl   0x4015ae
4015db:    90         nop
4015dc:    c9         leave
4015dd:    c3         ret
4015de:    55         push %ebp
4015df:    89 e5      mov  %esp,%ebp
4015e1:    83 ec 28    sub  $0x28,%esp
4015e4:    c7 45 f4 00 00 00 00 movl $0x0,-0xc(%ebp)
4015eb:    eb 10      jmp  0x4015fd
4015ed:    c7 04 24 9c 50 40 00 movl $0x40509c,(%esp)
4015f4:    e8 b7 26 00 00 call 0x403cb0
4015f9:    83 45 f4 01 addl $0x1,-0xc(%ebp)
4015fd:    8b 45 f4    mov  -0xc(%ebp),%eax
401600:    3b 45 0c    cmp  0xc(%ebp),%eax
401603:    7c e8      jl   0x4015ed
401605:    c7 45 f4 00 00 00 00 movl $0x0,-0xc(%ebp)
40160c:    e9 89 00 00 00 jmp  0x40169a
401611:    c7 45 f0 00 00 00 00 movl $0x0,-0x10(%ebp)
401618:    eb 74      jmp  0x40168e
40161a:    8b 45 f0    mov  -0x10(%ebp),%eax
40161d:    8d 14 85 00 00 00 00 lea  0x0(,%eax,4),%edx
401624:    8b 45 08    mov  0x8(%ebp),%eax
401627:    01 d0      add  %edx,%eax
401629:    8b 10      mov  (%eax),%edx
40162b:    8b 45 f4    mov  -0xc(%ebp),%eax
40162e:    8d 0c 85 00 00 00 00 lea  0x0(,%eax,4),%ecx
401635:    8b 45 08    mov  0x8(%ebp),%eax
401638:    01 c8      add  %ecx,%eax
40163a:    8b 00      mov  (%eax),%eax
40163c:    39 c2      cmp  %eax,%edx
40163e:    7e 4a      jle  0x40168a
401640:    8b 45 f0    mov  -0x10(%ebp),%eax
401643:    8d 14 85 00 00 00 00 lea  0x0(,%eax,4),%edx
40164a:    8b 45 08    mov  0x8(%ebp),%eax
40164d:    01 d0      add  %edx,%eax
40164f:    8b 00      mov  (%eax),%eax
401651:    89 45 ec    mov  %eax,-0x14(%ebp)
401654:    8b 45 f0    mov  -0x10(%ebp),%eax
401657:    8d 14 85 00 00 00 00 lea  0x0(,%eax,4),%edx
40165e:    8b 45 08    mov  0x8(%ebp),%eax
401661:    01 c2      add  %eax,%edx
401663:    8b 45 f4    mov  -0xc(%ebp),%eax
401666:    8d 0c 85 00 00 00 00 lea  0x0(,%eax,4),%ecx
40166d:    8b 45 08    mov  0x8(%ebp),%eax
401670:    01 c8      add  %ecx,%eax

```

```

401672:      8b 00      mov  (%eax),%eax
401674:      89 02      mov  %eax,(%edx)
401676:      8b 45 f4    mov  -0xc(%ebp),%eax
401679:      8d 14 85 00 00 00 00    lea  0x0(,%eax,4),%edx
401680:      8b 45 08    mov  0x8(%ebp),%eax
401683:      01 c2      add  %eax,%edx
401685:      8b 45 ec    mov  -0x14(%ebp),%eax
401688:      89 02      mov  %eax,(%edx)
40168a:      83 45 f0 01  addl $0x1,-0x10(%ebp)
40168e:      8b 45 f0    mov  -0x10(%ebp),%eax
401691:      3b 45 0c    cmp  0xc(%ebp),%eax
401694:      7c 84      jl   0x40161a
401696:      83 45 f4 01  addl $0x1,-0xc(%ebp)
40169a:      8b 45 f4    mov  -0xc(%ebp),%eax
40169d:      3b 45 0c    cmp  0xc(%ebp),%eax
4016a0:      0f 8c 6b ff ff ff    jl   0x401611
4016a6:      8b 45 0c    mov  0xc(%ebp),%eax
4016a9:      89 44 24 04    mov  %eax,0x4(%esp)
4016ad:      8b 45 08    mov  0x8(%ebp),%eax
4016b0:      89 04 24    mov  %eax,(%esp)
4016b3:      e8 e7 fe ff ff    call 0x40159f
4016b8:      90          nop
4016b9:      c9          leave
4016ba:      c3          ret
4016bb:      90          nop
4016bc:      66 90      xchg %ax,%ax
4016be:      66 90      xchg %ax,%ax
4016c0:      55          push %ebp
4016c1:      89 e5      mov  %esp,%ebp
4016c3:      57          push %edi
4016c4:      56          push %esi
4016c5:      53          push %ebx
4016c6:      83 ec 4c    sub  $0x4c,%esp
4016c9:      f6 05 04 40 40 00 02    testb $0x2,0x404004
4016d0:      0f 84 ea 02 00 00    je   0x4019c0
4016d6:      e8 ad 26 00 00    call 0x403d88
4016db:      89 65 c4      mov  %esp,-0x3c(%ebp)
4016de:      89 04 24      mov  %eax,(%esp)
4016e1:      89 c6      mov  %eax,%esi
4016e3:      e8 88 25 00 00    call 0x403c70
4016e8:      8d 44 00 11    lea  0x11(%eax,%eax,1),%eax
4016ec:      c1 e8 04      shr  $0x4,%eax
4016ef:      c1 e0 04      shl  $0x4,%eax
4016f2:      e8 49 0b 00 00    call 0x402240
4016f7:      29 c4      sub  %eax,%esp
4016f9:      c7 45 e4 00 00 00 00    movl $0x0,-0x1c(%ebp)
401700:      c7 45 d4 00 00 00 00    movl $0x0,-0x2c(%ebp)
401707:      8d 44 24 10    lea  0x10(%esp),%eax
40170b:      c7 45 d0 00 00 00 00    movl $0x0,-0x30(%ebp)
401712:      89 c2      mov  %eax,%edx
401714:      89 45 cc      mov  %eax,-0x34(%ebp)
401717:      a1 04 40 40 00    mov  0x404004,%eax
40171c:      25 00 44 00 00    and  $0x4400,%eax

```

```

401721: 83 c8 10      or  $0x10,%eax
401724: 89 45 c8      mov  %eax,-0x38(%ebp)
401727: 31 c0        xor  %eax,%eax
401729: 8d b4 26 00 00 00 00  lea  0x0(%esi,%eiz,1),%esi
401730: 83 c6 01      add  $0x1,%esi
401733: 0f be 4e ff   movsbl -0x1(%esi),%ecx
401737: 85 c9        test %ecx,%ecx
401739: 89 cb        mov  %ecx,%ebx
40173b: 74 73        je   0x4017b0
40173d: 80 fb 3f      cmp  $0x3f,%bl
401740: 0f 84 8d 01 00 00     je   0x4018d3
401746: 0f 8f b4 00 00 00     jg   0x401800
40174c: 80 fb 27      cmp  $0x27,%bl
40174f: 0f 84 b0 01 00 00     je   0x401905
401755: 80 fb 2a      cmp  $0x2a,%bl
401758: 0f 84 75 01 00 00     je   0x4018d3
40175e: 80 fb 22      cmp  $0x22,%bl
401761: 0f 85 09 01 00 00     jne  0x401870
401767: 89 c1        mov  %eax,%ecx
401769: d1 f9        sar  %ecx
40176b: 0f 84 d9 02 00 00     je   0x401a4a
401771: 01 d1        add  %edx,%ecx
401773: 83 c2 01      add  $0x1,%edx
401776: c6 42 ff 5c   movb  $0x5c,-0x1(%edx)
40177a: 39 ca        cmp  %ecx,%edx
40177c: 75 f5        jne  0x401773
40177e: 83 7d d4 27   cmpl  $0x27,-0x2c(%ebp)
401782: 0f 84 c9 01 00 00     je   0x401951
401788: a8 01        test $0x1,%al
40178a: 0f 85 c1 01 00 00     jne  0x401951
401790: 83 c6 01      add  $0x1,%esi
401793: 89 ca        mov  %ecx,%edx
401795: 83 75 d4 22   xorl  $0x22,-0x2c(%ebp)
401799: 0f be 4e ff   movsbl -0x1(%esi),%ecx
40179d: 31 c0        xor  %eax,%eax
40179f: c7 45 d0 01 00 00 00  movl  $0x1,-0x30(%ebp)
4017a6: 85 c9        test %ecx,%ecx
4017a8: 89 cb        mov  %ecx,%ebx
4017aa: 75 91        jne  0x40173d
4017ac: 8d 74 26 00  lea  0x0(%esi,%eiz,1),%esi
4017b0: 85 c0        test %eax,%eax
4017b2: 0f 84 99 02 00 00     je   0x401a51
4017b8: 01 d0        add  %edx,%eax
4017ba: 8d b6 00 00 00 00  lea  0x0(%esi),%esi
4017c0: 83 c2 01      add  $0x1,%edx
4017c3: c6 42 ff 5c   movb  $0x5c,-0x1(%edx)
4017c7: 39 c2        cmp  %eax,%edx
4017c9: 75 f5        jne  0x4017c0
4017cb: 39 45 cc      cmp  %eax,-0x34(%ebp)
4017ce: 0f 82 be 01 00 00     jb   0x401992
4017d4: 8b 55 d0      mov  -0x30(%ebp),%edx
4017d7: 85 d2        test %edx,%edx
4017d9: 0f 85 b3 01 00 00     jne  0x401992

```

```

4017df: 8b 45 dc      mov  -0x24(%ebp),%eax
4017e2: a3 04 70 40 00      mov  %eax,0x407004
4017e7: 8b 45 e0      mov  -0x20(%ebp),%eax
4017ea: a3 00 70 40 00      mov  %eax,0x407000
4017ef: 8b 65 c4      mov  -0x3c(%ebp),%esp
4017f2: 8d 65 f4      lea  -0xc(%ebp),%esp
4017f5: 5b           pop  %ebx
4017f6: 5e           pop  %esi
4017f7: 5f           pop  %edi
4017f8: 5d           pop  %ebp
4017f9: c3           ret
4017fa: 8d b6 00 00 00 00    lea  0x0(%esi),%esi
401800: 80 fb 5c      cmp  $0x5c,%bl
401803: 0f 84 ea 00 00 00    je   0x4018f3
401809: 80 fb 7f      cmp  $0x7f,%bl
40180c: 0f 84 c1 00 00 00    je   0x4018d3
401812: 80 fb 5b      cmp  $0x5b,%bl
401815: 75 59         jne  0x401870
401817: f6 05 04 40 40 00 20  testb $0x20,0x404004
40181e: 0f 85 af 00 00 00    jne  0x4018d3
401824: 85 c0         test %eax,%eax
401826: 8d 78 ff      lea  -0x1(%eax),%edi
401829: b9 01 00 00 00      mov  $0x1,%ecx
40182e: 74 32         je   0x401862
401830: 8d 7c 3a 01      lea  0x1(%edx,%edi,1),%edi
401834: 89 d0         mov  %edx,%eax
401836: 8d 76 00      lea  0x0(%esi),%esi
401839: 8d bc 27 00 00 00 00  lea  0x0(%edi,%eiz,1),%edi
401840: 83 c0 01      add  $0x1,%eax
401843: c6 40 ff 5c      movb $0x5c,-0x1(%eax)
401847: 39 f8         cmp  %edi,%eax
401849: 75 f5         jne  0x401840
40184b: 84 c9         test %cl,%cl
40184d: 75 11         jne  0x401860
40184f: 8d 50 01      lea  0x1(%eax),%edx
401852: 88 18         mov  %bl,(%eax)
401854: 31 c0         xor  %eax,%eax
401856: e9 d5 fe ff ff    jmp  0x401730
40185b: 90           nop
40185c: 8d 74 26 00      lea  0x0(%esi,%eiz,1),%esi
401860: 89 c2         mov  %eax,%edx
401862: 8d 42 01      lea  0x1(%edx),%eax
401865: c6 02 7f      movb $0x7f,(%edx)
401868: eb e5         jmp  0x40184f
40186a: 8d b6 00 00 00 00    lea  0x0(%esi),%esi
401870: 85 c0         test %eax,%eax
401872: 8d 3c 02      lea  (%edx,%eax,1),%edi
401875: 0f 84 c8 01 00 00    je   0x401a43
40187b: 90           nop
40187c: 8d 74 26 00      lea  0x0(%esi,%eiz,1),%esi
401880: 83 c2 01      add  $0x1,%edx
401883: c6 42 ff 5c      movb $0x5c,-0x1(%edx)
401887: 39 fa         cmp  %edi,%edx

```

```

401889: 75 f5      jne 0x401880
40188b: 8b 45 d4   mov -0x2c(%ebp),%eax
40188e: 85 c0      test %eax,%eax
401890: 75 35      jne 0x4018c7
401892: a1 98 81 40 00   mov 0x408198,%eax
401897: 83 38 01     cmpl $0x1,(%eax)
40189a: 0f 84 c5 00 00 00   je 0x401965
4018a0: c7 44 24 04 40 00 00   movl $0x40,0x4(%esp)
4018a7: 00
4018a8: 89 0c 24     mov %ecx,(%esp)
4018ab: 89 4d c0     mov %ecx,-0x40(%ebp)
4018ae: e8 4d 24 00 00   call 0x403d00
4018b3: 85 c0      test %eax,%eax
4018b5: 0f 85 bb 00 00 00   jne 0x401976
4018bb: 8b 4d c0     mov -0x40(%ebp),%ecx
4018be: 83 f9 09     cmp $0x9,%ecx
4018c1: 0f 84 af 00 00 00   je 0x401976
4018c7: 8d 57 01     lea 0x1(%edi),%edx
4018ca: 88 1f      mov %bl,(%edi)
4018cc: 31 c0      xor %eax,%eax
4018ce: e9 5d fe ff ff   jmp 0x401730
4018d3: 85 c0      test %eax,%eax
4018d5: 8d 78 ff     lea -0x1(%eax),%edi
4018d8: 0f 84 4e 01 00 00   je 0x401a2c
4018de: 8b 45 d4   mov -0x2c(%ebp),%eax
4018e1: 83 f9 7f     cmp $0x7f,%ecx
4018e4: 0f 94 c1     sete %cl
4018e7: 85 c0      test %eax,%eax
4018e9: 0f 95 c0     setne %al
4018ec: 09 c1      or %eax,%ecx
4018ee: e9 3d ff ff ff   jmp 0x401830
4018f3: 83 7d d4 27   cmpl $0x27,-0x2c(%ebp)
4018f7: 0f 84 e4 00 00 00   je 0x4019e1
4018fd: 83 c0 01     add $0x1,%eax
401900: e9 2b fe ff ff   jmp 0x401730
401905: f6 05 04 40 40 00 10   testb $0x10,0x404004
40190c: 0f 84 5e ff ff ff   je 0x401870
401912: 89 c1      mov %eax,%ecx
401914: d1 f9      sar %ecx
401916: 0f 84 3c 01 00 00   je 0x401a58
40191c: 01 d1      add %edx,%ecx
40191e: 66 90      xchg %ax,%ax
401920: 83 c2 01     add $0x1,%edx
401923: c6 42 ff 5c   movb $0x5c,-0x1(%edx)
401927: 39 ca      cmp %ecx,%edx
401929: 75 f5      jne 0x401920
40192b: 83 7d d4 22   cmpl $0x22,-0x2c(%ebp)
40192f: 0f 84 98 00 00 00   je 0x4019cd
401935: a8 01      test $0x1,%al
401937: 0f 85 90 00 00 00   jne 0x4019cd
40193d: 83 75 d4 27   xorl $0x27,-0x2c(%ebp)
401941: 89 ca      mov %ecx,%edx
401943: 31 c0      xor %eax,%eax

```

```

401945: c7 45 d0 01 00 00 00    movl $0x1,-0x30(%ebp)
40194c: e9 df fd ff ff         jmp 0x401730
401951: 8d 51 01              lea 0x1(%ecx),%edx
401954: c6 01 22             movb $0x22,(%ecx)
401957: 31 c0                xor %eax,%eax
401959: c7 45 d0 01 00 00 00    movl $0x1,-0x30(%ebp)
401960: e9 cb fd ff ff         jmp 0x401730
401965: a1 c4 81 40 00        mov 0x4081c4,%eax
40196a: 8b 00                mov (%eax),%eax
40196c: f6 04 48 40          testb $0x40,(%eax,%ecx,2)
401970: 0f 84 48 ff ff ff     je 0x4018be
401976: 39 7d cc             cmp %edi,-0x34(%ebp)
401979: 72 75              jb 0x4019f0
40197b: 8b 45 d0            mov -0x30(%ebp),%eax
40197e: 85 c0              test %eax,%eax
401980: 75 6e             jne 0x4019f0
401982: 89 fa             mov %edi,%edx
401984: 31 c0             xor %eax,%eax
401986: c7 45 d0 00 00 00 00    movl $0x0,-0x30(%ebp)
40198d: e9 9e fd ff ff         jmp 0x401730
401992: c6 00 00           movb $0x0,(%eax)
401995: 8d 45 d8          lea -0x28(%ebp),%eax
401998: c7 44 24 08 00 00 00    movl $0x0,0x8(%esp)
40199f: 00
4019a0: 89 44 24 0c        mov %eax,0xc(%esp)
4019a4: 8b 45 c8          mov -0x38(%ebp),%eax
4019a7: 89 44 24 04        mov %eax,0x4(%esp)
4019ab: 8b 45 cc          mov -0x34(%ebp),%eax
4019ae: 89 04 24          mov %eax,(%esp)
4019b1: e8 5a 18 00 00     call 0x403210
4019b6: e9 24 fe ff ff     jmp 0x4017df
4019bb: 90                nop
4019bc: 8d 74 26 00        lea 0x0(%esi,%eiz,1),%esi
4019c0: e8 db f8 ff ff     call 0x4012a0
4019c5: 8d 65 f4          lea -0xc(%ebp),%esp
4019c8: 5b                pop %ebx
4019c9: 5e                pop %esi
4019ca: 5f                pop %edi
4019cb: 5d                pop %ebp
4019cc: c3                ret
4019cd: 8d 51 01          lea 0x1(%ecx),%edx
4019d0: c6 01 27          movb $0x27,(%ecx)
4019d3: 31 c0             xor %eax,%eax
4019d5: c7 45 d0 01 00 00 00    movl $0x1,-0x30(%ebp)
4019dc: e9 4f fd ff ff         jmp 0x401730
4019e1: c6 02 5c          movb $0x5c,(%edx)
4019e4: 83 c2 01          add $0x1,%edx
4019e7: e9 44 fd ff ff         jmp 0x401730
4019ec: 8d 74 26 00        lea 0x0(%esi,%eiz,1),%esi
4019f0: 8d 45 d8          lea -0x28(%ebp),%eax
4019f3: c6 07 00          movb $0x0,(%edi)
4019f6: c7 44 24 08 00 00 00    movl $0x0,0x8(%esp)
4019fd: 00

```



```

4019fe:      89 44 24 0c      mov  %eax,0xc(%esp)
401a02:      8b 5d c8          mov  -0x38(%ebp),%ebx
401a05:      89 5c 24 04      mov  %ebx,0x4(%esp)
401a09:      8b 7d cc          mov  -0x34(%ebp),%edi
401a0c:      89 3c 24          mov  %edi,(%esp)
401a0f:e8 fc 17 00 00      call 0x403210
401a14:      89 d8             mov  %ebx,%eax
401a16:      89 fa             mov  %edi,%edx
401a18:      c7 45 d0 00 00 00 00  movl $0x0,-0x30(%ebp)
401a1f:83 c8 01           or   $0x1,%eax
401a22:      89 45 c8          mov  %eax,-0x38(%ebp)
401a25:      31 c0             xor  %eax,%eax
401a27:      e9 04 fd ff ff    jmp  0x401730
401a2c:      8b 45 d4          mov  -0x2c(%ebp),%eax
401a2f:85 c0             test %eax,%eax
401a31:      0f 95 c0          setne %al
401a34:      83 f9 7f          cmp  $0x7f,%ecx
401a37:      0f 94 c1          sete  %cl
401a3a:      09 c1             or   %eax,%ecx
401a3c:      89 d0             mov  %edx,%eax
401a3e:      e9 08 fe ff ff    jmp  0x40184b
401a43:      89 d7             mov  %edx,%edi
401a45:      e9 41 fe ff ff    jmp  0x40188b
401a4a:      89 d1             mov  %edx,%ecx
401a4c:      e9 2d fd ff ff    jmp  0x40177e
401a51:      89 d0             mov  %edx,%eax
401a53:      e9 73 fd ff ff    jmp  0x4017cb
401a58:      89 d1             mov  %edx,%ecx
401a5a:      e9 cc fe ff ff    jmp  0x40192b
401a5f:90               nop
401a60:      9c               pushf
401a61:      9c               pushf
401a62:      58               pop  %eax
401a63:      89 c2             mov  %eax,%edx
401a65:      35 00 00 20 00    xor  $0x200000,%eax
401a6a:      50               push %eax
401a6b:      9d               popf
401a6c:      9c               pushf
401a6d:      58               pop  %eax
401a6e:      9d               popf
401a6f:31 d0            xor  %edx,%eax
401a71:      a9 00 00 20 00    test $0x200000,%eax
401a76:      0f 84 e9 00 00 00  je  0x401b65
401a7c:      53               push %ebx
401a7d:      31 c0            xor  %eax,%eax
401a7f:0f a2           cpuid
401a81:      85 c0            test %eax,%eax
401a83:      0f 84 db 00 00 00  je  0x401b64
401a89:      b8 01 00 00 00    mov  $0x1,%eax
401a8e:      0f a2           cpuid
401a90:      31 c0            xor  %eax,%eax
401a92:      f6 c6 01         test $0x1,%dh
401a95:      74 03            je   0x401a9a

```

```

401a97:      83 c8 01      or  $0x1,%eax
401a9a:      f6 c5 20      test $0x20,%ch
401a9d:      74 05          je  0x401aa4
401a9f:0d 80 00 00 00      or  $0x80,%eax
401aa4:      f6 c6 80      test $0x80,%dh
401aa7:      74 03          je  0x401aac
401aa9:      83 c8 02      or  $0x2,%eax
401aac:      f7 c2 00 00 80 00      test $0x800000,%edx
401ab2:      74 03          je  0x401ab7
401ab4:      83 c8 04      or  $0x4,%eax
401ab7:      f7 c2 00 00 00 01      test $0x1000000,%edx
401abd:      74 6d          je  0x401b2c
401abf:      83 c8 08      or  $0x8,%eax
401ac2:      55            push %ebp
401ac3:      89 e5          mov  %esp,%ebp
401ac5:      81 ec 00 02 00 00      sub  $0x200,%esp
401acb:      83 e4 f0      and  $0xffffffff,%esp
401ace:      0f ae 04 24      fxsave (%esp)
401ad2:      8b 9c 24 c8 00 00 00      mov  0xc8(%esp),%ebx
401ad9:      81 b4 24 c8 00 00 00      xorl $0x13c0de,0xc8(%esp)
401ae0:      de c0 13 00
401ae4:      0f ae 0c 24      fxrstor (%esp)
401ae8:      89 9c 24 c8 00 00 00      mov  %ebx,0xc8(%esp)
401aef:0f ae 04 24      fxsave (%esp)
401af3:87 9c 24 c8 00 00 00      xchg %ebx,0xc8(%esp)
401afa:0f ae 0c 24      fxrstor (%esp)
401afe:33 9c 24 c8 00 00 00      xor  0xc8(%esp),%ebx
401b05:      c9            leave
401b06:      81 fb de c0 13 00      cmp  $0x13c0de,%ebx
401b0c:      75 1e          jne 0x401b2c
401b0e:      f7 c2 00 00 00 02      test $0x2000000,%edx
401b14:      74 03          je  0x401b19
401b16:      83 c8 10      or  $0x10,%eax
401b19:      f7 c2 00 00 00 04      test $0x4000000,%edx
401b1f:      74 03          je  0x401b24
401b21:      83 c8 20      or  $0x20,%eax
401b24:      f6 c1 01      test $0x1,%cl
401b27:      74 03          je  0x401b2c
401b29:      83 c8 40      or  $0x40,%eax
401b2c:      a3 24 70 40 00      mov  %eax,0x407024
401b31:      b8 00 00 00 80      mov  $0x80000000,%eax
401b36:      0f a2          cpuid
401b38:      3d 00 00 00 80      cmp  $0x80000000,%eax
401b3d:      76 25          jbe 0x401b64
401b3f:      b8 01 00 00 80      mov  $0x80000001,%eax
401b44:      0f a2          cpuid
401b46:      31 c0          xor  %eax,%eax
401b48:      85 d2          test %edx,%edx
401b4a:      79 05          jns 0x401b51
401b4c:      b8 00 01 00 00      mov  $0x100,%eax
401b51:      f7 c2 00 00 00 40      test $0x40000000,%edx
401b57:      74 05          je  0x401b5e
401b59:      0d 00 02 00 00      or  $0x200,%eax

```

```

401b5e: 09 05 24 70 40 00      or  %eax,0x407024
401b64: 5b                      pop  %ebx
401b65: f3 c3                  repz ret
401b67: 90                      nop
401b68: 90                      nop
401b69: 90                      nop
401b6a: 90                      nop
401b6b: 90                      nop
401b6c: 90                      nop
401b6d: 90                      nop
401b6e: 90                      nop
401b6f: 90                      nop
401b70: a1 10 40 40 00          mov  0x404010,%eax
401b75: 8b 00                  mov  (%eax),%eax
401b77: 85 c0                  test %eax,%eax
401b79: 74 1f                  je   0x401b9a
401b7b: 83 ec 0c               sub  $0xc,%esp
401b7e: 66 90                  xchg %ax,%ax
401b80: ff d0                  call *%eax
401b82: a1 10 40 40 00          mov  0x404010,%eax
401b87: 8d 50 04              lea  0x4(%eax),%edx
401b8a: 8b 40 04              mov  0x4(%eax),%eax
401b8d: 89 15 10 40 40 00      mov  %edx,0x404010
401b93: 85 c0                  test %eax,%eax
401b95: 75 e9                  jne  0x401b80
401b97: 83 c4 0c               add  $0xc,%esp
401b9a: f3 c3                  repz ret
401b9c: 8d 74 26 00           lea  0x0(%esi,%eiz,1),%esi
401ba0: 53                      push %ebx
401ba1: 83 ec 18               sub  $0x18,%esp
401ba4: 8b 1d f0 3d 40 00      mov  0x403df0,%ebx
401baa: 83 fb ff               cmp  $0xffffffff,%ebx
401bad: 74 21                  je   0x401bd0
401baf: 85 db                  test %ebx,%ebx
401bb1: 74 0c                  je   0x401bbf
401bb3: ff 14 9d f0 3d 40 00   call *0x403df0(,%ebx,4)
401bba: 83 eb 01               sub  $0x1,%ebx
401bbd: 75 f4                  jne  0x401bb3
401bbf: c7 04 24 70 1b 40 00   movl $0x401b70,(%esp)
401bc6: e8 55 f7 ff ff        call 0x401320
401bcb: 83 c4 18               add  $0x18,%esp
401bce: 5b                      pop  %ebx
401bcf:c3                      ret
401bd0: 31 db                  xor  %ebx,%ebx
401bd2: eb 02                  jmp  0x401bd6
401bd4: 89 c3                  mov  %eax,%ebx
401bd6: 8d 43 01              lea  0x1(%ebx),%eax
401bd9: 8b 14 85 f0 3d 40 00   mov  0x403df0(,%eax,4),%edx
401be0: 85 d2                  test %edx,%edx
401be2: 75 f0                  jne  0x401bd4
401be4: eb c9                  jmp  0x401baf
401be6: 8d 76 00              lea  0x0(%esi),%esi
401be9: 8d bc 27 00 00 00 00   lea  0x0(%edi,%eiz,1),%edi

```

```

401bf0:    a1 28 70 40 00        mov  0x407028,%eax
401bf5:    85 c0                 test %eax,%eax
401bf7:    74 07                 je   0x401c00
401bf9:    f3 c3                 repz ret
401bfb:    90                    nop
401bfc:8d 74 26 00        lea  0x0(%esi,%eiz,1),%esi
401c00:    c7 05 28 70 40 00 01  movl $0x1,0x407028
401c07:    00 00 00
401c0a:    eb 94                 jmp  0x401ba0
401c0c:    90                    nop
401c0d:    90                    nop
401c0e:    90                    nop
401c0f:90                    nop
401c10:    83 ec 1c              sub  $0x1c,%esp
401c13:    8b 44 24 24          mov  0x24(%esp),%eax
401c17:    83 f8 03             cmp  $0x3,%eax
401c1a:    74 14                 je   0x401c30
401c1c:    85 c0                 test %eax,%eax
401c1e:    74 10                 je   0x401c30
401c20:    b8 01 00 00 00        mov  $0x1,%eax
401c25:    83 c4 1c              add  $0x1c,%esp
401c28:    c2 0c 00             ret  $0xc
401c2b:    90                    nop
401c2c:    8d 74 26 00          lea  0x0(%esi,%eiz,1),%esi
401c30:    8b 54 24 28          mov  0x28(%esp),%edx
401c34:    89 44 24 04          mov  %eax,0x4(%esp)
401c38:    8b 44 24 20          mov  0x20(%esp),%eax
401c3c:    89 54 24 08          mov  %edx,0x8(%esp)
401c40:    89 04 24             mov  %eax,(%esp)
401c43:    e8 48 02 00 00        call 0x401e90
401c48:    b8 01 00 00 00        mov  $0x1,%eax
401c4d:    83 c4 1c              add  $0x1c,%esp
401c50:    c2 0c 00             ret  $0xc
401c53:    8d b6 00 00 00 00     lea  0x0(%esi),%esi
401c59:    8d bc 27 00 00 00 00  lea  0x0(%edi,%eiz,1),%edi
401c60:    56                    push %esi
401c61:    53                    push %ebx
401c62:    83 ec 14              sub  $0x14,%esp
401c65:    83 3d 64 70 40 00 02  cmpl $0x2,0x407064
401c6c:    8b 44 24 24          mov  0x24(%esp),%eax
401c70:    74 0a                 je   0x401c7c
401c72:    c7 05 64 70 40 00 02  movl $0x2,0x407064
401c79:    00 00 00
401c7c:    83 f8 02             cmp  $0x2,%eax
401c7f:74 12              je   0x401c93
401c81:    83 f8 01             cmp  $0x1,%eax
401c84:    74 3f                 je   0x401cc5
401c86:    83 c4 14              add  $0x14,%esp
401c89:    b8 01 00 00 00        mov  $0x1,%eax
401c8e:    5b                    pop  %ebx
401c8f:5e                    pop  %esi
401c90:    c2 0c 00             ret  $0xc
401c93:    be 14 90 40 00        mov  $0x409014,%esi

```

```

401c98: 81 ee 14 90 40 00    sub  $0x409014,%esi
401c9e: 83 fe 03            cmp  $0x3,%esi
401ca1: 7e e3             jle  0x401c86
401ca3: 31 db            xor  %ebx,%ebx
401ca5: 8b 83 14 90 40 00    mov  0x409014(%ebx),%eax
401cab: 85 c0            test %eax,%eax
401cad: 74 02            je   0x401cb1
401caf: ff d0           call *%eax
401cb1: 83 c3 04          add  $0x4,%ebx
401cb4: 39 de            cmp  %ebx,%esi
401cb6: 75 ed            jne  0x401ca5
401cb8: 83 c4 14          add  $0x14,%esp
401cbb: b8 01 00 00 00     mov  $0x1,%eax
401cc0: 5b              pop  %ebx
401cc1: 5e              pop  %esi
401cc2: c2 0c 00         ret  $0xc
401cc5: 8b 44 24 28       mov  0x28(%esp),%eax
401cc9: c7 44 24 04 01 00 00 movl $0x1,0x4(%esp)
401cd0: 00
401cd1: 89 44 24 08       mov  %eax,0x8(%esp)
401cd5: 8b 44 24 20       mov  0x20(%esp),%eax
401cd9: 89 04 24          mov  %eax,(%esp)
401cdc: e8 af 01 00 00     call 0x401e90
401ce1: eb a3            jmp  0x401c86
401ce3: 8d b6 00 00 00 00 lea  0x0(%esi),%esi
401ce9: 8d bc 27 00 00 00 00 lea  0x0(%edi,%eiz,1),%edi
401cf0: 31 c0           xor  %eax,%eax
401cf2: c3             ret
401cf3: 90             nop
401cf4: 90             nop
401cf5: 90             nop
401cf6: 90             nop
401cf7: 90             nop
401cf8: 90             nop
401cf9: 90             nop
401cfa: 90             nop
401cfb: 90             nop
401cfc: 90             nop
401cfd: 90             nop
401cfe: 90             nop
401cff: 90             nop
401d00: 56             push %esi
401d01: 53             push %ebx
401d02: 83 ec 14        sub  $0x14,%esp
401d05: c7 04 24 44 70 40 00 movl $0x407044,(%esp)
401d0c: e8 a7 20 00 00     call 0x403db8
401d11: 8b 1d 3c 70 40 00    mov  0x40703c,%ebx
401d17: 83 ec 04        sub  $0x4,%esp
401d1a: 85 db            test %ebx,%ebx
401d1c: 74 2d            je   0x401d4b
401d1e: 66 90           xchg %ax,%ax
401d20: 8b 03           mov  (%ebx),%eax
401d22: 89 04 24        mov  %eax,(%esp)

```

```

401d25:    e8 1e 20 00 00        call 0x403d48
401d2a:    83 ec 04              sub $0x4,%esp
401d2d:    89 c6                mov %eax,%esi
401d2f:    e8 4c 20 00 00        call 0x403d80
401d34:    85 c0                test %eax,%eax
401d36:    75 0c                jne 0x401d44
401d38:    85 f6                test %esi,%esi
401d3a:    74 08                je 0x401d44
401d3c:    8b 43 04             mov 0x4(%ebx),%eax
401d3f:    89 34 24             mov %esi,(%esp)
401d42:    ff d0                call *%eax
401d44:    8b 5b 08             mov 0x8(%ebx),%ebx
401d47:    85 db                test %ebx,%ebx
401d49:    75 d5                jne 0x401d20
401d4b:    c7 04 24 44 70 40 00  movl $0x407044,(%esp)
401d52:    e8 09 20 00 00        call 0x403d60
401d57:    83 ec 04              sub $0x4,%esp
401d5a:    83 c4 14             add $0x14,%esp
401d5d:    5b                  pop %ebx
401d5e:    5e                  pop %esi
401d5f:    c3                  ret
401d60:    56                  push %esi
401d61:    53                  push %ebx
401d62:    31 f6                xor %esi,%esi
401d64:    83 ec 14             sub $0x14,%esp
401d67:    a1 40 70 40 00        mov 0x407040,%eax
401d6c:    85 c0                test %eax,%eax
401d6e:    75 10                jne 0x401d80
401d70:    83 c4 14             add $0x14,%esp
401d73:    89 f0                mov %esi,%eax
401d75:    5b                  pop %ebx
401d76:    5e                  pop %esi
401d77:    c3                  ret
401d78:    90                  nop
401d79:    8d b4 26 00 00 00 00  lea 0x0(%esi,%eiz,1),%esi
401d80:    c7 44 24 04 0c 00 00  movl $0xc,0x4(%esp)
401d87:    00
401d88:    c7 04 24 01 00 00 00  movl $0x1,(%esp)
401d8f:    e8 54 1f 00 00        call 0x403ce8
401d94:    85 c0                test %eax,%eax
401d96:    89 c3                mov %eax,%ebx
401d98:    74 41                je 0x401ddb
401d9a:    8b 44 24 20          mov 0x20(%esp),%eax
401d9e:    c7 04 24 44 70 40 00  movl $0x407044,(%esp)
401da5:    89 03                mov %eax,(%ebx)
401da7:    8b 44 24 24          mov 0x24(%esp),%eax
401dab:    89 43 04             mov %eax,0x4(%ebx)
401dae:    e8 05 20 00 00        call 0x403db8
401db3:    a1 3c 70 40 00        mov 0x40703c,%eax
401db8:    83 ec 04              sub $0x4,%esp
401dbb:    89 1d 3c 70 40 00     mov %ebx,0x40703c
401dc1:    c7 04 24 44 70 40 00  movl $0x407044,(%esp)
401dc8:    89 43 08             mov %eax,0x8(%ebx)

```

```

401dcb: e8 90 1f 00 00      call 0x403d60
401dd0: 83 ec 04           sub $0x4,%esp
401dd3: 89 f0             mov %esi,%eax
401dd5: 83 c4 14          add $0x14,%esp
401dd8: 5b              pop %ebx
401dd9: 5e              pop %esi
401dda: c3              ret
401ddb: be ff ff ff ff    mov $0xffffffff,%esi
401de0: eb 8e           jmp 0x401d70
401de2: 8d b4 26 00 00 00 lea 0x0(%esi,%eiz,1),%esi
401de9: 8d bc 27 00 00 00 lea 0x0(%edi,%eiz,1),%edi
401df0: 53             push %ebx
401df1: 83 ec 18        sub $0x18,%esp
401df4: a1 40 70 40 00    mov 0x407040,%eax
401df9: 8b 5c 24 20      mov 0x20(%esp),%ebx
401dfd: 85 c0          test %eax,%eax
401dff: 75 0f          jne 0x401e10
401e01: 83 c4 18        add $0x18,%esp
401e04: 31 c0          xor %eax,%eax
401e06: 5b            pop %ebx
401e07: c3            ret
401e08: 90            nop
401e09: 8d b4 26 00 00 00 lea 0x0(%esi,%eiz,1),%esi
401e10: c7 04 24 44 70 40 movl $0x407044,(%esp)
401e17: e8 9c 1f 00 00    call 0x403db8
401e1c: 8b 15 3c 70 40 00 mov 0x40703c,%edx
401e22: 83 ec 04        sub $0x4,%esp
401e25: 85 d2          test %edx,%edx
401e27: 74 17          je 0x401e40
401e29: 8b 02          mov (%edx),%eax
401e2b: 39 c3          cmp %eax,%ebx
401e2d: 75 0a          jne 0x401e39
401e2f: eb 4e          jmp 0x401e7f
401e31: 8b 08          mov (%eax),%ecx
401e33: 39 d9          cmp %ebx,%ecx
401e35: 74 29          je 0x401e60
401e37: 89 c2          mov %eax,%edx
401e39: 8b 42 08      mov 0x8(%edx),%eax
401e3c: 85 c0          test %eax,%eax
401e3e: 75 f1          jne 0x401e31
401e40: c7 04 24 44 70 40 movl $0x407044,(%esp)
401e47: e8 14 1f 00 00    call 0x403d60
401e4c: 83 ec 04        sub $0x4,%esp
401e4f: 83 c4 18        add $0x18,%esp
401e52: 31 c0          xor %eax,%eax
401e54: 5b            pop %ebx
401e55: c3            ret
401e56: 8d 76 00      lea 0x0(%esi),%esi
401e59: 8d bc 27 00 00 00 lea 0x0(%edi,%eiz,1),%edi
401e60: 8b 48 08      mov 0x8(%eax),%ecx
401e63: 89 4a 08      mov %ecx,0x8(%edx)
401e66: 89 04 24      mov %eax,(%esp)
401e69: e8 72 1e 00 00    call 0x403ce0

```

```

401e6e: c7 04 24 44 70 40 00    movl $0x407044,(%esp)
401e75: e8 e6 1e 00 00          call 0x403d60
401e7a: 83 ec 04                sub $0x4,%esp
401e7d: eb d0                  jmp 0x401e4f
401e7f: 8b 42 08                mov 0x8(%edx),%eax
401e82: a3 3c 70 40 00          mov %eax,0x40703c
401e87: 89 d0                  mov %edx,%eax
401e89: eb db                  jmp 0x401e66
401e8b: 90                      nop
401e8c: 8d 74 26 00            lea 0x0(%esi,%eiz,1),%esi
401e90: 83 ec 1c                sub $0x1c,%esp
401e93: 8b 44 24 24            mov 0x24(%esp),%eax
401e97: 83 f8 01                cmp $0x1,%eax
401e9a: 74 47                  je 0x401ee3
401e9c: 72 17                  jb 0x401eb5
401e9e: 83 f8 03                cmp $0x3,%eax
401ea1: 75 09                  jne 0x401eac
401ea3: a1 40 70 40 00          mov 0x407040,%eax
401ea8: 85 c0                  test %eax,%eax
401eaa: 75 65                  jne 0x401f11
401eac: b8 01 00 00 00          mov $0x1,%eax
401eb1: 83 c4 1c                add $0x1c,%esp
401eb4: c3                      ret
401eb5: a1 40 70 40 00          mov 0x407040,%eax
401eba: 85 c0                  test %eax,%eax
401ebc: 75 62                  jne 0x401f20
401ebe: a1 40 70 40 00          mov 0x407040,%eax
401ec3: 83 f8 01                cmp $0x1,%eax
401ec6: 75 e4                  jne 0x401eac
401ec8: c7 04 24 44 70 40 00    movl $0x407044,(%esp)
401ecf: c7 05 40 70 40 00 00    movl $0x0,0x407040
401ed6: 00 00 00
401ed9: e8 e2 1e 00 00          call 0x403dc0
401ede: 83 ec 04                sub $0x4,%esp
401ee1: eb c9                  jmp 0x401eac
401ee3: a1 40 70 40 00          mov 0x407040,%eax
401ee8: 85 c0                  test %eax,%eax
401eea: 74 14                  je 0x401f00
401eec: c7 05 40 70 40 00 01    movl $0x1,0x407040
401ef3: 00 00 00
401ef6: b8 01 00 00 00          mov $0x1,%eax
401efb: 83 c4 1c                add $0x1c,%esp
401efe: c3                      ret
401eff: 90                      nop
401f00: c7 04 24 44 70 40 00    movl $0x407044,(%esp)
401f07: e8 5c 1e 00 00          call 0x403d68
401f0c: 83 ec 04                sub $0x4,%esp
401f0f: eb db                  jmp 0x401eec
401f11: e8 ea fd ff ff          call 0x401d00
401f16: eb 94                  jmp 0x401eac
401f18: 90                      nop
401f19: 8d b4 26 00 00 00 00    lea 0x0(%esi,%eiz,1),%esi
401f20: e8 db fd ff ff          call 0x401d00

```



```

401f25:    eb 97            jmp 0x401ebe
401f27:    90              nop
401f28:    90              nop
401f29:    90              nop
401f2a:90              nop
401f2b:    90              nop
401f2c:90              nop
401f2d:    90              nop
401f2e:    90              nop
401f2f: 90              nop
401f30:    56              push %esi
401f31:    53              push %ebx
401f32:    83 ec 14        sub $0x14,%esp
401f35:    a1 b8 81 40 00    mov 0x4081b8,%eax
401f3a:c7 44 24 08 17 00 00 movl $0x17,0x8(%esp)
401f41:    00
401f42:    c7 44 24 04 01 00 00 movl $0x1,0x4(%esp)
401f49:    00
401f4a:8d 74 24 24      lea 0x24(%esp),%esi
401f4e:    c7 04 24 d0 50 40 00 movl $0x4050d0,(%esp)
401f55:    8d 58 40        lea 0x40(%eax),%ebx
401f58:    89 5c 24 0c     mov %ebx,0xc(%esp)
401f5c:e8 77 1d 00 00    call 0x403cd8
401f61:    8b 44 24 20     mov 0x20(%esp),%eax
401f65:    89 74 24 08     mov %esi,0x8(%esp)
401f69:    89 1c 24        mov %ebx,(%esp)
401f6c:89 44 24 04     mov %eax,0x4(%esp)
401f70:    e8 e3 1c 00 00    call 0x403c58
401f75:    e8 76 1d 00 00    call 0x403cf0
401f7a:8d b6 00 00 00 00 lea 0x0(%esi),%esi
401f80:    55              push %ebp
401f81:    57              push %edi
401f82:    89 cf           mov %ecx,%edi
401f84:    56              push %esi
401f85:    53              push %ebx
401f86:    89 c3           mov %eax,%ebx
401f88:    89 d6           mov %edx,%esi
401f8a:83 ec 4c        sub $0x4c,%esp
401f8d:    8d 44 24 24     lea 0x24(%esp),%eax
401f91:    c7 44 24 08 1c 00 00 movl $0x1c,0x8(%esp)
401f98:    00
401f99:    89 1c 24        mov %ebx,(%esp)
401f9c:89 44 24 04     mov %eax,0x4(%esp)
401fa0:e8 93 1d 00 00    call 0x403d38
401fa5:83 ec 0c        sub $0xc,%esp
401fa8:85 c0           test %eax,%eax
401faa:0f 84 a8 00 00 00 je 0x402058
401fb0:    8b 44 24 38     mov 0x38(%esp),%eax
401fb4:    83 f8 40        cmp $0x40,%eax
401fb7:    74 05           je 0x401fbe
401fb9:    83 f8 04        cmp $0x4,%eax
401fbc:75 22           jne 0x401fe0
401fbe:    89 7c 24 08     mov %edi,0x8(%esp)

```

```

401fc2:89 74 24 04    mov  %esi,0x4(%esp)
401fc6:89 1c 24        mov  %ebx,(%esp)
401fc9:e8 f2 1c 00 00    call 0x403cc0
401fce:83 c4 4c        add  $0x4c,%esp
401fd1:    5b            pop  %ebx
401fd2:    5e            pop  %esi
401fd3:    5f            pop  %edi
401fd4:    5d            pop  %ebp
401fd5:    c3            ret
401fd6:    8d 76 00      lea  0x0(%esi),%esi
401fd9:    8d bc 27 00 00 00 00 lea  0x0(%edi,%eiz,1),%edi
401fe0:    8b 44 24 30    mov  0x30(%esp),%eax
401fe4:    8d 6c 24 20    lea  0x20(%esp),%ebp
401fe8:    c7 44 24 08 40 00 00 movl $0x40,0x8(%esp)
401fef: 00
401ff0:89 6c 24 0c     mov  %ebp,0xc(%esp)
401ff4:89 44 24 04     mov  %eax,0x4(%esp)
401ff8:8b 44 24 24     mov  0x24(%esp),%eax
401ffc:89 04 24        mov  %eax,(%esp)
401fff:e8 3c 1d 00 00    call 0x403d40
402004:    83 ec 10      sub  $0x10,%esp
402007:    8b 54 24 38    mov  0x38(%esp),%edx
40200b:    89 7c 24 08    mov  %edi,0x8(%esp)
40200f:    89 74 24 04    mov  %esi,0x4(%esp)
402013:    89 1c 24        mov  %ebx,(%esp)
402016:    89 54 24 1c    mov  %edx,0x1c(%esp)
40201a:e8 a1 1c 00 00    call 0x403cc0
40201f:    8b 54 24 1c    mov  0x1c(%esp),%edx
402023:    83 fa 40      cmp  $0x40,%edx
402026:    74 a6        je   0x401fce
402028:    83 fa 04      cmp  $0x4,%edx
40202b:    74 a1        je   0x401fce
40202d:    8b 44 24 20    mov  0x20(%esp),%eax
402031:    89 6c 24 0c    mov  %ebp,0xc(%esp)
402035:    89 44 24 08    mov  %eax,0x8(%esp)
402039:    8b 44 24 30    mov  0x30(%esp),%eax
40203d:    89 44 24 04    mov  %eax,0x4(%esp)
402041:    8b 44 24 24    mov  0x24(%esp),%eax
402045:    89 04 24        mov  %eax,(%esp)
402048:e8 f3 1c 00 00    call 0x403d40
40204d:    83 ec 10      sub  $0x10,%esp
402050:    83 c4 4c      add  $0x4c,%esp
402053:    5b            pop  %ebx
402054:    5e            pop  %esi
402055:    5f            pop  %edi
402056:    5d            pop  %ebp
402057:    c3            ret
402058:    89 5c 24 08    mov  %ebx,0x8(%esp)
40205c:c7 44 24 04 1c 00 00 movl $0x1c,0x4(%esp)
402063: 00
402064:c7 04 24 e8 50 40 00 movl $0x4050e8,(%esp)
40206b:e8 c0 fe ff ff    call 0x401f30
402070:a1 5c 70 40 00    mov  0x40705c,%eax

```

```

402075: 85 c0          test %eax,%eax
402077: 74 07          je 0x402080
402079: c3            ret
40207a: 8d b6 00 00 00 00 lea 0x0(%esi),%esi
402080: b8 38 53 40 00 mov $0x405338,%eax
402085: c7 05 5c 70 40 00 01 movl $0x1,0x40705c
40208c: 00 00 00
40208f: 2d 38 53 40 00 sub $0x405338,%eax
402094: 83 f8 07      cmp $0x7,%eax
402097: 7e e0         jle 0x402079
402099: 57           push %edi
40209a: 56           push %esi
40209b: 53           push %ebx
40209c: 83 ec 20      sub $0x20,%esp
40209f: 83 f8 0b      cmp $0xb,%eax
4020a2: 0f 8e e8 00 00 00 jle 0x402190
4020a8: 8b 35 38 53 40 00 mov 0x405338,%esi
4020ae: 85 f6         test %esi,%esi
4020b0: 0f 85 8f 00 00 00 jne 0x402145
4020b6: 8b 1d 3c 53 40 00 mov 0x40533c,%ebx
4020bc: 85 db         test %ebx,%ebx
4020be: 0f 85 81 00 00 00 jne 0x402145
4020c4: 8b 0d 40 53 40 00 mov 0x405340,%ecx
4020ca: bb 44 53 40 00 mov $0x405344,%ebx
4020cf: 85 c9         test %ecx,%ecx
4020d1: 0f 84 be 00 00 00 je 0x402195
4020d7: bb 38 53 40 00 mov $0x405338,%ebx
4020dc: 8b 43 08      mov 0x8(%ebx),%eax
4020df: 83 f8 01      cmp $0x1,%eax
4020e2: 0f 85 43 01 00 00 jne 0x40222b
4020e8: 83 c3 0c      add $0xc,%ebx
4020eb: 81 fb 38 53 40 00 cmp $0x405338,%ebx
4020f1: 0f 83 89 00 00 00 jae 0x402180
4020f7: 8b 13         mov (%ebx),%edx
4020f9: 8b 7b 04      mov 0x4(%ebx),%edi
4020fc: 8d b2 00 00 40 00 lea 0x400000(%edx),%esi
402102: 8b 8a 00 00 40 00 mov 0x400000(%edx),%ecx
402108: 0f b6 53 08   movzbl 0x8(%ebx),%edx
40210c: 8d 87 00 00 40 00 lea 0x400000(%edi),%eax
402112: 83 fa 10      cmp $0x10,%edx
402115: 0f 84 95 00 00 00 je 0x4021b0
40211b: 83 fa 20      cmp $0x20,%edx
40211e: 0f 84 ec 00 00 00 je 0x402210
402124: 83 fa 08      cmp $0x8,%edx
402127: 0f 84 b3 00 00 00 je 0x4021e0
40212d: 89 54 24 04   mov %edx,0x4(%esp)
402131: c7 04 24 50 51 40 00 movl $0x405150,(%esp)
402138: c7 44 24 1c 00 00 00 movl $0x0,0x1c(%esp)
40213f: 00
402140: e8 eb fd ff ff call 0x401f30
402145: bb 38 53 40 00 mov $0x405338,%ebx
40214a: 81 fb 38 53 40 00 cmp $0x405338,%ebx
402150: 73 2e         jae 0x402180

```

```

402152: 8b 4b 04      mov  0x4(%ebx),%ecx
402155: 8b 13         mov  (%ebx),%edx
402157: 83 c3 08      add  $0x8,%ebx
40215a: 03 91 00 00 40 00      add  0x400000(%ecx),%edx
402160: 8d 81 00 00 40 00      lea   0x400000(%ecx),%eax
402166: b9 04 00 00 00      mov  $0x4,%ecx
40216b: 89 54 24 1c      mov  %edx,0x1c(%esp)
40216f: 8d 54 24 1c      lea   0x1c(%esp),%edx
402173: e8 08 fe ff ff      call 0x401f80
402178: 81 fb 38 53 40 00      cmp  $0x405338,%ebx
40217e: 72 d2         jb   0x402152
402180: 83 c4 20      add  $0x20,%esp
402183: 5b          pop  %ebx
402184: 5e          pop  %esi
402185: 5f          pop  %edi
402186: c3          ret
402187: 89 f6        mov  %esi,%esi
402189: 8d bc 27 00 00 00 00      lea   0x0(%edi,%eiz,1),%edi
402190: bb 38 53 40 00      mov  $0x405338,%ebx
402195: 8b 13        mov  (%ebx),%edx
402197: 85 d2        test %edx,%edx
402199: 75 af        jne  0x40214a
40219b: 8b 43 04      mov  0x4(%ebx),%eax
40219e: 85 c0        test %eax,%eax
4021a0: 0f 84 36 ff ff ff      je   0x4020dc
4021a6: eb a2        jmp  0x40214a
4021a8: 90          nop
4021a9: 8d b4 26 00 00 00 00      lea   0x0(%esi,%eiz,1),%esi
4021b0: 0f b7 97 00 00 40 00      movzwl 0x400000(%edi),%edx
4021b7: 66 85 d2      test %dx,%dx
4021ba: 79 06        jns  0x4021c2
4021bc: 81 ca 00 00 ff ff      or   $0xffff0000,%edx
4021c2: 29 f2        sub  %esi,%edx
4021c4: 01 d1        add  %edx,%ecx
4021c6: 8d 54 24 1c      lea   0x1c(%esp),%edx
4021ca: 89 4c 24 1c      mov  %ecx,0x1c(%esp)
4021ce: b9 02 00 00 00      mov  $0x2,%ecx
4021d3: e8 a8 fd ff ff      call 0x401f80
4021d8: e9 0b ff ff ff      jmp  0x4020e8
4021dd: 8d 76 00      lea   0x0(%esi),%esi
4021e0: 0f b6 38      movzbl (%eax),%edi
4021e3: 89 fa        mov  %edi,%edx
4021e5: 84 d2        test %dl,%dl
4021e7: 79 06        jns  0x4021ef
4021e9: 81 cf 00 ff ff ff      or   $0xfffff00,%edi
4021ef: 29 f7        sub  %esi,%edi
4021f1: 8d 54 24 1c      lea   0x1c(%esp),%edx
4021f5: 01 f9        add  %edi,%ecx
4021f7: 89 4c 24 1c      mov  %ecx,0x1c(%esp)
4021fb: b9 01 00 00 00      mov  $0x1,%ecx
402200: e8 7b fd ff ff      call 0x401f80
402205: e9 de fe ff ff      jmp  0x4020e8
40220a: 8d b6 00 00 00 00      lea   0x0(%esi),%esi

```

```

402210: 29 f1      sub  %esi,%ecx
402212: 03 08      add  (%eax),%ecx
402214: 8d 54 24 1c lea  0x1c(%esp),%edx
402218: 89 4c 24 1c mov  %ecx,0x1c(%esp)
40221c: b9 04 00 00 00      mov  $0x4,%ecx
402221: e8 5a fd ff ff      call 0x401f80
402226: e9 bd fe ff ff      jmp  0x4020e8
40222b: 89 44 24 04      mov  %eax,0x4(%esp)
40222f: c7 04 24 1c 51 40 00      movl $0x40511c,(%esp)
402236: e8 f5 fc ff ff      call 0x401f30
40223b: 90          nop
40223c: 90          nop
40223d: 90          nop
40223e: 90          nop
40223f: 90          nop
402240: 51          push %ecx
402241: 50          push %eax
402242: 3d 00 10 00 00      cmp  $0x1000,%eax
402247: 8d 4c 24 0c      lea  0xc(%esp),%ecx
40224b: 72 15      jb   0x402262
40224d: 81 e9 00 10 00 00      sub  $0x1000,%ecx
402253: 83 09 00      orl  $0x0,(%ecx)
402256: 2d 00 10 00 00      sub  $0x1000,%eax
40225b: 3d 00 10 00 00      cmp  $0x1000,%eax
402260: 77 eb      ja   0x40224d
402262: 29 c1      sub  %eax,%ecx
402264: 83 09 00      orl  $0x0,(%ecx)
402267: 58          pop  %eax
402268: 59          pop  %ecx
402269: c3          ret
40226a: 90          nop
40226b: 90          nop
40226c: 66 90      xchg %ax,%ax
40226e: 66 90      xchg %ax,%ax
402270: 83 ec 1c      sub  $0x1c,%esp
402273: 8b 44 24 20      mov  0x20(%esp),%eax
402277: c7 44 24 0c 80 1f 00      movl $0x1f80,0xc(%esp)
40227e: 00
40227f: 83 f8 fd      cmp  $0xffffffff,%eax
402282: 74 31      je   0x4022b5
402284: 83 f8 fc      cmp  $0xffffffff,%eax
402287: 74 3a      je   0x4022c3
402289: 85 c0      test %eax,%eax
40228b: 74 48      je   0x4022d5
40228d: 83 f8 ff      cmp  $0xffffffff,%eax
402290: 74 2d      je   0x4022bf
402292: 83 f8 fe      cmp  $0xffffffff,%eax
402295: 74 36      je   0x4022cd
402297: d9 20      fldenv (%eax)
402299: 0f b7 40 1c      movzwl 0x1c(%eax),%eax
40229d: 89 44 24 0c      mov  %eax,0xc(%esp)
4022a1: f6 05 24 70 40 00 10      testb $0x10,0x407024
4022a8: 74 05      je   0x4022af

```

```

4022aa: 0f ae 54 24 0c      ldmxcsr 0xc(%esp)
4022af:31 c0              xor  %eax,%eax
4022b1: 83 c4 1c          add  $0x1c,%esp
4022b4: c3              ret
4022b5: c7 05 14 40 40 00 ff      movl $0xffffffff,0x404014
4022bc: ff ff ff
4022bf: db e3          fninit
4022c1: eb de          jmp  0x4022a1
4022c3: c7 05 14 40 40 00 fe      movl $0xffffffff,0x404014
4022ca: ff ff ff
4022cd: ff 15 b0 81 40 00      call *0x4081b0
4022d3: eb cc          jmp  0x4022a1
4022d5: a1 14 40 40 00      mov  0x404014,%eax
4022da: eb b1          jmp  0x40228d
4022dc: 90              nop
4022dd: 90              nop
4022de: 90              nop
4022df: 90              nop
4022e0: 85 c0          test %eax,%eax
4022e2: 0f 84 82 00 00 00      je   0x40236a
4022e8: 56              push %esi
4022e9: 53              push %ebx
4022ea: 89 d3          mov  %edx,%ebx
4022ec: c1 eb 05      shr  $0x5,%ebx
4022ef: 31 c9          xor  %ecx,%ecx
4022f1: 83 f3 01      xor  $0x1,%ebx
4022f4: 83 e3 01      and  $0x1,%ebx
4022f7: 89 f6          mov  %esi,%esi
4022f9: 8d bc 27 00 00 00 00      lea  0x0(%edi,%eiz,1),%edi
402300: 0f be 10      movsbl (%eax),%edx
402303: 85 d2          test %edx,%edx
402305: 74 29          je   0x402330
402307: 84 db          test %bl,%bl
402309: 74 05          je   0x402310
40230b: 83 fa 7f      cmp  $0x7f,%edx
40230e: 74 40          je   0x402350
402310: 83 c0 01      add  $0x1,%eax
402313: 85 c9          test %ecx,%ecx
402315: 75 1e          jne  0x402335
402317: 83 fa 2a      cmp  $0x2a,%edx
40231a: 74 44          je   0x402360
40231c: 83 fa 3f      cmp  $0x3f,%edx
40231f: 74 3f          je   0x402360
402321: 31 c9          xor  %ecx,%ecx
402323: 83 fa 5b      cmp  $0x5b,%edx
402326: 0f be 10      movsbl (%eax),%edx
402329: 0f 94 c1      sete %cl
40232c: 85 d2          test %edx,%edx
40232e: 75 d7          jne  0x402307
402330: 89 d0          mov  %edx,%eax
402332: 5b              pop  %ebx
402333: 5e              pop  %esi
402334: c3              ret

```

```

402335: 83 f9 01      cmp $0x1,%ecx
402338: 7e 05        jle 0x40233f
40233a: 83 fa 5d      cmp $0x5d,%edx
40233d: 74 21        je 0x402360
40233f: 83 fa 21      cmp $0x21,%edx
402342: 0f 95 c2      setne %dl
402345: 0f b6 d2      movzbl %dl,%edx
402348: 01 d1        add %edx,%ecx
40234a: eb b4        jmp 0x402300
40234c: 8d 74 26 00   lea 0x0(%esi,%eiz,1),%esi
402350: 80 78 01 00   cmpb $0x0,0x1(%eax)
402354: 8d 70 02      lea 0x2(%eax),%esi
402357: 74 16        je 0x40236f
402359: 89 f0        mov %esi,%eax
40235b: eb b6        jmp 0x402313
40235d: 8d 76 00      lea 0x0(%esi),%esi
402360: ba 01 00 00 00 mov $0x1,%edx
402365: 89 d0        mov %edx,%eax
402367: 5b          pop %ebx
402368: 5e          pop %esi
402369: c3          ret
40236a: 31 d2        xor %edx,%edx
40236c: 89 d0        mov %edx,%eax
40236e: c3          ret
40236f: 31 d2        xor %edx,%edx
402371: eb bd        jmp 0x402330
402373: 8d b6 00 00 00 00 lea 0x0(%esi),%esi
402379: 8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
402380: 85 c0        test %eax,%eax
402382: 74 5c        je 0x4023e0
402384: 56          push %esi
402385: 53          push %ebx
402386: 89 c6        mov %eax,%esi
402388: 83 ec 14      sub $0x14,%esp
40238b: 8b 40 0c      mov 0xc(%eax),%eax
40238e: 8d 58 01      lea 0x1(%eax),%ebx
402391: 8d 04 9d 00 00 00 00 lea 0x0(,%ebx,4),%eax
402398: 89 04 24      mov %eax,(%esp)
40239b: e8 30 19 00 00 call 0x403cd0
4023a0: 89 c1        mov %eax,%ecx
4023a2: 89 46 08      mov %eax,0x8(%esi)
4023a5: b8 03 00 00 00 mov $0x3,%eax
4023aa: 85 c9        test %ecx,%ecx
4023ac: 74 22        je 0x4023d0
4023ae: 85 db        test %ebx,%ebx
4023b0: 89 da        mov %ebx,%edx
4023b2: c7 46 04 00 00 00 00 movl $0x0,0x4(%esi)
4023b9: 7e 13        jle 0x4023ce
4023bb: 90          nop
4023bc: 8d 74 26 00   lea 0x0(%esi,%eiz,1),%esi
4023c0: 83 ea 01      sub $0x1,%edx
4023c3: 85 d2        test %edx,%edx
4023c5: c7 04 91 00 00 00 00 movl $0x0,(%ecx,%edx,4)

```

```

4023cc: 75 f2      jne 0x4023c0
4023ce: 31 c0      xor %eax,%eax
4023d0: 83 c4 14   add $0x14,%esp
4023d3: 5b        pop %ebx
4023d4: 5e        pop %esi
4023d5: c3        ret
4023d6: 8d 76 00   lea 0x0(%esi),%esi
4023d9: 8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
4023e0: 31 c0      xor %eax,%eax
4023e2: c3        ret
4023e3: 8d b6 00 00 00 00   lea 0x0(%esi),%esi
4023e9: 8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
4023f0: 55        push %ebp
4023f1: 57        push %edi
4023f2: 89 c7      mov %eax,%edi
4023f4: 56        push %esi
4023f5: 53        push %ebx
4023f6: 83 ec 3c   sub $0x3c,%esp
4023f9: 0f be 18   movsbl (%eax),%ebx
4023fc: 89 54 24 1c   mov %edx,0x1c(%esp)
402400: 89 4c 24 20   mov %ecx,0x20(%esp)
402404: 83 fb 5d     cmp $0x5d,%ebx
402407: 89 dd      mov %ebx,%ebp
402409: 0f 84 61 01 00 00   je 0x402570
40240f: 83 fb 2d     cmp $0x2d,%ebx
402412: 0f 84 58 01 00 00   je 0x402570
402418: 8b 4c 24 1c   mov 0x1c(%esp),%ecx
40241c: 89 c8      mov %ecx,%eax
40241e: f7 d0      not %eax
402420: 89 44 24 28   mov %eax,0x28(%esp)
402424: b8 01 00 00 00   mov $0x1,%eax
402429: 29 c8      sub %ecx,%eax
40242b: 89 44 24 2c   mov %eax,0x2c(%esp)
40242f: eb 0d      jmp 0x40243e
402431: 89 ee      mov %ebp,%esi
402433: 2b 74 24 1c   sub 0x1c(%esp),%esi
402437: 85 f6      test %esi,%esi
402439: 74 68      je 0x4024a3
40243b: 0f be da     movsbl %dl,%ebx
40243e: 83 fb 5d     cmp $0x5d,%ebx
402441: 8d 77 01     lea 0x1(%edi),%esi
402444: 0f 84 1a 01 00 00   je 0x402564
40244a: 83 fb 2d     cmp $0x2d,%ebx
40244d: 0f 84 8d 00 00 00   je 0x4024e0
402453: 85 db      test %ebx,%ebx
402455: 0f 84 09 01 00 00   je 0x402564
40245b: 83 fb 2f     cmp $0x2f,%ebx
40245e: 0f 84 00 01 00 00   je 0x402564
402464: 83 fb 5c     cmp $0x5c,%ebx
402467: 0f 84 f7 00 00 00   je 0x402564
40246d: 0f b6 16     movzbl (%esi),%edx
402470: 89 dd      mov %ebx,%ebp
402472: 89 f7      mov %esi,%edi

```



```

402474: f7 44 24 20 00 40 00    testl $0x4000,0x20(%esp)
40247b: 00
40247c: 75 b3                jne 0x402431
40247e: 89 2c 24            mov  %ebp,(%esp)
402481: 88 54 24 24        mov  %dl,0x24(%esp)
402485: e8 d6 17 00 00      call 0x403c60
40248a: 89 c6                mov  %eax,%esi
40248c: 8b 44 24 1c        mov  0x1c(%esp),%eax
402490: 89 04 24            mov  %eax,(%esp)
402493: e8 c8 17 00 00      call 0x403c60
402498: 29 c6                sub  %eax,%esi
40249a: 0f b6 54 24 24      movzbl 0x24(%esp),%edx
40249f: 85 f6                test %esi,%esi
4024a1: 75 98                jne 0x40243b
4024a3: 8b 44 24 20        mov  0x20(%esp),%eax
4024a7: 83 e0 20            and  $0x20,%eax
4024aa: eb 12                jmp  0x4024be
4024ac: 8d 74 26 00        lea  0x0(%esi,%eiz,1),%esi
4024b0: 83 c7 01            add  $0x1,%edi
4024b3: 84 d2                test %dl,%dl
4024b5: 0f 84 a9 00 00 00    je   0x402564
4024bb: 0f b6 17            movzbl (%edi),%edx
4024be: 80 fa 5d            cmp  $0x5d,%dl
4024c1: 0f 84 3e 01 00 00    je   0x402605
4024c7: 80 fa 7f            cmp  $0x7f,%dl
4024ca: 75 e4                jne 0x4024b0
4024cc: 85 c0                test %eax,%eax
4024ce: 0f 85 3c 01 00 00    jne 0x402610
4024d4: 0f b6 57 01        movzbl 0x1(%edi),%edx
4024d8: 83 c7 01            add  $0x1,%edi
4024db: eb d3                jmp  0x4024b0
4024dd: 8d 76 00            lea  0x0(%esi),%esi
4024e0: 0f b6 57 01        movzbl 0x1(%edi),%edx
4024e4: 80 fa 5d            cmp  $0x5d,%dl
4024e7: 0f 84 95 00 00 00    je   0x402582
4024ed: 0f be da            movsbl %dl,%ebx
4024f0: 85 db                test %ebx,%ebx
4024f2: 74 70                je   0x402564
4024f4: 8b 4c 24 20        mov  0x20(%esp),%ecx
4024f8: 8d 77 02            lea  0x2(%edi),%esi
4024fb: 81 e1 00 40 00 00    and  $0x4000,%ecx
402501: 39 dd                cmp  %ebx,%ebp
402503: 0f 8d 0f 01 00 00    jge 0x402618
402509: 89 74 24 24        mov  %esi,0x24(%esp)
40250d: 89 e8                mov  %ebp,%eax
40250f: 89 ce                mov  %ecx,%esi
402511: eb 11                jmp  0x402524
402513: 8b 44 24 28        mov  0x28(%esp),%eax
402517: 8d 3c 28            lea  (%eax,%ebp,1),%edi
40251a: 85 ff                test %edi,%edi
40251c: 74 29                je   0x402547
40251e: 39 eb                cmp  %ebp,%ebx
402520: 89 e8                mov  %ebp,%eax

```

```

402522: 74 6c      je  0x402590
402524: 85 f6      test %esi,%esi
402526: 8d 68 01   lea  0x1(%eax),%ebp
402529: 75 e8      jne  0x402513
40252b: 89 04 24   mov  %eax,(%esp)
40252e: e8 2d 17 00 00 call 0x403c60
402533: 89 c7      mov  %eax,%edi
402535: 8b 44 24 1c mov  0x1c(%esp),%eax
402539: 89 04 24   mov  %eax,(%esp)
40253c: e8 1f 17 00 00 call 0x403c60
402541: 29 c7      sub  %eax,%edi
402543: 85 ff      test %edi,%edi
402545: 75 d7      jne  0x40251e
402547: 8b 54 24 20 mov  0x20(%esp),%edx
40254b: 8b 74 24 24 mov  0x24(%esp),%esi
40254f: 83 e2 20   and  $0x20,%edx
402552: 0f b6 06   movzbl (%esi),%eax
402555: 3c 5d      cmp  $0x5d,%al
402557: 74 61      je   0x4025ba
402559: 3c 7f      cmp  $0x7f,%al
40255b: 74 43      je   0x4025a0
40255d: 83 c6 01   add  $0x1,%esi
402560: 84 c0      test %al,%al
402562: 75 ee      jne  0x402552
402564: 83 c4 3c   add  $0x3c,%esp
402567: 31 c0      xor  %eax,%eax
402569: 5b        pop  %ebx
40256a: 5e        pop  %esi
40256b: 5f        pop  %edi
40256c: 5d        pop  %ebp
40256d: c3        ret
40256e: 66 90      xchg %ax,%ax
402570: 3b 5c 24 1c cmp  0x1c(%esp),%ebx
402574: 74 4f      je   0x4025c5
402576: 0f be 5f 01 movsbl 0x1(%edi),%ebx
40257a: 83 c7 01   add  $0x1,%edi
40257d: e9 96 fe ff jmp  0x402418
402582: bd 2d 00 00 00 00 mov  $0x2d,%ebp
402587: 89 f7      mov  %esi,%edi
402589: e9 e6 fe ff jmp  0x402474
40258e: 66 90      xchg %ax,%ax
402590: 8b 74 24 24 mov  0x24(%esp),%esi
402594: e9 c2 fe ff jmp  0x40245b
402599: 8d b4 26 00 00 00 00 lea  0x0(%esi,%eiz,1),%esi
4025a0: 85 d2      test %edx,%edx
4025a2: 75 0c      jne  0x4025b0
4025a4: 0f b6 46 01 movzbl 0x1(%esi),%eax
4025a8: 83 c6 01   add  $0x1,%esi
4025ab: eb b0      jmp  0x40255d
4025ad: 8d 76 00   lea  0x0(%esi),%esi
4025b0: 83 c6 01   add  $0x1,%esi
4025b3: 0f b6 06   movzbl (%esi),%eax
4025b6: 3c 5d      cmp  $0x5d,%al

```

```

4025b8: 75 9f      jne 0x402559
4025ba: 83 c4 3c   add $0x3c,%esp
4025bd: 8d 46 01   lea 0x1(%esi),%eax
4025c0: 5b        pop %ebx
4025c1: 5e        pop %esi
4025c2: 5f        pop %edi
4025c3: 5d        pop %ebp
4025c4: c3        ret
4025c5: 8b 54 24 20 mov 0x20(%esp),%edx
4025c9: 83 c7 01   add $0x1,%edi
4025cc: 83 e2 20   and $0x20,%edx
4025cf: 90        nop
4025d0: 0f b6 07   movzbl (%edi),%eax
4025d3: 3c 5d      cmp $0x5d,%al
4025d5: 74 2e      je 0x402605
4025d7: 3c 7f      cmp $0x7f,%al
4025d9: 74 15      je 0x4025f0
4025db: 83 c7 01   add $0x1,%edi
4025de: 84 c0      test %al,%al
4025e0: 75 ee      jne 0x4025d0
4025e2: e9 7d ff ff jmp 0x402564
4025e7: 89 f6      mov %esi,%esi
4025e9: 8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
4025f0: 85 d2      test %edx,%edx
4025f2: 75 0c      jne 0x402600
4025f4: 0f b6 47 01 movzbl 0x1(%edi),%eax
4025f8: 83 c7 01   add $0x1,%edi
4025fb: eb de      jmp 0x4025db
4025fd: 8d 76 00   lea 0x0(%esi),%esi
402600: 83 c7 01   add $0x1,%edi
402603: eb cb      jmp 0x4025d0
402605: 83 c4 3c   add $0x3c,%esp
402608: 8d 47 01   lea 0x1(%edi),%eax
40260b: 5b        pop %ebx
40260c: 5e        pop %esi
40260d: 5f        pop %edi
40260e: 5d        pop %ebp
40260f: c3        ret
402610: 83 c7 01   add $0x1,%edi
402613: e9 a3 fe ff jmp 0x4024bb
402618: 0f 8e 3d fe ff ff jle 0x40245b
40261e: 89 74 24 24 mov %esi,0x24(%esp)
402622: 89 ce      mov %ecx,%esi
402624: eb 1f      jmp 0x402645
402626: 8d 76 00   lea 0x0(%esi),%esi
402629: 8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
402630: 8b 44 24 2c mov 0x2c(%esp),%eax
402634: 8d 2c 38   lea (%eax,%edi,1),%ebp
402637: 85 ed      test %ebp,%ebp
402639: 74 2d      je 0x402668
40263b: 39 fb      cmp %edi,%ebx
40263d: 89 fd      mov %edi,%ebp
40263f: 0f 84 4b ff ff je 0x402590

```

402645:	85 f6	test %esi,%esi
402647:	8d 7d ff	lea -0x1(%ebp),%edi
40264a:	75 e4	jne 0x402630
40264c:	89 2c 24	mov %ebp,(%esp)
40264f:	e8 0c 16 00 00	call 0x403c60
402654:	89 c5	mov %eax,%ebp
402656:	8b 44 24 1c	mov 0x1c(%esp),%eax
40265a:	89 04 24	mov %eax,(%esp)
40265d:	e8 fe 15 00 00	call 0x403c60
402662:	29 c5	sub %eax,%ebp
402664:	85 ed	test %ebp,%ebp
402666:	75 d3	jne 0x40263b
402668:	8b 54 24 20	mov 0x20(%esp),%edx
40266c:	8b 74 24 24	mov 0x24(%esp),%esi
402670:	83 e2 20	and \$0x20,%edx
402673:	0f b6 06	movzbl (%esi),%eax
402676:	3c 5d	cmp \$0x5d,%al
402678:	0f 84 3c ff ff ff	je 0x4025ba
40267e:	3c 7f	cmp \$0x7f,%al
402680:	74 0e	je 0x402690
402682:	83 c6 01	add \$0x1,%esi
402685:	84 c0	test %al,%al
402687:	75 ea	jne 0x402673
402689:	e9 d6 fe ff ff	jmp 0x402564
40268e:	66 90	xchg %ax,%ax
402690:	85 d2	test %edx,%edx
402692:	75 0c	jne 0x4026a0
402694:	0f b6 46 01	movzbl 0x1(%esi),%eax
402698:	83 c6 01	add \$0x1,%esi
40269b:	eb e5	jmp 0x402682
40269d:	8d 76 00	lea 0x0(%esi),%esi
4026a0:	83 c6 01	add \$0x1,%esi
4026a3:	eb ce	jmp 0x402673
4026a5:	8d 74 26 00	lea 0x0(%esi,%eiz,1),%esi
4026a9:	8d bc 27 00 00 00 00	lea 0x0(%edi,%eiz,1),%edi
4026b0:	55	push %ebp
4026b1:	57	push %edi
4026b2:	89 c5	mov %eax,%ebp
4026b4:	56	push %esi
4026b5:	53	push %ebx
4026b6:	83 ec 2c	sub \$0x2c,%esp
4026b9:	80 3a 2e	cmpl \$0x2e,%edx
4026bc:	89 4c 24 14	mov %ecx,0x14(%esp)
4026c0:	0f b6 08	movzbl (%eax),%ecx
4026c3:	0f 84 37 01 00 00	je 0x402800
4026c9:	8b 44 24 14	mov 0x14(%esp),%eax
4026cd:	8d 7a 01	lea 0x1(%edx),%edi
4026d0:	c1 e8 05	shr \$0x5,%eax
4026d3:	83 f0 01	xor \$0x1,%eax
4026d6:	89 44 24 18	mov %eax,0x18(%esp)
4026da:	0f be d1	movsbl %cl,%edx
4026dd:	8d 77 ff	lea -0x1(%edi),%esi
4026e0:	8d 45 01	lea 0x1(%ebp),%eax

```

4026e3: 85 d2      test %edx,%edx
4026e5: 0f 84 69 01 00 00    je 0x402854
4026eb: 80 f9 3f      cmp $0x3f,%cl
4026ee: 0f 84 ed 00 00 00    je 0x4027e1
4026f4: 80 f9 5b      cmp $0x5b,%cl
4026f7: 0f 84 b3 00 00 00    je 0x4027b0
4026fd: 80 f9 2a      cmp $0x2a,%cl
402700: 74 5e      je 0x402760
402702: f6 44 24 18 01      testb $0x1,0x18(%esp)
402707: 74 09      je 0x402712
402709: 83 fa 7f      cmp $0x7f,%edx
40270c: 0f 84 2e 01 00 00    je 0x402840
402712: 89 c5      mov %eax,%ebp
402714: 0f be 5f ff      movsbl -0x1(%edi),%ebx
402718: 84 db      test %bl,%bl
40271a: 0f 84 86 01 00 00    je 0x4028a6
402720: f7 44 24 14 00 40 00    testl $0x4000,0x14(%esp)
402727: 00
402728: 0f 85 c2 00 00 00    jne 0x4027f0
40272e: 89 14 24      mov %edx,(%esp)
402731: 89 54 24 1c      mov %edx,0x1c(%esp)
402735: e8 26 15 00 00      call 0x403c60
40273a: 89 1c 24      mov %ebx,(%esp)
40273d: 89 c6      mov %eax,%esi
40273f: e8 1c 15 00 00      call 0x403c60
402744: 8b 54 24 1c      mov 0x1c(%esp),%edx
402748: 29 c6      sub %eax,%esi
40274a: 85 f6      test %esi,%esi
40274c: 0f 84 83 00 00 00    je 0x4027d5
402752: 89 d0      mov %edx,%eax
402754: 29 d8      sub %ebx,%eax
402756: 83 c4 2c      add $0x2c,%esp
402759: 5b      pop %ebx
40275a: 5e      pop %esi
40275b: 5f      pop %edi
40275c: 5d      pop %ebp
40275d: c3      ret
40275e: 66 90      xchg %ax,%ax
402760: 0f b6 55 01      movzbl 0x1(%ebp),%edx
402764: 89 c3      mov %eax,%ebx
402766: 80 fa 2a      cmp $0x2a,%dl
402769: 75 10      jne 0x40277b
40276b: 90      nop
40276c: 8d 74 26 00      lea 0x0(%esi,%eiz,1),%esi
402770: 83 c3 01      add $0x1,%ebx
402773: 0f b6 13      movzbl (%ebx),%edx
402776: 80 fa 2a      cmp $0x2a,%dl
402779: 74 f5      je 0x402770
40277b: 31 c0      xor %eax,%eax
40277d: 84 d2      test %dl,%dl
40277f: 74 d5      je 0x402756
402781: 8b 7c 24 14      mov 0x14(%esp),%edi
402785: 81 cf 00 00 01 00      or $0x10000,%edi

```

```

40278b:  eb 0c          jmp  0x402799
40278d:  8d 76 00      lea  0x0(%esi),%esi
402790:  83 c6 01      add  $0x1,%esi
402793:  80 7e ff 00   cmpb $0x0,-0x1(%esi)
402797:  74 bd        je   0x402756
402799:  89 f9        mov  %edi,%ecx
40279b:  89 f2        mov  %esi,%edx
40279d:  89 d8        mov  %ebx,%eax
40279f:  e8 0c ff ff   call 0x4026b0
4027a4:  85 c0        test %eax,%eax
4027a6:  75 e8        jne  0x402790
4027a8:  83 c4 2c      add  $0x2c,%esp
4027ab:  5b          pop  %ebx
4027ac:  5e          pop  %esi
4027ad:  5f          pop  %edi
4027ae:  5d          pop  %ebp
4027af:c3          ret
4027b0:  0f be 57 ff   movsbl -0x1(%edi),%edx
4027b4:  85 d2        test %edx,%edx
4027b6:  0f 84 fb 00 00 00   je   0x4028b7
4027bc:  80 7d 01 21   cmpb $0x21,0x1(%ebp)
4027c0:  74 60        je   0x402822
4027c2:  8b 4c 24 14   mov  0x14(%esp),%ecx
4027c6:  e8 25 fc ff ff   call 0x4023f0
4027cb:  89 c5        mov  %eax,%ebp
4027cd:  85 ed        test %ebp,%ebp
4027cf:0f 84 c7 00 00 00   je   0x40289c
4027d5:  0f b6 4d 00   movzbl 0x0(%ebp),%ecx
4027d9:  83 c7 01      add  $0x1,%edi
4027dc:  e9 f9 fe ff ff   jmp  0x4026da
4027e1:  80 7f ff 00   cmpb $0x0,-0x1(%edi)
4027e5:  0f 84 c2 00 00 00   je   0x4028ad
4027eb:  89 c5        mov  %eax,%ebp
4027ed:  eb e6        jmp  0x4027d5
4027ef:  90          nop
4027f0:  89 d6        mov  %edx,%esi
4027f2:  29 de        sub  %ebx,%esi
4027f4:  e9 51 ff ff ff   jmp  0x40274a
4027f9:  8d b4 26 00 00 00 00   lea  0x0(%esi,%eiz,1),%esi
402800:  80 f9 2e      cmp  $0x2e,%cl
402803:  0f 84 c0 fe ff ff   je   0x4026c9
402809:  0f be c1      movsbl %cl,%eax
40280c:  83 e8 2e      sub  $0x2e,%eax
40280f:  f7 44 24 14 00 00 01   testl $0x10000,0x14(%esp)
402816:  00
402817:  0f 85 ac fe ff ff   jne  0x4026c9
40281d:  e9 34 ff ff ff   jmp  0x402756
402822:  8d 5d 02      lea  0x2(%ebp),%ebx
402825:  8b 4c 24 14   mov  0x14(%esp),%ecx
402829:  89 d8        mov  %ebx,%eax
40282b:  e8 c0 fb ff ff   call 0x4023f0
402830:  85 c0        test %eax,%eax
402832:  74 2a        je   0x40285e

```

```

402834: 89 dd      mov  %ebx,%ebp
402836: eb 95      jmp  0x4027cd
402838: 90         nop
402839: 8d b4 26 00 00 00 00    lea  0x0(%esi,%eiz,1),%esi
402840: 0f be 55 01    movsbl 0x1(%ebp),%edx
402844: 83 c5 02      add  $0x2,%ebp
402847: 85 d2      test %edx,%edx
402849: 0f 85 c5 fe ff ff    jne  0x402714
40284f: e9 be fe ff ff    jmp  0x402712
402854: 0f be 06      movsbl (%esi),%eax
402857: f7 d8      neg  %eax
402859: e9 f8 fe ff ff    jmp  0x402756
40285e: 0f b6 45 02    movzbl 0x2(%ebp),%eax
402862: 3c 5d      cmp  $0x5d,%al
402864: 74 5b      je   0x4028c1
402866: 8b 54 24 14    mov  0x14(%esp),%edx
40286a: 83 e2 20      and  $0x20,%edx
40286d: eb 0b      jmp  0x40287a
40286f: 90         nop
402870: 83 c3 01      add  $0x1,%ebx
402873: 84 c0      test %al,%al
402875: 74 25      je   0x40289c
402877: 0f b6 03      movzbl (%ebx),%eax
40287a: 3c 5d      cmp  $0x5d,%al
40287c: 74 16      je   0x402894
40287e: 3c 7f      cmp  $0x7f,%al
402880: 75 ee      jne  0x402870
402882: 85 d2      test %edx,%edx
402884: 75 09      jne  0x40288f
402886: 0f b6 43 01    movzbl 0x1(%ebx),%eax
40288a: 83 c3 01      add  $0x1,%ebx
40288d: eb e1      jmp  0x402870
40288f: 83 c3 01      add  $0x1,%ebx
402892: eb e3      jmp  0x402877
402894: 8d 6b 01      lea  0x1(%ebx),%ebp
402897: e9 31 ff ff ff    jmp  0x4027cd
40289c: b8 5d 00 00 00    mov  $0x5d,%eax
4028a1: e9 b0 fe ff ff    jmp  0x402756
4028a6: 31 db      xor  %ebx,%ebx
4028a8: e9 a5 fe ff ff    jmp  0x402752
4028ad: b8 3f 00 00 00    mov  $0x3f,%eax
4028b2: e9 9f fe ff ff    jmp  0x402756
4028b7: b8 5b 00 00 00    mov  $0x5b,%eax
4028bc: e9 95 fe ff ff    jmp  0x402756
4028c1: 8d 5d 03      lea  0x3(%ebp),%ebx
4028c4: 0f b6 45 03    movzbl 0x3(%ebp),%eax
4028c8: eb 9c      jmp  0x402866
4028ca: 8d b6 00 00 00 00    lea  0x0(%esi),%esi
4028d0: 57         push %edi
4028d1: 56         push %esi
4028d2: 89 c6      mov  %eax,%esi
4028d4: 53         push %ebx
4028d5: 89 d3      mov  %edx,%ebx

```

```

4028d7:      83 ec 10      sub    $0x10,%esp
4028da:      8b 42 0c      mov    0xc(%edx),%eax
4028dd:      03 42 04      add    0x4(%edx),%eax
4028e0:      8d 04 85 08 00 00 00    lea    0x8(,%eax,4),%eax
4028e7:      89 44 24 04      mov    %eax,0x4(%esp)
4028eb:      8b 42 08      mov    0x8(%edx),%eax
4028ee:      89 04 24      mov    %eax,(%esp)
4028f1:      e8 aa 13 00 00      call   0x403ca0
4028f6:      85 c0          test   %eax,%eax
4028f8:      74 26          je     0x402920
4028fa:8b 4b 04      mov    0x4(%ebx),%ecx
4028fd:      8b 53 0c      mov    0xc(%ebx),%edx
402900:      89 43 08      mov    %eax,0x8(%ebx)
402903:      8d 79 01      lea    0x1(%ecx),%edi
402906:      01 d1          add    %edx,%ecx
402908:      01 fa          add    %edi,%edx
40290a:      89 7b 04      mov    %edi,0x4(%ebx)
40290d:      89 34 88      mov    %esi,(%eax,%ecx,4)
402910:      c7 04 90 00 00 00 00    movl   $0x0,(%eax,%edx,4)
402917:      83 c4 10      add    $0x10,%esp
40291a:      31 c0          xor    %eax,%eax
40291c:      5b            pop    %ebx
40291d:      5e            pop    %esi
40291e:      5f            pop    %edi
40291f:      c3            ret
402920:      83 c4 10      add    $0x10,%esp
402923:      b8 01 00 00 00      mov    $0x1,%eax
402928:      5b            pop    %ebx
402929:      5e            pop    %esi
40292a:      5f            pop    %edi
40292b:      c3            ret
40292c:      8d 74 26 00      lea    0x0(%esi,%eiz,1),%esi
402930:      56            push   %esi
402931:      53            push   %ebx
402932:      89 c3          mov    %eax,%ebx
402934:      89 d6          mov    %edx,%esi
402936:      83 ec 14      sub    $0x14,%esp
402939:      8b 00          mov    (%eax),%eax
40293b:      85 c0          test   %eax,%eax
40293d:      74 05          je     0x402944
40293f:      e8 ec ff ff      call   0x402930
402944:      8b 43 08      mov    0x8(%ebx),%eax
402947:      85 c0          test   %eax,%eax
402949:      74 04          je     0x40294f
40294b:      85 f6          test   %esi,%esi
40294d:      75 21          jne    0x402970
40294f:      8b 43 04      mov    0x4(%ebx),%eax
402952:      85 c0          test   %eax,%eax
402954:      74 07          je     0x40295d
402956:      89 f2          mov    %esi,%edx
402958:      e8 d3 ff ff      call   0x402930
40295d:      89 1c 24      mov    %ebx,(%esp)
402960:      e8 7b 13 00 00      call   0x403ce0

```



```

402965:      83 c4 14      add    $0x14,%esp
402968:      5b            pop    %ebx
402969:      5e            pop    %esi
40296a:      c3            ret
40296b:      90            nop
40296c:      8d 74 26 00    lea    0x0(%esi,%eiz,1),%esi
402970:      89 f2          mov    %esi,%edx
402972:      e8 59 ff ff    call   0x4028d0
402977:      eb d6          jmp    0x40294f
402979:      8d b4 26 00 00 00 00    lea    0x0(%esi,%eiz,1),%esi
402980:      55            push   %ebp
402981:      89 e5          mov    %esp,%ebp
402983:      57            push   %edi
402984:      56            push   %esi
402985:      53            push   %ebx
402986:      89 c3          mov    %eax,%ebx
402988:      83 ec 6c       sub    $0x6c,%esp
40298b:      89 55 d0       mov    %edx,-0x30(%ebp)
40298e:      80 e6 04       and    $0x4,%dh
402991:      89 4d c4       mov    %ecx,-0x3c(%ebp)
402994:      0f 85 56 03 00 00    jne    0x402cf0
40299a:      89 65 a8       mov    %esp,-0x58(%ebp)
40299d:      89 1c 24       mov    %ebx,(%esp)
4029a0:      e8 cb 12 00 00    call   0x403c70
4029a5:      8d 50 01       lea    0x1(%eax),%edx
4029a8:      83 c0 10       add    $0x10,%eax
4029ab:      c1 e8 04       shr    $0x4,%eax
4029ae:      c1 e0 04       shl    $0x4,%eax
4029b1:      e8 8a f8 ff ff    call   0x402240
4029b6:      29 c4          sub    %eax,%esp
4029b8:      8d 44 24 0c     lea    0xc(%esp),%eax
4029bc:      89 54 24 08     mov    %edx,0x8(%esp)
4029c0:      89 5c 24 04     mov    %ebx,0x4(%esp)
4029c4:      89 04 24       mov    %eax,(%esp)
4029c7:      e8 f4 12 00 00    call   0x403cc0
4029cc:      89 04 24       mov    %eax,(%esp)
4029cf: e8 8c 09 00 00    call   0x403360
4029d4:      89 45 d4       mov    %eax,-0x2c(%ebp)
4029d7:      89 c6          mov    %eax,%esi
4029d9:      8d 45 d8       lea    -0x28(%ebp),%eax
4029dc:      c7 45 e4 00 00 00 00    movl   $0x0,-0x1c(%ebp)
4029e3:      e8 98 f9 ff ff    call   0x402380
4029e8:      85 c0          test   %eax,%eax
4029ea:      89 45 cc       mov    %eax,-0x34(%ebp)
4029ed:      0f 85 ed 02 00 00    jne    0x402ce0
4029f3:      8b 7d d0       mov    -0x30(%ebp),%edi
4029f6:      89 f0          mov    %esi,%eax
4029f8:      89 fa          mov    %edi,%edx
4029fa: e8 e1 f8 ff ff    call   0x4022e0
4029ff: 85 c0          test   %eax,%eax
402a01:      0f 84 d7 04 00 00    je     0x402ede
402a07:      8d 45 d8       lea    -0x28(%ebp),%eax
402a0a:      89 fa          mov    %edi,%edx

```

```

402a0c:      80 ce 80      or    $0x80,%dh
402a0f:89 04 24      mov    %eax,(%esp)
402a12:      8b 4d c4      mov    -0x3c(%ebp),%ecx
402a15:      89 f0        mov    %esi,%eax
402a17:      e8 64 ff ff   call   0x402980
402a1c:      89 45 cc      mov    %eax,-0x34(%ebp)
402a1f:8b 4d cc      mov    -0x34(%ebp),%ecx
402a22:      85 c9        test   %ecx,%ecx
402a24:      0f 85 b6 02 00 00    jne    0x402ce0
402a2a:      0f b6 43 01     movzbl 0x1(%ebx),%eax
402a2e:      3c 2f        cmp    $0x2f,%al
402a30:      74 19        je     0x402a4b
402a32:      3c 5c        cmp    $0x5c,%al
402a34:      74 15        je     0x402a4b
402a36:      8b 75 d4      mov    -0x2c(%ebp),%esi
402a39:      bf 7c 51 40 00    mov    $0x40517c,%edi
402a3e:      b9 02 00 00 00    mov    $0x2,%ecx
402a43:      f3 a6        repz   cmpsb %es:(%edi),%ds:(%esi)
402a45:      0f 84 0b 05 00 00    je     0x402f56
402a4b:      8b 45 d4      mov    -0x2c(%ebp),%eax
402a4e:      89 04 24      mov    %eax,(%esp)
402a51:      e8 1a 12 00 00    call   0x403c70
402a56:      01 d8        add    %ebx,%eax
402a58:      39 c3        cmp    %eax,%ebx
402a5a:      0f 83 66 07 00 00    jae    0x4031c6
402a60:      0f b6 08      movzbl (%eax),%ecx
402a63:      80 f9 2f      cmp    $0x2f,%cl
402a66:      88 4d a3      mov    %cl,-0x5d(%ebp)
402a69:      0f 84 4f 07 00 00    je     0x4031be
402a6f:80 f9 5c      cmp    $0x5c,%cl
402a72:      75 24        jne    0x402a98
402a74:      e9 45 07 00 00    jmp    0x4031be
402a79:      8d b4 26 00 00 00 00    lea    0x0(%esi,%eiz,1),%esi
402a80:      0f b6 48 ff     movzbl -0x1(%eax),%ecx
402a84:      89 d0        mov    %edx,%eax
402a86:      80 f9 2f      cmp    $0x2f,%cl
402a89:      0f 84 6b 06 00 00    je     0x4030fa
402a8f:80 f9 5c      cmp    $0x5c,%cl
402a92:      0f 84 62 06 00 00    je     0x4030fa
402a98:      8d 50 ff      lea    -0x1(%eax),%edx
402a9b:      39 d3        cmp    %edx,%ebx
402a9d:      75 e1        jne    0x402a80
402a9f:0f b6 40 ff     movzbl -0x1(%eax),%eax
402aa3:      89 55 c8      mov    %edx,-0x38(%ebp)
402aa6:      88 45 a3      mov    %al,-0x5d(%ebp)
402aa9:      0f b6 45 a3     movzbl -0x5d(%ebp),%eax
402aad:      3c 2f        cmp    $0x2f,%al
402aaf:74 08        je     0x402ab9
402ab1:      3c 5c        cmp    $0x5c,%al
402ab3:      0f 85 72 06 00 00    jne    0x40312b
402ab9:      8b 55 c8      mov    -0x38(%ebp),%edx
402abc:      0f b6 75 a3     movzbl -0x5d(%ebp),%esi
402ac0:      eb 02        jmp    0x402ac4

```

```

402ac2:      89 c6      mov  %eax,%esi
402ac4:      83 c2 01    add  $0x1,%edx
402ac7:      0f b6 02    movzbl (%edx),%eax
402aca:      3c 2f      cmp  $0x2f,%al
402acc:      0f 94 c3    sete %bl
402acf: 3c 5c      cmp  $0x5c,%al
402ad1:      0f 94 c1    sete %cl
402ad4:      08 cb      or   %cl,%bl
402ad6:      75 ea      jne  0x402ac2
402ad8:      89 f0      mov  %esi,%eax
402ada:      89 55 c8    mov  %edx,-0x38(%ebp)
402add:      88 45 a3    mov  %al,-0x5d(%ebp)
402ae0:      8b 45 d4    mov  -0x2c(%ebp),%eax
402ae3:      89 45 a4    mov  %eax,-0x5c(%ebp)
402ae6:      8b 45 e0    mov  -0x20(%ebp),%eax
402ae9:      8b 7d d0    mov  -0x30(%ebp),%edi
402aec:      c7 45 cc 02 00 00 00    movl $0x2,-0x34(%ebp)
402af3: 89 45 bc    mov  %eax,-0x44(%ebp)
402af6: 8b 00      mov  (%eax),%eax
402af8: 81 e7 00 80 00 00    and  $0x8000,%edi
402afe: 89 7d d4    mov  %edi,-0x2c(%ebp)
402b01:      85 c0      test %eax,%eax
402b03:      0f 84 11 05 00 00    je   0x40301a
402b09:      89 04 24    mov  %eax,(%esp)
402b0c:      e8 cf 0d 00 00    call 0x4038e0
402b11:      85 c0      test %eax,%eax
402b13:      89 c7      mov  %eax,%edi
402b15:      0f 84 b8 04 00 00    je   0x402fd3
402b1b:      8b 45 a4    mov  -0x5c(%ebp),%eax
402b1e:      85 c0      test %eax,%eax
402b20:      0f 84 74 05 00 00    je   0x40309a
402b26:      8b 45 bc    mov  -0x44(%ebp),%eax
402b29:      8b 00      mov  (%eax),%eax
402b2b:      89 04 24    mov  %eax,(%esp)
402b2e:      e8 3d 11 00 00    call 0x403c70
402b33:      89 45 c0    mov  %eax,-0x40(%ebp)
402b36:      8b 45 c0    mov  -0x40(%ebp),%eax
402b39:      c7 45 b8 00 00 00 00    movl $0x0,-0x48(%ebp)
402b40:      83 c0 02    add  $0x2,%eax
402b43:      89 45 ac    mov  %eax,-0x54(%ebp)
402b46:      8d 76 00    lea  0x0(%esi),%esi
402b49:      8d bc 27 00 00 00 00    lea  0x0(%edi,%eiz,1),%edi
402b50:      89 3c 24    mov  %edi,(%esp)
402b53:      e8 48 0f 00 00    call 0x403aa0
402b58:      85 c0      test %eax,%eax
402b5a:      89 c6      mov  %eax,%esi
402b5c:      0f 84 11 04 00 00    je   0x402f73
402b62:      8b 45 d4    mov  -0x2c(%ebp),%eax
402b65:      85 c0      test %eax,%eax
402b67:      74 06      je   0x402b6f
402b69:      83 7e 08 10    cmpl $0x10,0x8(%esi)
402b6d:      75 e1      jne  0x402b50
402b6f:      8d 5e 0c    lea  0xc(%esi),%ebx

```

```

402b72:    8b 4d d0      mov  -0x30(%ebp),%ecx
402b75:    8b 45 c8      mov  -0x38(%ebp),%eax
402b78:    89 da        mov  %ebx,%edx
402b7a:    e8 31 fb ff  call 0x4026b0
402b7f:    85 c0        test %eax,%eax
402b81:    75 cd        jne  0x402b50
402b83:    0f b7 56 06   movzwl 0x6(%esi),%edx
402b87:    8b 45 ac      mov  -0x54(%ebp),%eax
402b8a:    89 65 b0      mov  %esp,-0x50(%ebp)
402b8d:    8d 44 02 0f   lea  0xf(%edx,%eax,1),%eax
402b91:    c1 e8 04      shr  $0x4,%eax
402b94:    c1 e0 04      shl  $0x4,%eax
402b97:    e8 a4 f6 ff  call 0x402240
402b9c:    29 c4        sub  %eax,%esp
402b9e:    8b 45 c0      mov  -0x40(%ebp),%eax
402ba1:    c7 45 b4 00 00 00 00  movl $0x0,-0x4c(%ebp)
402ba8:    8d 74 24 0c   lea  0xc(%esp),%esi
402bac:    85 c0        test %eax,%eax
402bae:    0f 85 7c 04 00 00    jne  0x403030
402bb4:    8b 45 b4      mov  -0x4c(%ebp),%eax
402bb7:    83 c2 01      add  $0x1,%edx
402bba:    89 5c 24 04   mov  %ebx,0x4(%esp)
402bbe:    89 54 24 08   mov  %edx,0x8(%esp)
402bc2:    89 e3        mov  %esp,%ebx
402bc4:    01 f0        add  %esi,%eax
402bc6:    89 04 24      mov  %eax,(%esp)
402bc9:    e8 f2 10 00 00    call 0x403cc0
402bce:    89 34 24      mov  %esi,(%esp)
402bd1:    e8 9a 10 00 00    call 0x403c70
402bd6:    83 c0 10      add  $0x10,%eax
402bd9:    c1 e8 04      shr  $0x4,%eax
402bdc:    c1 e0 04      shl  $0x4,%eax
402bdf:    e8 5c f6 ff  call 0x402240
402be4:    29 c4        sub  %eax,%esp
402be6:    89 f0        mov  %esi,%eax
402be8:    8d 4c 24 0c   lea  0xc(%esp),%ecx
402bec:    89 ce        mov  %ecx,%esi
402bee:    eb 0d        jmp  0x402bfd
402bf0:    83 c6 01      add  $0x1,%esi
402bf3:    83 c0 01      add  $0x1,%eax
402bf6:    84 d2        test %dl,%dl
402bf8:    88 56 ff      mov  %dl,-0x1(%esi)
402bfb:    74 1c        je   0x402c19
402bfd:    0f b6 10      movzbl (%eax),%edx
402c00:    80 fa 7f      cmp  $0x7f,%dl
402c03:    75 eb        jne  0x402bf0
402c05:    0f b6 50 01   movzbl 0x1(%eax),%edx
402c09:    83 c0 01      add  $0x1,%eax
402c0c:    83 c6 01      add  $0x1,%esi
402c0f: 83 c0 01      add  $0x1,%eax
402c12:    84 d2        test %dl,%dl
402c14:    88 56 ff      mov  %dl,-0x1(%esi)
402c17:    75 e4        jne  0x402bfd

```

```

402c19: 89 0c 24      mov  %ecx,(%esp)
402c1c: e8 af 11 00 00      call 0x403dd0
402c21: 85 c0         test %eax,%eax
402c23: 89 c6         mov  %eax,%esi
402c25: 89 dc         mov  %ebx,%esp
402c27: 0f 84 47 04 00 00    je  0x403074
402c2d: 8b 5d cc      mov  -0x34(%ebp),%ebx
402c30: 83 fb 02      cmp  $0x2,%ebx
402c33: 0f 94 c0      sete %al
402c36: 0f b6 c0      movzbl %al,%eax
402c39: 83 e8 01      sub  $0x1,%eax
402c3c: 21 c3         and  %eax,%ebx
402c3e: 8b 45 d0      mov  -0x30(%ebp),%eax
402c41: 89 5d cc      mov  %ebx,-0x34(%ebp)
402c44: a8 40         test $0x40,%al
402c46: 0f 85 74 03 00 00    jne 0x402fc0
402c4c: 8b 5d b8      mov  -0x48(%ebp),%ebx
402c4f:85 db         test %ebx,%ebx
402c51: 0f 84 ae 04 00 00    je  0x403105
402c57: 25 00 40 00 00      and  $0x4000,%eax
402c5c: 89 7d b4      mov  %edi,-0x4c(%ebp)
402c5f:89 c7         mov  %eax,%edi
402c61: eb 14         jmp  0x402c77
402c63: e8 10 10 00 00      call 0x403c78
402c68: 85 c0         test %eax,%eax
402c6a: 8b 13         mov  (%ebx),%edx
402c6c: 8b 4b 04      mov  0x4(%ebx),%ecx
402c6f:7e 22         jle  0x402c93
402c71: 85 c9         test %ecx,%ecx
402c73: 74 24         je   0x402c99
402c75: 89 cb         mov  %ecx,%ebx
402c77: 8b 43 08      mov  0x8(%ebx),%eax
402c7a: 85 ff         test %edi,%edi
402c7c: 89 34 24      mov  %esi,(%esp)
402c7f:89 44 24 04    mov  %eax,0x4(%esp)
402c83: 75 de         jne  0x402c63
402c85: e8 3e 11 00 00      call 0x403dc8
402c8a: 85 c0         test %eax,%eax
402c8c: 8b 13         mov  (%ebx),%edx
402c8e: 8b 4b 04      mov  0x4(%ebx),%ecx
402c91: 7f de         jg   0x402c71
402c93: 89 d1         mov  %edx,%ecx
402c95: 85 c9         test %ecx,%ecx
402c97: 75 dc         jne  0x402c75
402c99: 8b 7d b4      mov  -0x4c(%ebp),%edi
402c9c: 89 45 b4      mov  %eax,-0x4c(%ebp)
402c9f:c7 04 24 0c 00 00 00 movl $0xc,(%esp)
402ca6: e8 25 10 00 00      call 0x403cd0
402cab: 85 c0         test %eax,%eax
402cad: 0f 84 18 03 00 00    je  0x402fcb
402cb3: 8b 55 b4      mov  -0x4c(%ebp),%edx
402cb6: 89 70 08      mov  %esi,0x8(%eax)
402cb9: c7 40 04 00 00 00 00 movl $0x0,0x4(%eax)

```

```

402cc0:    c7 00 00 00 00 00    movl $0x0,(%eax)
402cc6:    85 d2                test %edx,%edx
402cc8:    0f 8e d8 03 00 00    jle 0x4030a6
402cce:    89 43 04            mov  %eax,0x4(%ebx)
402cd1:    e9 f5 02 00 00      jmp 0x402fcb
402cd6:    c7 45 cc 01 00 00 00    movl $0x1,-0x34(%ebp)
402cdd:    8d 76 00            lea 0x0(%esi),%esi
402ce0:    8b 65 a8            mov -0x58(%ebp),%esp
402ce3:    8b 45 cc            mov -0x34(%ebp),%eax
402ce6:    8d 65 f4            lea -0xc(%ebp),%esp
402ce9:    5b                  pop  %ebx
402cea:    5e                  pop  %esi
402ceb:    5f                  pop  %edi
402cec:    5d                  pop  %ebp
402ced:    c3                  ret
402cee:    66 90              xchg %ax,%ax
402cf0:89 65 c0            mov  %esp,-0x40(%ebp)
402cf3:89 04 24            mov  %eax,(%esp)
402cf6:e8 75 0f 00 00      call 0x403c70
402cfb:83 c0 10            add  $0x10,%eax
402cfe:c1 e8 04            shr  $0x4,%eax
402d01:    c1 e0 04            shl  $0x4,%eax
402d04:    e8 37 f5 ff ff      call 0x402240
402d09:    29 c4              sub  %eax,%esp
402d0b:    89 de              mov  %ebx,%esi
402d0d:    8d 44 24 0c        lea 0xc(%esp),%eax
402d11:    89 c7              mov  %eax,%edi
402d13:    89 45 c8            mov  %eax,-0x38(%ebp)
402d16:    0f b6 03            movzbl (%ebx),%eax
402d19:    3c 7f              cmp  $0x7f,%al
402d1b:    74 28              je   0x402d45
402d1d:    3c 7b              cmp  $0x7b,%al
402d1f:    74 3f              je   0x402d60
402d21:    84 c0              test %al,%al
402d23:    8d 57 01            lea 0x1(%edi),%edx
402d26:    8d 4e 01            lea 0x1(%esi),%ecx
402d29:    88 07              mov  %al,(%edi)
402d2b:    0f 84 bc 04 00 00    je   0x4031ed
402d31:    3c 7b              cmp  $0x7b,%al
402d33:    0f 84 b4 04 00 00    je   0x4031ed
402d39:    0f b6 46 01        movzbl 0x1(%esi),%eax
402d3d:    89 d7              mov  %edx,%edi
402d3f:    89 ce              mov  %ecx,%esi
402d41:    3c 7f              cmp  $0x7f,%al
402d43:    75 d8              jne 0x402d1d
402d45:    0f b6 46 01        movzbl 0x1(%esi),%eax
402d49:    c6 07 7f            movb $0x7f,(%edi)
402d4c:    84 c0              test %al,%al
402d4e:    0f 85 ac 00 00 00    jne 0x402e00
402d54:    83 c7 01            add  $0x1,%edi
402d57:    83 c6 01            add  $0x1,%esi
402d5a:    eb c5              jmp 0x402d21
402d5c:    8d 74 26 00        lea 0x0(%esi,%eiz,1),%esi

```

```

402d60: 89 7d cc      mov  %edi,-0x34(%ebp)
402d63: 89 f7         mov  %esi,%edi
402d65: 8b 55 cc      mov  -0x34(%ebp),%edx
402d68: b9 01 00 00 00      mov  $0x1,%ecx
402d6d: 0f b6 47 01    movzbl 0x1(%edi),%eax
402d71: 3c 7f         cmp  $0x7f,%al
402d73: 74 26         je   0x402d9b
402d75: 83 c7 01      add  $0x1,%edi
402d78: 3c 7d         cmp  $0x7d,%al
402d7a: 74 09         je   0x402d85
402d7c: 3c 2c         cmp  $0x2c,%al
402d7e: 75 40         jne  0x402dc0
402d80: 83 f9 01      cmp  $0x1,%ecx
402d83: 75 3b         jne  0x402dc0
402d85: 83 e9 01      sub  $0x1,%ecx
402d88: 0f 84 83 00 00 00    je   0x402e11
402d8e: 88 02         mov  %al,(%edx)
402d90: 0f b6 47 01    movzbl 0x1(%edi),%eax
402d94: 83 c2 01      add  $0x1,%edx
402d97: 3c 7f         cmp  $0x7f,%al
402d99: 75 da         jne  0x402d75
402d9b: 0f b6 47 02    movzbl 0x2(%edi),%eax
402d9f: c6 02 7f      movb  $0x7f,(%edx)
402da2: 8d 5a 02      lea  0x2(%edx),%ebx
402da5: 84 c0         test %al,%al
402da7: 88 42 01      mov  %al,0x1(%edx)
402daa: 75 34         jne  0x402de0
402dac: c6 42 02 00    movb  $0x0,0x2(%edx)
402db0: c7 45 cc 01 00 00 00  movl $0x1,-0x34(%ebp)
402db7: e9 0e 01 00 00    jmp  0x402eca
402dbc: 8d 74 26 00    lea  0x0(%esi,%eiz,1),%esi
402dc0: 3c 7b         cmp  $0x7b,%al
402dc2: 74 2c         je   0x402df0
402dc4: 84 c0         test %al,%al
402dc6: 0f 95 45 d4    setne -0x2c(%ebp)
402dca: 0f b6 5d d4    movzbl -0x2c(%ebp),%ebx
402dce: 84 db         test %bl,%bl
402dd0: 8d 72 01      lea  0x1(%edx),%esi
402dd3: 88 02         mov  %al,(%edx)
402dd5: 0f 84 f9 03 00 00    je   0x4031d4
402ddb: 89 f2         mov  %esi,%edx
402ddd: eb 8e         jmp  0x402d6d
402ddf: 90           nop
402de0: 0f b6 47 03    movzbl 0x3(%edi),%eax
402de4: 89 da         mov  %ebx,%edx
402de6: 83 c7 03      add  $0x3,%edi
402de9: eb 8d         jmp  0x402d78
402deb: 90           nop
402dec: 8d 74 26 00    lea  0x0(%esi,%eiz,1),%esi
402df0: 83 c1 01      add  $0x1,%ecx
402df3: bb 01 00 00 00    mov  $0x1,%ebx
402df8: c6 45 d4 01    movb  $0x1,-0x2c(%ebp)
402dfc: eb d0         jmp  0x402dce

```

402dfe:	66 90	xchg %ax,%ax
402e00:	88 47 01	mov %al,0x1(%edi)
402e03:	83 c6 02	add \$0x2,%esi
402e06:	0f b6 06	movzbl (%esi),%eax
402e09:	83 c7 02	add \$0x2,%edi
402e0c:	e9 08 ff ff	jmp 0x402d19
402e11:	3c 2c	cmp \$0x2c,%al
402e13:	0f 85 c1 00 00 00	jne 0x402eda
402e19:	89 f8	mov %edi,%eax
402e1b:	be 01 00 00 00	mov \$0x1,%esi
402e20:	0f b6 58 01	movzbl 0x1(%eax),%ebx
402e24:	8d 48 01	lea 0x1(%eax),%ecx
402e27:	80 fb 7f	cmp \$0x7f,%bl
402e2a:	0f 85 1f 01 00 00	jne 0x402f4f
402e30:	80 78 02 00	cmpb \$0x0,0x2(%eax)
402e34:	75 12	jne 0x402e48
402e36:	e9 85 00 00 00	jmp 0x402ec0
402e3b:	90	nop
402e3c:	8d 74 26 00	lea 0x0(%esi,%eiz,1),%esi
402e40:	80 78 01 00	cmpb \$0x0,0x1(%eax)
402e44:	74 7a	je 0x402ec0
402e46:	89 c1	mov %eax,%ecx
402e48:	0f b6 59 02	movzbl 0x2(%ecx),%ebx
402e4c:	8d 41 02	lea 0x2(%ecx),%eax
402e4f:	80 fb 7f	cmp \$0x7f,%bl
402e52:	74 ec	je 0x402e40
402e54:	80 fb 7b	cmp \$0x7b,%bl
402e57:	74 79	je 0x402ed2
402e59:	80 fb 7d	cmp \$0x7d,%bl
402e5c:	75 55	jne 0x402eb3
402e5e:	83 ee 01	sub \$0x1,%esi
402e61:	75 bd	jne 0x402e20
402e63:	8d 48 01	lea 0x1(%eax),%ecx
402e66:	0f b6 40 01	movzbl 0x1(%eax),%eax
402e6a:	eb 07	jmp 0x402e73
402e6c:	8d 74 26 00	lea 0x0(%esi,%eiz,1),%esi
402e70:	0f b6 01	movzbl (%ecx),%eax
402e73:	83 c2 01	add \$0x1,%edx
402e76:	83 c1 01	add \$0x1,%ecx
402e79:	84 c0	test %al,%al
402e7b:	88 42 ff	mov %al,-0x1(%edx)
402e7e:	75 f0	jne 0x402e70
402e80:	8b 45 08	mov 0x8(%ebp),%eax
402e83:	89 04 24	mov %eax,(%esp)
402e86:	8b 75 d0	mov -0x30(%ebp),%esi
402e89:	8b 4d c4	mov -0x3c(%ebp),%ecx
402e8c:	8b 45 c8	mov -0x38(%ebp),%eax
402e8f:	89 f2	mov %esi,%edx
402e91:	83 ce 01	or \$0x1,%esi
402e94:	e8 e7 fa ff ff	call 0x402980
402e99:	83 f8 01	cmp \$0x1,%eax
402e9c:	89 75 d0	mov %esi,-0x30(%ebp)
402e9f:	0f 84 0b ff ff ff	je 0x402db0


```

402ea5: 80 3f 2c      cmpb $0x2c,(%edi)
402ea8: 0f 84 b7 fe ff je 0x402d65
402eae: 89 45 cc      mov %eax,-0x34(%ebp)
402eb1: eb 17        jmp 0x402eca
402eb3: 84 db        test %bl,%bl
402eb5: 0f 85 65 ff ff jne 0x402e20
402ebb: 90          nop
402ebc: 8d 74 26 00   lea 0x0(%esi,%eiz,1),%esi
402ec0: c6 02 00      movb $0x0,(%edx)
402ec3: c7 45 cc 01 00 00 00 movl $0x1,-0x34(%ebp)
402eca: 8b 65 c0      mov -0x40(%ebp),%esp
402ecd: e9 11 fe ff ff jmp 0x402ce3
402ed2: 83 c6 01      add $0x1,%esi
402ed5: e9 46 ff ff ff jmp 0x402e20
402eda: 89 f8        mov %edi,%eax
402edc: eb 85        jmp 0x402e63
402ede: 8b 45 d4      mov -0x2c(%ebp),%eax
402ee1: 89 e6        mov %esp,%esi
402ee3: 89 04 24      mov %eax,(%esp)
402ee6: e8 85 0d 00 00 call 0x403c70
402eeb: 83 c0 10      add $0x10,%eax
402eee: c1 e8 04      shr $0x4,%eax
402ef1: c1 e0 04      shl $0x4,%eax
402ef4: e8 47 f3 ff ff call 0x402240
402ef9: 8b 55 d4      mov -0x2c(%ebp),%edx
402efc: 29 c4        sub %eax,%esp
402efe: 8d 7c 24 0c   lea 0xc(%esp),%edi
402f02: 89 f9        mov %edi,%ecx
402f04: eb 17        jmp 0x402f1d
402f06: 8d 76 00      lea 0x0(%esi),%esi
402f09: 8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
402f10: 83 c1 01      add $0x1,%ecx
402f13: 83 c2 01      add $0x1,%edx
402f16: 84 c0        test %al,%al
402f18: 88 41 ff      mov %al,-0x1(%ecx)
402f1b: 74 10        je 0x402f2d
402f1d: 0f b6 02      movzbl (%edx),%eax
402f20: 3c 7f        cmp $0x7f,%al
402f22: 75 ec        jne 0x402f10
402f24: 0f b6 42 01   movzbl 0x1(%edx),%eax
402f28: 83 c2 01      add $0x1,%edx
402f2b: eb e3        jmp 0x402f10
402f2d: 89 3c 24      mov %edi,(%esp)
402f30: e8 9b 0e 00 00 call 0x403dd0
402f35: 85 c0        test %eax,%eax
402f37: 89 f4        mov %esi,%esp
402f39: 0f 84 97 fd ff je 0x402cd6
402f3f: 8d 55 d8      lea -0x28(%ebp),%edx
402f42: e8 89 f9 ff ff call 0x4028d0
402f47: 89 45 cc      mov %eax,-0x34(%ebp)
402f4a: e9 d0 fa ff ff jmp 0x402a1f
402f4f: 89 c8        mov %ecx,%eax
402f51: e9 fe ff ff ff jmp 0x402e54

```

```

402f56:      f6 45 d0 10      testb $0x10,-0x30(%ebp)
402f5a:0f 85 da 01 00 00      jne 0x40313a
402f60:      89 5d c8      mov %ebx,-0x38(%ebp)
402f63:      c6 45 a3 5c      movb $0x5c,-0x5d(%ebp)
402f67:      c7 45 a4 00 00 00 00      movl $0x0,-0x5c(%ebp)
402f6e:      e9 73 fb ff ff      jmp 0x402ae6
402f73:      89 3c 24      mov %edi,(%esp)
402f76:      e8 75 0b 00 00      call 0x403af0
402f7b:      8b 55 b8      mov -0x48(%ebp),%edx
402f7e:      85 d2      test %edx,%edx
402f80:      74 0b      je 0x402f8d
402f82:      8b 55 08      mov 0x8(%ebp),%edx
402f85:      8b 45 b8      mov -0x48(%ebp),%eax
402f88:      e8 a3 f9 ff ff      call 0x402930
402f8d:      8b 7d bc      mov -0x44(%ebp),%edi
402f90:      8d 5f 04      lea 0x4(%edi),%ebx
402f93:      8b 43 fc      mov -0x4(%ebx),%eax
402f96:      89 04 24      mov %eax,(%esp)
402f99:      e8 42 0d 00 00      call 0x403ce0
402f9e:      8b 47 04      mov 0x4(%edi),%eax
402fa1:85 c0      test %eax,%eax
402fa3:0f 84 12 01 00 00      je 0x4030bb
402fa9:83 7d cc 01      cmpl $0x1,-0x34(%ebp)
402fad:      74 47      je 0x402ff6
402faf:89 5d bc      mov %ebx,-0x44(%ebp)
402fb2:      e9 52 fb ff ff      jmp 0x402b09
402fb7:      89 f6      mov %esi,%esi
402fb9:      8d bc 27 00 00 00 00      lea 0x0(%edi,%eiz,1),%edi
402fc0:8b 4d 08      mov 0x8(%ebp),%ecx
402fc3:85 c9      test %ecx,%ecx
402fc5:0f 85 c0 00 00 00      jne 0x40308b
402fcb:8b 65 b0      mov -0x50(%ebp),%esp
402fce:e9 7d fb ff ff      jmp 0x402b50
402fd3:      f6 45 d0 04      testb $0x4,-0x30(%ebp)
402fd7:      0f 84 e9 00 00 00      je 0x4030c6
402fdd:      8b 7d bc      mov -0x44(%ebp),%edi
402fe0:      8d 5f 04      lea 0x4(%edi),%ebx
402fe3:      89 f8      mov %edi,%eax
402fe5:      8b 00      mov (%eax),%eax
402fe7:      89 04 24      mov %eax,(%esp)
402fea:e8 f1 0c 00 00      call 0x403ce0
402fef:8b 47 04      mov 0x4(%edi),%eax
402ff2:85 c0      test %eax,%eax
402ff4:74 17      je 0x40300d
402ff6:8b 45 bc      mov -0x44(%ebp),%eax
402ff9:8b 40 04      mov 0x4(%eax),%eax
402ffc:83 c3 04      add $0x4,%ebx
402fff:89 04 24      mov %eax,(%esp)
403002:      e8 d9 0c 00 00      call 0x403ce0
403007:      8b 03      mov (%ebx),%eax
403009:      85 c0      test %eax,%eax
40300b:      75 ef      jne 0x402ffc
40300d:      8b 45 e0      mov -0x20(%ebp),%eax

```

```

403010: c7 45 cc 01 00 00 00    movl $0x1,-0x34(%ebp)
403017: 89 45 bc                mov  %eax,-0x44(%ebp)
40301a: 8b 45 bc                mov  -0x44(%ebp),%eax
40301d: 89 04 24                mov  %eax,(%esp)
403020: e8 bb 0c 00 00          call 0x403ce0
403025: 8b 65 a8                mov  -0x58(%ebp),%esp
403028: e9 b6 fc ff ff          jmp  0x402ce3
40302d: 8d 76 00                lea  0x0(%esi),%esi
403030: 8b 45 bc                mov  -0x44(%ebp),%eax
403033: 89 55 b4                mov  %edx,-0x4c(%ebp)
403036: 8b 55 c0                mov  -0x40(%ebp),%edx
403039: 8b 00                  mov  (%eax),%eax
40303b: 89 34 24                mov  %esi,(%esp)
40303e: 89 54 24 08            mov  %edx,0x8(%esp)
403042: 89 44 24 04            mov  %eax,0x4(%esp)
403046: e8 75 0c 00 00          call 0x403cc0
40304b: 8b 4d c0                mov  -0x40(%ebp),%ecx
40304e: 8b 55 b4                mov  -0x4c(%ebp),%edx
403051: 0f b6 44 0c 0b          movzbl 0xb(%esp,%ecx,1),%eax
403056: 3c 2f                  cmp  $0x2f,%al
403058: 74 26                  je   0x403080
40305a: 3c 5c                  cmp  $0x5c,%al
40305c: 74 22                  je   0x403080
40305e: 89 c8                  mov  %ecx,%eax
403060: 83 c0 01              add  $0x1,%eax
403063: 89 45 b4                mov  %eax,-0x4c(%ebp)
403066: 89 c8                  mov  %ecx,%eax
403068: 0f b6 4d a3            movzbl -0x5d(%ebp),%ecx
40306c: 88 0c 06              mov  %cl,(%esi,%eax,1)
40306f: e9 40 fb ff ff          jmp  0x402bb4
403074: c7 45 cc 03 00 00 00    movl $0x3,-0x34(%ebp)
40307b: e9 4b ff ff ff          jmp  0x402fcb
403080: 8b 45 c0                mov  -0x40(%ebp),%eax
403083: 89 45 b4                mov  %eax,-0x4c(%ebp)
403086: e9 29 fb ff ff          jmp  0x402bb4
40308b: 8b 55 08                mov  0x8(%ebp),%edx
40308e: 89 f0                  mov  %esi,%eax
403090: e8 3b f8 ff ff          call 0x4028d0
403095: e9 31 ff ff ff          jmp  0x402fcb
40309a: c7 45 c0 00 00 00 00    movl $0x0,-0x40(%ebp)
4030a1: e9 90 fa ff ff          jmp  0x402b36
4030a6: 89 03                  mov  %eax,(%ebx)
4030a8: 8b 5d b8                mov  -0x48(%ebp),%ebx
4030ab: 85 db                  test %ebx,%ebx
4030ad: 0f 85 18 ff ff ff      jne  0x402fcb
4030b3: 89 45 b8                mov  %eax,-0x48(%ebp)
4030b6: e9 10 ff ff ff          jmp  0x402fcb
4030bb: 8b 45 e0                mov  -0x20(%ebp),%eax
4030be: 89 45 bc                mov  %eax,-0x44(%ebp)
4030c1: e9 54 ff ff ff          jmp  0x40301a
4030c6: 8b 7d c4                mov  -0x3c(%ebp),%edi
4030c9: 85 ff                  test %edi,%edi
4030cb: 0f 84 bc fe ff ff      je   0x402f8d

```

```

4030d1:    e8 3a 0c 00 00        call 0x403d10
4030d6:    8b 00                 mov  (%eax),%eax
4030d8:    89 44 24 04          mov  %eax,0x4(%esp)
4030dc:    8b 75 bc             mov  -0x44(%ebp),%esi
4030df:    8b 06                 mov  (%esi),%eax
4030e1:    89 04 24             mov  %eax,(%esp)
4030e4:    ff d7                call *%edi
4030e6:    85 c0                 test %eax,%eax
4030e8:    0f 84 9f fe ff ff    je   0x402f8d
4030ee:    89 f0                 mov  %esi,%eax
4030f0:    8d 5e 04             lea  0x4(%esi),%ebx
4030f3:    89 f7                 mov  %esi,%edi
4030f5:    e9 eb fe ff ff      jmp  0x402fe5
4030fa:89 55 c8             mov  %edx,-0x38(%ebp)
4030fd:    88 4d a3             mov  %cl,-0x5d(%ebp)
403100:    e9 a4 f9 ff ff      jmp  0x402aa9
403105:    c7 04 24 0c 00 00 00 movl $0xc,(%esp)
40310c:    e8 bf 0b 00 00      call 0x403cd0
403111:    85 c0                 test %eax,%eax
403113:    0f 84 b2 fe ff ff    je   0x402fcb
403119:    89 70 08             mov  %esi,0x8(%eax)
40311c:    c7 40 04 00 00 00 00 movl $0x0,0x4(%eax)
403123:    c7 00 00 00 00 00 00 movl $0x0,(%eax)
403129:    eb 88                jmp  0x4030b3
40312b:    8b 45 d4             mov  -0x2c(%ebp),%eax
40312e:    c6 45 a3 5c          movb $0x5c,-0x5d(%ebp)
403132:    89 45 a4             mov  %eax,-0x5c(%ebp)
403135:    e9 ac f9 ff ff      jmp  0x402ae6
40313a:    8b 55 d0             mov  -0x30(%ebp),%edx
40313d:    89 d8                 mov  %ebx,%eax
40313f:    e8 9c f1 ff ff      call 0x4022e0
403144:    85 c0                 test %eax,%eax
403146:    89 45 cc             mov  %eax,-0x34(%ebp)
403149:    0f 85 11 fe ff ff    jne  0x402f60
40314f:    89 1c 24             mov  %ebx,(%esp)
403152:    89 e6                 mov  %esp,%esi
403154:    e8 17 0b 00 00      call 0x403c70
403159:    83 c0 10             add  $0x10,%eax
40315c:    c1 e8 04             shr  $0x4,%eax
40315f:    c1 e0 04             shl  $0x4,%eax
403162:    e8 d9 f0 ff ff      call 0x402240
403167:    29 c4                 sub  %eax,%esp
403169:    8d 4c 24 0c          lea  0xc(%esp),%ecx
40316d:    89 ca                 mov  %ecx,%edx
40316f:    eb 0d                jmp  0x40317e
403171:    83 c2 01             add  $0x1,%edx
403174:    83 c3 01             add  $0x1,%ebx
403177:    84 c0                 test %al,%al
403179:    88 42 ff             mov  %al,-0x1(%edx)
40317c:    74 10                 je   0x40318e
40317e:    0f b6 03             movzbl (%ebx),%eax
403181:    3c 7f                 cmp  $0x7f,%al
403183:    75 ec                 jne  0x403171

```

```

403185:    0f b6 43 01    movzbl 0x1(%ebx),%eax
403189:    83 c3 01       add $0x1,%ebx
40318c:    eb e3         jmp 0x403171
40318e:    89 0c 24       mov %ecx,(%esp)
403191:    e8 3a 0c 00 00    call 0x403dd0
403196:    85 c0         test %eax,%eax
403198:    89 f4         mov %esi,%esp
40319a:    0f 84 1b ff ff ff    je 0x4030bb
4031a0:    8b 55 08       mov 0x8(%ebp),%edx
4031a3:    85 d2         test %edx,%edx
4031a5:    0f 84 10 ff ff ff    je 0x4030bb
4031ab:    8b 55 08       mov 0x8(%ebp),%edx
4031ae:    e8 1d f7 ff ff    call 0x4028d0
4031b3:    8b 45 e0       mov -0x20(%ebp),%eax
4031b6:    89 45 bc       mov %eax,-0x44(%ebp)
4031b9:    e9 5c fe ff ff    jmp 0x40301a
4031be:    89 45 c8       mov %eax,-0x38(%ebp)
4031c1:    e9 e3 f8 ff ff    jmp 0x402aa9
4031c6:    0f b6 18       movzbl (%eax),%ebx
4031c9:    89 45 c8       mov %eax,-0x38(%ebp)
4031cc:    88 5d a3       mov %bl,-0x5d(%ebp)
4031cf:e9 d5 f8 ff ff    jmp 0x402aa9
4031d4:    80 7d d4 00     cmpb $0x0,-0x2c(%ebp)
4031d8:    0f 84 d2 fb ff ff    je 0x402db0
4031de:    3c 2c         cmp $0x2c,%al
4031e0:    89 f2         mov %esi,%edx
4031e2:    0f 85 d8 fc ff ff    jne 0x402ec0
4031e8:    e9 2c fc ff ff    jmp 0x402e19
4031ed:    3c 7b         cmp $0x7b,%al
4031ef:    74 08         je 0x4031f9
4031f1:    8b 65 c0       mov -0x40(%ebp),%esp
4031f4:    e9 a1 f7 ff ff    jmp 0x40299a
4031f9:    89 55 cc       mov %edx,-0x34(%ebp)
4031fc:89 cf         mov %ecx,%edi
4031fe:    e9 62 fb ff ff    jmp 0x402d65
403203:    8d b6 00 00 00 00    lea 0x0(%esi),%esi
403209:    8d bc 27 00 00 00 00    lea 0x0(%edi,%eiz,1),%edi
403210:    55           push %ebp
403211:    89 e5         mov %esp,%ebp
403213:    57           push %edi
403214:    56           push %esi
403215:    53           push %ebx
403216:    83 ec 2c     sub $0x2c,%esp
403219:    8b 75 14     mov 0x14(%ebp),%esi
40321c:    8b 5d 08     mov 0x8(%ebp),%ebx
40321f:    8b 7d 0c     mov 0xc(%ebp),%edi
403222:    85 f6         test %esi,%esi
403224:    74 08         je 0x40322e
403226:    f7 c7 02 00 00 00    test $0x2,%edi
40322c:    74 35         je 0x403263
40322e:    81 3e 7e 51 40 00    cmpl $0x40517e,(%esi)
403234:    74 0d         je 0x403243
403236:    89 f0         mov %esi,%eax

```

```

403238: e8 43 f1 ff ff    call 0x402380
40323d: c7 06 7e 51 40 00    movl $0x40517e,(%esi)
403243: 89 34 24          mov  %esi,(%esp)
403246: 8b 4d 10          mov  0x10(%ebp),%ecx
403249: 89 fa            mov  %edi,%edx
40324b: 89 d8            mov  %ebx,%eax
40324d: e8 2e f7 ff ff    call 0x402980
403252: 83 f8 02          cmp  $0x2,%eax
403255: 89 c1            mov  %eax,%ecx
403257: 74 17            je   0x403270
403259: 8d 65 f4          lea  -0xc(%ebp),%esp
40325c: 89 c8            mov  %ecx,%eax
40325e: 5b              pop  %ebx
40325f: 5e              pop  %esi
403260: 5f              pop  %edi
403261: 5d              pop  %ebp
403262: c3              ret
403263: c7 46 0c 00 00 00 00    movl $0x0,0xc(%esi)
40326a: eb c2            jmp  0x40322e
40326c: 8d 74 26 00       lea  0x0(%esi,%eiz,1),%esi
403270: 83 e7 10          and  $0x10,%edi
403273: 74 e4            je   0x403259
403275: 89 45 e0          mov  %eax,-0x20(%ebp)
403278: 89 65 e4          mov  %esp,-0x1c(%ebp)
40327b: 89 1c 24          mov  %ebx,(%esp)
40327e: e8 ed 09 00 00    call 0x403c70
403283: 83 c0 10          add  $0x10,%eax
403286: c1 e8 04          shr  $0x4,%eax
403289: c1 e0 04          shl  $0x4,%eax
40328c: e8 af ef ff ff    call 0x402240
403291: 8b 4d e0          mov  -0x20(%ebp),%ecx
403294: 29 c4            sub  %eax,%esp
403296: 8d 7c 24 04       lea  0x4(%esp),%edi
40329a: 89 fa            mov  %edi,%edx
40329c: eb 0f            jmp  0x4032ad
40329e: 66 90            xchg %ax,%ax
4032a0: 83 c2 01          add  $0x1,%edx
4032a3: 83 c3 01          add  $0x1,%ebx
4032a6: 84 c0            test %al,%al
4032a8: 88 42 ff          mov  %al,-0x1(%edx)
4032ab: 74 1b            je   0x4032c8
4032ad: 0f b6 03          movzbl (%ebx),%eax
4032b0: 3c 7f            cmp  $0x7f,%al
4032b2: 75 ec            jne  0x4032a0
4032b4: 0f b6 43 01       movzbl 0x1(%ebx),%eax
4032b8: 83 c3 01          add  $0x1,%ebx
4032bb: 83 c2 01          add  $0x1,%edx
4032be: 83 c3 01          add  $0x1,%ebx
4032c1: 84 c0            test %al,%al
4032c3: 88 42 ff          mov  %al,-0x1(%edx)
4032c6: 75 e5            jne  0x4032ad
4032c8: 89 4d e0          mov  %ecx,-0x20(%ebp)
4032cb: 89 3c 24          mov  %edi,(%esp)

```

```

4032ce:    e8 fd 0a 00 00        call 0x403dd0
4032d3:    85 c0                test %eax,%eax
4032d5:    8b 65 e4            mov -0x1c(%ebp),%esp
4032d8:    8b 4d e0            mov -0x20(%ebp),%ecx
4032db:    0f 84 78 ff ff ff   je 0x403259
4032e1:    89 f2                mov %esi,%edx
4032e3:    89 4d e4            mov %ecx,-0x1c(%ebp)
4032e6:    e8 e5 f5 ff ff     call 0x4028d0
4032eb:    8b 4d e4            mov -0x1c(%ebp),%ecx
4032ee:    e9 66 ff ff ff     jmp 0x403259
4032f3:    8d b6 00 00 00 00   lea 0x0(%esi),%esi
4032f9:    8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
403300:    57                  push %edi
403301:    56                  push %esi
403302:    53                  push %ebx
403303:    83 ec 10            sub $0x10,%esp
403306:    8b 74 24 20        mov 0x20(%esp),%esi
40330a:    81 3e 7e 51 40 00   cmpl $0x40517e,(%esi)
403310:    74 0e                je 0x403320
403312:    83 c4 10            add $0x10,%esp
403315:    5b                  pop %ebx
403316:    5e                  pop %esi
403317:    5f                  pop %edi
403318:    c3                  ret
403319:    8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi
403320:    8b 46 04            mov 0x4(%esi),%eax
403323:    8b 56 0c            mov 0xc(%esi),%edx
403326:    85 c0                test %eax,%eax
403328:    8d 78 ff            lea -0x1(%eax),%edi
40332b:    8d 1c 95 00 00 00 00 lea 0x0(,%edx,4),%ebx
403332:    7e 19                jle 0x40334d
403334:    8b 46 08            mov 0x8(%esi),%eax
403337:    83 ef 01            sub $0x1,%edi
40333a:    8b 04 18            mov (%eax,%ebx,1),%eax
40333d:    83 c3 04            add $0x4,%ebx
403340:    89 04 24            mov %eax,(%esp)
403343:    e8 98 09 00 00     call 0x403ce0
403348:    83 ff ff            cmp $0xffffffff,%edi
40334b:    75 e7                jne 0x403334
40334d:    8b 46 08            mov 0x8(%esi),%eax
403350:    89 44 24 20        mov %eax,0x20(%esp)
403354:    83 c4 10            add $0x10,%esp
403357:    5b                  pop %ebx
403358:    5e                  pop %esi
403359:    5f                  pop %edi
40335a:    e9 81 09 00 00     jmp 0x403ce0
40335f:    90                  nop
403360:    55                  push %ebp
403361:    89 e5                mov %esp,%ebp
403363:    57                  push %edi
403364:    56                  push %esi
403365:    53                  push %ebx
403366:    83 ec 2c            sub $0x2c,%esp

```

```

403369: c7 44 24 04 00 00 00    movl $0x0,0x4(%esp)
403370: 00
403371: c7 04 24 02 00 00 00    movl $0x2,(%esp)
403378: e8 13 09 00 00          call 0x403c90
40337d: 85 c0                    test %eax,%eax
40337f: 89 c3                    mov  %eax,%ebx
403381: 74 0a                    je  0x40338d
403383: 89 04 24                mov  %eax,(%esp)
403386: e8 45 0a 00 00          call 0x403dd0
40338b: 89 c3                    mov  %eax,%ebx
40338d: c7 44 24 04 90 51 40    movl $0x405190,0x4(%esp)
403394: 00
403395: c7 04 24 02 00 00 00    movl $0x2,(%esp)
40339c: e8 ef 08 00 00          call 0x403c90
4033a1: 8b 75 08                mov  0x8(%ebp),%esi
4033a4: 85 f6                    test %esi,%esi
4033a6: 74 08                    je  0x4033b0
4033a8: 8b 45 08                mov  0x8(%ebp),%eax
4033ab: 80 38 00                cmpb $0x0,(%eax)
4033ae: 75 71                    jne 0x403421
4033b0: c7 44 24 08 00 00 00    movl $0x0,0x8(%esp)
4033b7: 00
4033b8: c7 44 24 04 92 51 40    movl $0x405192,0x4(%esp)
4033bf: 00
4033c0: c7 04 24 00 00 00 00    movl $0x0,(%esp)
4033c7: e8 84 08 00 00          call 0x403c50
4033cc: 8d 70 01                lea  0x1(%eax),%esi
4033cf: 89 74 24 04            mov  %esi,0x4(%esp)
4033d3: a1 68 70 40 00          mov  0x407068,%eax
4033d8: 89 04 24                mov  %eax,(%esp)
4033db: e8 c0 08 00 00          call 0x403ca0
4033e0: a3 68 70 40 00          mov  %eax,0x407068
4033e5: 89 74 24 08            mov  %esi,0x8(%esp)
4033e9: c7 44 24 04 92 51 40    movl $0x405192,0x4(%esp)
4033f0: 00
4033f1: 89 04 24                mov  %eax,(%esp)
4033f4: e8 57 08 00 00          call 0x403c50
4033f9: 89 5c 24 04            mov  %ebx,0x4(%esp)
4033fd: c7 04 24 02 00 00 00    movl $0x2,(%esp)
403404: e8 87 08 00 00          call 0x403c90
403409: 89 1c 24                mov  %ebx,(%esp)
40340c: e8 cf 08 00 00          call 0x403ce0
403411: 8b 35 68 70 40 00      mov  0x407068,%esi
403417: 8d 65 f4                lea  -0xc(%ebp),%esp
40341a: 5b                      pop  %ebx
40341b: 89 f0                    mov  %esi,%eax
40341d: 5e                      pop  %esi
40341e: 5f                      pop  %edi
40341f: 5d                      pop  %ebp
403420: c3                      ret
403421: 89 65 dc                mov  %esp,-0x24(%ebp)
403424: c7 44 24 08 00 00 00    movl $0x0,0x8(%esp)
40342b: 00

```



```

40342c: 8b 45 08      mov  0x8(%ebp),%eax
40342f: c7 04 24 00 00 00      movl $0x0,(%esp)
403436: 89 44 24 04      mov  %eax,0x4(%esp)
40343a: e8 89 08 00 00      call 0x403cc8
40343f: 89 c2          mov  %eax,%edx
403441: 8d 44 00 12      lea  0x12(%eax,%eax,1),%eax
403445: c1 e8 04        shr  $0x4,%eax
403448: c1 e0 04        shl  $0x4,%eax
40344b: e8 f0 ed ff ff      call 0x402240
403450: 29 c4          sub  %eax,%esp
403452: 89 54 24 08      mov  %edx,0x8(%esp)
403456: 8b 45 08      mov  0x8(%ebp),%eax
403459: 8d 7c 24 0c      lea  0xc(%esp),%edi
40345d: 89 3c 24        mov  %edi,(%esp)
403460: 89 44 24 04      mov  %eax,0x4(%esp)
403464: e8 5f 08 00 00      call 0x403cc8
403469: 31 c9          xor  %ecx,%ecx
40346b: 89 45 d8      mov  %eax,-0x28(%ebp)
40346e: 83 f8 01      cmp  $0x1,%eax
403471: 66 89 0c 47      mov  %cx,(%edi,%eax,2)
403475: 0f b7 07      movzwl (%edi),%eax
403478: 89 7d e4      mov  %edi,-0x1c(%ebp)
40347b: 66 89 45 e2      mov  %ax,-0x1e(%ebp)
40347f: 76 1f          jbe  0x4034a0
403481: 66 83 f8 2f      cmp  $0x2f,%ax
403485: 0f 84 1c 02 00 00      je   0x4036a7
40348b: 66 83 f8 5c      cmp  $0x5c,%ax
40348f: 0f 84 12 02 00 00      je   0x4036a7
403495: 66 83 7f 02 3a      cmpw $0x3a,0x2(%edi)
40349a: 0f 84 4f 02 00 00      je   0x4036ef
4034a0: 0f b7 45 e2      movzwl -0x1e(%ebp),%eax
4034a4: 66 85 c0      test %ax,%ax
4034a7: 0f 84 e1 00 00 00      je   0x40358e
4034ad: 8b 4d e4      mov  -0x1c(%ebp),%ecx
4034b0: 89 c2          mov  %eax,%edx
4034b2: 89 ce          mov  %ecx,%esi
4034b4: eb 1e          jmp  0x4034d4
4034b6: 8d 76 00      lea  0x0(%esi),%esi
4034b9: 8d bc 27 00 00 00 00      lea  0x0(%edi,%eiz,1),%edi
4034c0: 66 83 fa 5c      cmp  $0x5c,%dx
4034c4: 89 c8          mov  %ecx,%eax
4034c6: 74 12          je   0x4034da
4034c8: 0f b7 50 02      movzwl 0x2(%eax),%edx
4034cc: 8d 48 02      lea  0x2(%eax),%ecx
4034cf: 66 85 d2      test %dx,%dx
4034d2: 74 36          je   0x40350a
4034d4: 66 83 fa 2f      cmp  $0x2f,%dx
4034d8: 75 e6          jne  0x4034c0
4034da: 0f b7 11      movzwl (%ecx),%edx
4034dd: 89 c8          mov  %ecx,%eax
4034df: 66 83 fa 2f      cmp  $0x2f,%dx
4034e3: 75 0c          jne  0x4034f1
4034e5: 83 c0 02      add  $0x2,%eax

```

```

4034e8:    0f b7 10      movzwl (%eax),%edx
4034eb:    66 83 fa 2f   cmp $0x2f,%dx
4034ef:    74 f4         je 0x4034e5
4034f1:    66 83 fa 5c   cmp $0x5c,%dx
4034f5:    74 ee         je 0x4034e5
4034f7:    66 85 d2      test %dx,%dx
4034fa: 74 0e         je 0x40350a
4034fc: 0f b7 50 02   movzwl 0x2(%eax),%edx
403500:    89 c6         mov %eax,%esi
403502:    8d 48 02      lea 0x2(%eax),%ecx
403505:    66 85 d2      test %dx,%dx
403508:    75 ca         jne 0x4034d4
40350a:    39 75 e4      cmp %esi,-0x1c(%ebp)
40350d:    0f 82 8d 00 00 00  jb 0x4035a0
403513:    0f b7 45 e2   movzwl -0x1e(%ebp),%eax
403517:    66 83 f8 2f   cmp $0x2f,%ax
40351b:    0f 84 e1 01 00 00  je 0x403702
403521:    66 83 f8 5c   cmp $0x5c,%ax
403525:    0f 84 d7 01 00 00  je 0x403702
40352b:    8b 75 e4      mov -0x1c(%ebp),%esi
40352e:    b9 2e 00 00 00   mov $0x2e,%ecx
403533:    89 f0         mov %esi,%eax
403535:    66 89 0e      mov %cx,(%esi)
403538:    83 c0 02      add $0x2,%eax
40353b:    31 d2         xor %edx,%edx
40353d:    66 89 10      mov %dx,(%eax)
403540:    c7 44 24 08 00 00 00  movl $0x0,0x8(%esp)
403547:    00
403548:    89 7c 24 04   mov %edi,0x4(%esp)
40354c:    c7 04 24 00 00 00 00  movl $0x0,(%esp)
403553:    e8 f8 06 00 00   call 0x403c50
403558:    8d 50 01      lea 0x1(%eax),%edx
40355b:    89 54 24 04   mov %edx,0x4(%esp)
40355f:    a1 68 70 40 00   mov 0x407068,%eax
403564:    89 55 e4      mov %edx,-0x1c(%ebp)
403567:    89 04 24      mov %eax,(%esp)
40356a:    e8 31 07 00 00   call 0x403ca0
40356f:    8b 55 e4      mov -0x1c(%ebp),%edx
403572:    a3 68 70 40 00   mov %eax,0x407068
403577:    89 c6         mov %eax,%esi
403579:    89 7c 24 04   mov %edi,0x4(%esp)
40357d:    89 04 24      mov %eax,(%esp)
403580:    89 54 24 08   mov %edx,0x8(%esp)
403584:    e8 c7 06 00 00   call 0x403c50
403589:    e9 c2 00 00 00   jmp 0x403650
40358e:    8b 65 dc      mov -0x24(%ebp),%esp
403591:    e9 1a fe ff ff  jmp 0x4033b0
403596:    8d 76 00      lea 0x0(%esi),%esi
403599:    8d bc 27 00 00 00 00  lea 0x0(%edi,%eiz,1),%edi
4035a0:    8d 46 fe      lea -0x2(%esi),%eax
4035a3:    39 45 e4      cmp %eax,-0x1c(%ebp)
4035a6:    0f 83 61 01 00 00  jae 0x40370d
4035ac:    0f b7 56 fe   movzwl -0x2(%esi),%edx

```

```

4035b0:      89 c6      mov  %eax,%esi
4035b2:      66 83 fa 2f    cmp  $0x2f,%dx
4035b6:      74 e8      je   0x4035a0
4035b8:      66 83 fa 5c    cmp  $0x5c,%dx
4035bc:      74 e2      je   0x4035a0
4035be:      31 d2      xor  %edx,%edx
4035c0:      89 f9      mov  %edi,%ecx
4035c2:      66 89 50 02    mov  %dx,0x2(%eax)
4035c6:      0f b7 17      movzwl (%edi),%edx
4035c9:      66 83 fa 2f    cmp  $0x2f,%dx
4035cd:      74 11      je   0x4035e0
4035cf: 66 83 fa 5c    cmp  $0x5c,%dx
4035d3:      0f 85 04 01 00 00    jne  0x4036dd
4035d9:      8d b4 26 00 00 00 00    lea  0x0(%esi,%eiz,1),%esi
4035e0:      83 c1 02      add  $0x2,%ecx
4035e3:      0f b7 01      movzwl (%ecx),%eax
4035e6:      66 83 f8 2f    cmp  $0x2f,%ax
4035ea:      74 f4      je   0x4035e0
4035ec:      66 83 f8 5c    cmp  $0x5c,%ax
4035f0:      74 ee      je   0x4035e0
4035f2:      89 c8      mov  %ecx,%eax
4035f4:      29 f8      sub  %edi,%eax
4035f6:      83 f8 05      cmp  $0x5,%eax
4035f9:      0f 8e de 00 00 00    jle  0x4036dd
4035ff: 89 f9      mov  %edi,%ecx
403601:      89 c8      mov  %ecx,%eax
403603:      66 85 d2      test %dx,%dx
403606:      74 21      je   0x403629
403608:      83 c1 02      add  $0x2,%ecx
40360b:      66 83 fa 2f    cmp  $0x2f,%dx
40360f:      66 89 51 fe    mov  %dx,-0x2(%ecx)
403613:      74 62      je   0x403677
403615:      66 83 38 5c    cmpw $0x5c,(%eax)
403619:      8d 70 02      lea  0x2(%eax),%esi
40361c:      74 57      je   0x403675
40361e:      0f b7 50 02    movzwl 0x2(%eax),%edx
403622:      89 f0      mov  %esi,%eax
403624:      66 85 d2      test %dx,%dx
403627:      75 df      jne  0x403608
403629:      8b 45 d8      mov  -0x28(%ebp),%eax
40362c:      31 f6      xor  %esi,%esi
40362e:      66 89 31      mov  %si,(%ecx)
403631:      89 7c 24 04    mov  %edi,0x4(%esp)
403635:      89 44 24 08    mov  %eax,0x8(%esp)
403639:      8b 45 08      mov  0x8(%ebp),%eax
40363c:      89 04 24      mov  %eax,(%esp)
40363f:      e8 0c 06 00 00    call 0x403c50
403644:      83 f8 ff      cmp  $0xffffffff,%eax
403647:      8b 75 08      mov  0x8(%ebp),%esi
40364a:      74 04      je   0x403650
40364c:      c6 04 06 00    movb $0x0,(%esi,%eax,1)
403650:      89 5c 24 04    mov  %ebx,0x4(%esp)
403654:      c7 04 24 02 00 00 00    movl $0x2,(%esp)

```

```

40365b: e8 30 06 00 00      call 0x403c90
403660: 89 1c 24            mov  %ebx,(%esp)
403663: e8 78 06 00 00      call 0x403ce0
403668: 8b 65 dc            mov  -0x24(%ebp),%esp
40366b: 8d 65 f4            lea  -0xc(%ebp),%esp
40366e: 89 f0              mov  %esi,%eax
403670: 5b                 pop  %ebx
403671: 5e                 pop  %esi
403672: 5f                 pop  %edi
403673: 5d                 pop  %ebp
403674: c3                 ret
403675: 89 f0              mov  %esi,%eax
403677: 0f b7 10            movzwl (%eax),%edx
40367a: 66 83 fa 5c         cmp  $0x5c,%dx
40367e: 74 10              je   0x403690
403680: 66 83 fa 2f         cmp  $0x2f,%dx
403684: 0f 85 79 ff ff ff   jne  0x403603
40368a: 8d b6 00 00 00 00   lea  0x0(%esi),%esi
403690: 83 c0 02            add  $0x2,%eax
403693: 0f b7 10            movzwl (%eax),%edx
403696: 66 83 fa 2f         cmp  $0x2f,%dx
40369a: 74 f4              je   0x403690
40369c: 66 83 fa 5c         cmp  $0x5c,%dx
4036a0: 74 ee              je   0x403690
4036a2: e9 5c ff ff ff     jmp  0x403603
4036a7: 0f b7 45 e2         movzwl -0x1e(%ebp),%eax
4036ab: 66 3b 47 02         cmp  0x2(%edi),%ax
4036af: 0f 85 eb fd ff ff   jne  0x4034a0
4036b5: 66 83 7f 04 00      cmpw $0x0,0x4(%edi)
4036ba: 0f 85 e0 fd ff ff   jne  0x4034a0
4036c0: 89 5c 24 04         mov  %ebx,0x4(%esp)
4036c4: c7 04 24 02 00 00 00 movl $0x2,(%esp)
4036cb: e8 c0 05 00 00      call 0x403c90
4036d0: 89 1c 24            mov  %ebx,(%esp)
4036d3: e8 08 06 00 00      call 0x403ce0
4036d8: 8b 75 08            mov  0x8(%ebp),%esi
4036db: eb 8b              jmp  0x403668
4036dd: 66 39 57 02         cmp  %dx,0x2(%edi)
4036e1: 0f 85 18 ff ff ff   jne  0x4035ff
4036e7: 0f b7 11            movzwl (%ecx),%edx
4036ea: e9 12 ff ff ff     jmp  0x403601
4036ef: 8d 47 04            lea  0x4(%edi),%eax
4036f2: 89 45 e4            mov  %eax,-0x1c(%ebp)
4036f5: 0f b7 47 04         movzwl 0x4(%edi),%eax
4036f9: 66 89 45 e2         mov  %ax,-0x1e(%ebp)
4036fd: e9 9e fd ff ff     jmp  0x4034a0
403702: 8b 45 e4            mov  -0x1c(%ebp),%eax
403705: 83 c0 02            add  $0x2,%eax
403708: e9 2e fe ff ff     jmp  0x40353b
40370d: 0f 85 ab fe ff ff   jne  0x4035be
403713: 0f b7 4d e2         movzwl -0x1e(%ebp),%ecx
403717: 66 83 f9 2f         cmp  $0x2f,%cx
40371b: 74 0a              je   0x403727

```

40371d:	66 83 f9 5c	cmp \$0x5c,%cx
403721:	0f 85 97 fe ff ff	jne 0x4035be
403727:	0f b7 4d e2	movzwl -0x1e(%ebp),%ecx
40372b:	66 39 48 02	cmp %cx,0x2(%eax)
40372f:	0f 85 89 fe ff ff	jne 0x4035be
403735:	0f b7 50 04	movzwl 0x4(%eax),%edx
403739:	66 83 fa 2f	cmp \$0x2f,%dx
40373d:	0f 84 7b fe ff ff	je 0x4035be
403743:	66 83 fa 5c	cmp \$0x5c,%dx
403747:	0f 84 71 fe ff ff	je 0x4035be
40374d:	89 f0	mov %esi,%eax
40374f:	e9 6a fe ff ff	jmp 0x4035be
403754:	90	nop
403755:	90	nop
403756:	90	nop
403757:	90	nop
403758:	90	nop
403759:	90	nop
40375a:	90	nop
40375b:	90	nop
40375c:	90	nop
40375d:	90	nop
40375e:	90	nop
40375f:	90	nop
403760:	56	push %esi
403761:	53	push %ebx
403762:	89 d3	mov %edx,%ebx
403764:	81 ec 54 01 00 00	sub \$0x154,%esp
40376a:	8d 54 24 10	lea 0x10(%esp),%edx
40376e:	89 04 24	mov %eax,(%esp)
403771:	89 54 24 04	mov %edx,0x4(%esp)
403775:	e8 26 06 00 00	call 0x403da0
40377a:	83 ec 08	sub \$0x8,%esp
40377d:	83 f8 ff	cmp \$0xffffffff,%eax
403780:	89 c6	mov %eax,%esi
403782:	74 5a	je 0x4037de
403784:	31 c0	xor %eax,%eax
403786:	8d 4b 0c	lea 0xc(%ebx),%ecx
403789:	66 89 43 06	mov %ax,0x6(%ebx)
40378d:	31 c0	xor %eax,%eax
40378f:	eb 12	jmp 0x4037a3
403791:	0f b7 43 06	movzwl 0x6(%ebx),%eax
403795:	83 c0 01	add \$0x1,%eax
403798:	66 3d 04 01	cmp \$0x104,%ax
40379c:	66 89 43 06	mov %ax,0x6(%ebx)
4037a0:	83 d1 00	adc \$0x0,%ecx
4037a3:	0f b7 c0	movzwl %ax,%eax
4037a6:	0f b6 44 04 3c	movzbl 0x3c(%esp,%eax,1),%eax
4037ab:	84 c0	test %al,%al
4037ad:	88 01	mov %al,(%ecx)
4037af:75 e0	jne 0x403791	
4037b1:	8b 44 24 10	mov 0x10(%esp),%eax
4037b5:	24 58	and \$0x58,%al

```

4037b7: 83 f8 10      cmp  $0x10,%eax
4037ba: 76 14         jbe  0x4037d0
4037bc: c7 43 08 18 00 00 00      movl $0x18,0x8(%ebx)
4037c3: 81 c4 54 01 00 00      add  $0x154,%esp
4037c9: 89 f0         mov  %esi,%eax
4037cb: 5b           pop  %ebx
4037cc: 5e           pop  %esi
4037cd: c3           ret
4037ce: 66 90         xchg %ax,%ax
4037d0: 89 43 08      mov  %eax,0x8(%ebx)
4037d3: 81 c4 54 01 00 00      add  $0x154,%esp
4037d9: 89 f0         mov  %esi,%eax
4037db: 5b           pop  %ebx
4037dc: 5e           pop  %esi
4037dd: c3           ret
4037de: e8 2d 05 00 00      call 0x403d10
4037e3: 89 c3         mov  %eax,%ebx
4037e5: e8 96 05 00 00      call 0x403d80
4037ea: 83 f8 03      cmp  $0x3,%eax
4037ed: 89 03         mov  %eax,(%ebx)
4037ef: 74 31         je   0x403822
4037f1: e8 1a 05 00 00      call 0x403d10
4037f6: 81 38 0b 01 00 00      cmpl $0x10b,(%eax)
4037fc: 74 17         je   0x403815
4037fe: e8 0d 05 00 00      call 0x403d10
403803: 83 38 02      cmpl $0x2,(%eax)
403806: 74 bb         je   0x4037c3
403808: e8 03 05 00 00      call 0x403d10
40380d: c7 00 16 00 00 00      movl $0x16,(%eax)
403813: eb ae         jmp  0x4037c3
403815: e8 f6 04 00 00      call 0x403d10
40381a: c7 00 14 00 00 00      movl $0x14,(%eax)
403820: eb a1         jmp  0x4037c3
403822: e8 e9 04 00 00      call 0x403d10
403827: c7 00 02 00 00 00      movl $0x2,(%eax)
40382d: eb 94         jmp  0x4037c3
40382f: 90           nop
403830: 56           push %esi
403831: 53           push %ebx
403832: 89 d3         mov  %edx,%ebx
403834: 81 ec 54 01 00 00      sub  $0x154,%esp
40383a: 8d 54 24 10      lea  0x10(%esp),%edx
40383e: 89 04 24      mov  %eax,(%esp)
403841: 89 54 24 04      mov  %edx,0x4(%esp)
403845: e8 4e 05 00 00      call 0x403d98
40384a: 83 ec 08      sub  $0x8,%esp
40384d: 85 c0         test %eax,%eax
40384f: 89 c6         mov  %eax,%esi
403851: 74 5f         je   0x4038b2
403853: 31 c0         xor  %eax,%eax
403855: 8d 4b 0c      lea  0xc(%ebx),%ecx
403858: 66 89 43 06      mov  %ax,0x6(%ebx)
40385c: 31 c0         xor  %eax,%eax

```

```

40385e:    eb 12          jmp  0x403872
403860:    0f b7 43 06    movzwl 0x6(%ebx),%eax
403864:    83 c0 01        add  $0x1,%eax
403867:    66 3d 04 01     cmp  $0x104,%ax
40386b:    66 89 43 06     mov  %ax,0x6(%ebx)
40386f:    83 d1 00        adc  $0x0,%ecx
403872:    0f b7 c0        movzwl %ax,%eax
403875:    0f b6 44 04 3c  movzbl 0x3c(%esp,%eax,1),%eax
40387a:    84 c0          test %al,%al
40387c:    88 01          mov  %al,(%ecx)
40387e:    75 e0          jne  0x403860
403880:    8b 44 24 10     mov  0x10(%esp),%eax
403884:    24 58          and  $0x58,%al
403886:    83 f8 10        cmp  $0x10,%eax
403889:    77 15          ja   0x4038a0
40388b:    89 43 08        mov  %eax,0x8(%ebx)
40388e:    81 c4 54 01 00 00 add  $0x154,%esp
403894:    89 f0          mov  %esi,%eax
403896:    5b            pop  %ebx
403897:    5e            pop  %esi
403898:    c3            ret
403899:    8d b4 26 00 00 00 00 lea  0x0(%esi,%eiz,1),%esi
4038a0:    c7 43 08 18 00 00 00 movl  $0x18,0x8(%ebx)
4038a7:    81 c4 54 01 00 00 00 add  $0x154,%esp
4038ad:    89 f0          mov  %esi,%eax
4038af:5b          pop  %ebx
4038b0:    5e            pop  %esi
4038b1:    c3            ret
4038b2:    e8 c9 04 00 00    call 0x403d80
4038b7:    83 f8 12        cmp  $0x12,%eax
4038ba:    74 d2          je   0x40388e
4038bc:    e8 4f 04 00 00    call 0x403d10
4038c1:    c7 00 02 00 00 00 00 movl  $0x2,(%eax)
4038c7:    81 c4 54 01 00 00 00 add  $0x154,%esp
4038cd:    89 f0          mov  %esi,%eax
4038cf:5b          pop  %ebx
4038d0:    5e            pop  %esi
4038d1:    c3            ret
4038d2:    8d b4 26 00 00 00 00 lea  0x0(%esi,%eiz,1),%esi
4038d9:    8d bc 27 00 00 00 00 lea  0x0(%edi,%eiz,1),%edi
4038e0:    55            push %ebp
4038e1:    57            push %edi
4038e2:    56            push %esi
4038e3:    53            push %ebx
4038e4:    81 ec 2c 01 00 00    sub  $0x12c,%esp
4038ea:    8b 84 24 40 01 00 00 mov  0x140(%esp),%eax
4038f1:    85 c0          test %eax,%eax
4038f3:    0f 84 83 01 00 00    je   0x403a7c
4038f9:    80 38 00        cmpb $0x0,(%eax)
4038fc:0f 84 5e 01 00 00    je   0x403a60
403902:    8d 7c 24 1c     lea  0x1c(%esp),%edi
403906:    c7 44 24 08 04 01 00 movl  $0x104,0x8(%esp)
40390d:    00

```

```

40390e: 89 44 24 04    mov  %eax,0x4(%esp)
403912: 89 3c 24       mov  %edi,(%esp)
403915: e8 ee 03 00 00    call 0x403d08
40391a: 80 7c 24 1c 00    cmpb $0x0,0x1c(%esp)
40391f: 89 f8         mov  %edi,%eax
403921: 74 4d         je   0x403970
403923: 8b 08         mov  (%eax),%ecx
403925: 83 c0 04      add  $0x4,%eax
403928: 8d 91 ff fe fe    lea  -0x1010101(%ecx),%edx
40392e: f7 d1        not  %ecx
403930: 21 ca        and  %ecx,%edx
403932: 81 e2 80 80 80 80    and  $0x80808080,%edx
403938: 74 e9         je   0x403923
40393a: f7 c2 80 80 00 00    test $0x8080,%edx
403940: 0f 84 0a 01 00 00    je   0x403a50
403946: 89 d1        mov  %edx,%ecx
403948: 00 d1        add  %dl,%cl
40394a: 83 d8 03      sbb  $0x3,%eax
40394d: 29 f8        sub  %edi,%eax
40394f: 0f b6 54 04 1b    movzbl 0x1b(%esp,%eax,1),%edx
403954: 80 fa 2f      cmp  $0x2f,%dl
403957: 74 43         je   0x40399c
403959: 80 fa 5c      cmp  $0x5c,%dl
40395c: 74 3e         je   0x40399c
40395e: b9 5c 00 00 00    mov  $0x5c,%ecx
403963: 66 89 0c 07    mov  %cx,(%edi,%eax,1)
403967: 83 c0 01      add  $0x1,%eax
40396a: eb 30        jmp  0x40399c
40396c: 8d 74 26 00    lea  0x0(%esi,%eiz,1),%esi
403970: 8b 08        mov  (%eax),%ecx
403972: 83 c0 04      add  $0x4,%eax
403975: 8d 91 ff fe fe    lea  -0x1010101(%ecx),%edx
40397b: f7 d1        not  %ecx
40397d: 21 ca        and  %ecx,%edx
40397f: 81 e2 80 80 80 80    and  $0x80808080,%edx
403985: 74 e9         je   0x403970
403987: f7 c2 80 80 00 00    test $0x8080,%edx
40398d: 0f 84 ad 00 00 00    je   0x403a40
403993: 89 d1        mov  %edx,%ecx
403995: 00 d1        add  %dl,%cl
403997: 83 d8 03      sbb  $0x3,%eax
40399a: 29 f8        sub  %edi,%eax
40399c: ba 2a 00 00 00    mov  $0x2a,%edx
4039a1: 89 fb        mov  %edi,%ebx
4039a3: 66 89 14 07    mov  %dx,(%edi,%eax,1)
4039a7: 8b 13        mov  (%ebx),%edx
4039a9: 83 c3 04      add  $0x4,%ebx
4039ac: 8d 82 ff fe fe    lea  -0x1010101(%edx),%eax
4039b2: f7 d2        not  %edx
4039b4: 21 d0        and  %edx,%eax
4039b6: 25 80 80 80 80    and  $0x80808080,%eax
4039bb: 74 ea         je   0x4039a7
4039bd: a9 80 80 00 00    test $0x8080,%eax

```



```

4039c2: 75 06      jne 0x4039ca
4039c4: c1 e8 10   shr $0x10,%eax
4039c7: 83 c3 02   add $0x2,%ebx
4039ca: 89 c1      mov %eax,%ecx
4039cc: 00 c1      add %al,%cl
4039ce: 83 db 03   sbb $0x3,%ebx
4039d1: 29 fb      sub %edi,%ebx
4039d3: 8d 83 1c 01 00 00   lea 0x11c(%ebx),%eax
4039d9: 89 04 24   mov %eax,(%esp)
4039dc: e8 ef 02 00 00   call 0x403cd0
4039e1: 85 c0      test %eax,%eax
4039e3: 89 c6      mov %eax,%esi
4039e5: 0f 84 84 00 00 00   je 0x403a6f
4039eb: 8d a8 18 01 00 00   lea 0x118(%eax),%ebp
4039f1: 83 c3 01   add $0x1,%ebx
4039f4: 89 7c 24 04   mov %edi,0x4(%esp)
4039f8: 89 5c 24 08   mov %ebx,0x8(%esp)
4039fc: 89 2c 24   mov %ebp,(%esp)
4039ff: e8 bc 02 00 00   call 0x403cc0
403a04: 89 f2      mov %esi,%edx
403a06: 89 e8      mov %ebp,%eax
403a08: e8 53 fd ff ff   call 0x403760
403a0d: 83 f8 ff   cmp $0xffffffff,%eax
403a10: 89 86 10 01 00 00   mov %eax,0x110(%esi)
403a16: 74 73      je 0x403a8b
403a18: b8 10 01 00 00   mov $0x110,%eax
403a1d: c7 86 14 01 00 00 00   movl $0x0,0x114(%esi)
403a24: 00 00 00
403a27: c7 06 00 00 00 00   movl $0x0,(%esi)
403a2d: 66 89 46 04   mov %ax,0x4(%esi)
403a31: 81 c4 2c 01 00 00   add $0x12c,%esp
403a37: 89 f0      mov %esi,%eax
403a39: 5b        pop %ebx
403a3a: 5e        pop %esi
403a3b: 5f        pop %edi
403a3c: 5d        pop %ebp
403a3d: c3        ret
403a3e: 66 90      xchg %ax,%ax
403a40: c1 ea 10   shr $0x10,%edx
403a43: 83 c0 02   add $0x2,%eax
403a46: e9 48 ff ff   jmp 0x403993
403a4b: 90        nop
403a4c: 8d 74 26 00   lea 0x0(%esi,%eiz,1),%esi
403a50: c1 ea 10   shr $0x10,%edx
403a53: 83 c0 02   add $0x2,%eax
403a56: e9 eb fe ff   jmp 0x403946
403a5b: 90        nop
403a5c: 8d 74 26 00   lea 0x0(%esi,%eiz,1),%esi
403a60: e8 ab 02 00 00   call 0x403d10
403a65: 31 f6      xor %esi,%esi
403a67: c7 00 02 00 00 00   movl $0x2,(%eax)
403a6d: eb c2      jmp 0x403a31
403a6f: e8 9c 02 00 00   call 0x403d10

```

```

403a74: c7 00 0c 00 00 00      movl $0xc,(%eax)
403a7a: eb b5                  jmp 0x403a31
403a7c: e8 8f 02 00 00        call 0x403d10
403a81: 31 f6                  xor %esi,%esi
403a83: c7 00 16 00 00 00      movl $0x16,(%eax)
403a89: eb a6                  jmp 0x403a31
403a8b: 89 34 24              mov %esi,(%esp)
403a8e: 31 f6                  xor %esi,%esi
403a90: e8 4b 02 00 00        call 0x403ce0
403a95: eb 9a                  jmp 0x403a31
403a97: 89 f6                  mov %esi,%esi
403a99: 8d bc 27 00 00 00 00    lea 0x0(%edi,%eiz,1),%edi
403aa0: 53                     push %ebx
403aa1: 83 ec 08              sub $0x8,%esp
403aa4: 8b 5c 24 10          mov 0x10(%esp),%ebx
403aa8: 85 db                  test %ebx,%ebx
403aaa: 74 2b                  je 0x403ad7
403aac: 8b 83 14 01 00 00      mov 0x114(%ebx),%eax
403ab2: 8d 50 01              lea 0x1(%eax),%edx
403ab5: 85 c0                  test %eax,%eax
403ab7: 89 93 14 01 00 00      mov %edx,0x114(%ebx)
403abd: 7e 11                  jle 0x403ad0
403abf: 8b 83 10 01 00 00      mov 0x110(%ebx),%eax
403ac5: 89 da                  mov %ebx,%edx
403ac7: e8 64 fd ff ff        call 0x403830
403acc: 85 c0                  test %eax,%eax
403ace: 74 02                  je 0x403ad2
403ad0: 89 d8                  mov %ebx,%eax
403ad2: 83 c4 08              add $0x8,%esp
403ad5: 5b                     pop %ebx
403ad6: c3                     ret
403ad7: e8 34 02 00 00        call 0x403d10
403adc: c7 00 09 00 00 00      movl $0x9,(%eax)
403ae2: 31 c0                  xor %eax,%eax
403ae4: eb ec                  jmp 0x403ad2
403ae6: 8d 76 00              lea 0x0(%esi),%esi
403ae9: 8d bc 27 00 00 00 00    lea 0x0(%edi,%eiz,1),%edi
403af0:53                     push %ebx
403af1:83 ec 18              sub $0x18,%esp
403af4:8b 5c 24 20          mov 0x20(%esp),%ebx
403af8:85 db                  test %ebx,%ebx
403afa:74 24                  je 0x403b20
403afc:8b 83 10 01 00 00      mov 0x110(%ebx),%eax
403b02: 89 04 24              mov %eax,(%esp)
403b05: e8 9e 02 00 00        call 0x403da8
403b0a: 83 ec 04              sub $0x4,%esp
403b0d: 85 c0                  test %eax,%eax
403b0f: 74 0f                  je 0x403b20
403b11: 89 1c 24              mov %ebx,(%esp)
403b14: e8 c7 01 00 00        call 0x403ce0
403b19: 31 c0                  xor %eax,%eax
403b1b: 83 c4 18              add $0x18,%esp
403b1e: 5b                     pop %ebx

```

```

403b1f: c3          ret
403b20: e8 eb 01 00 00      call 0x403d10
403b25: c7 00 09 00 00 00   movl $0x9,(%eax)
403b2b: b8 ff ff ff ff      mov  $0xffffffff,%eax
403b30: eb e9             jmp 0x403b1b
403b32: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi
403b39: 8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
403b40: 53              push %ebx
403b41: 83 ec 18         sub $0x18,%esp
403b44: 8b 5c 24 20      mov 0x20(%esp),%ebx
403b48: 85 db          test %ebx,%ebx
403b4a: 74 15          je 0x403b61
403b4c: 8b 83 10 01 00 00   mov 0x110(%ebx),%eax
403b52: 89 04 24        mov %eax,(%esp)
403b55: e8 4e 02 00 00      call 0x403da8
403b5a: 83 ec 04         sub $0x4,%esp
403b5d: 85 c0          test %eax,%eax
403b5f: 75 10          jne 0x403b71
403b61: e8 aa 01 00 00      call 0x403d10
403b66: c7 00 09 00 00 00   movl $0x9,(%eax)
403b6c: 83 c4 18         add $0x18,%esp
403b6f: 5b             pop %ebx
403b70: c3          ret
403b71: 8d 83 18 01 00 00   lea 0x118(%ebx),%eax
403b77: 89 da          mov %ebx,%edx
403b79: e8 e2 fb ff ff      call 0x403760
403b7e: 83 f8 ff        cmp $0xffffffff,%eax
403b81: 89 83 10 01 00 00   mov %eax,0x110(%ebx)
403b87: 74 e3          je 0x403b6c
403b89: c7 83 14 01 00 00 00 movl $0x0,0x114(%ebx)
403b90: 00 00 00
403b93: 83 c4 18         add $0x18,%esp
403b96: 5b             pop %ebx
403b97: c3          ret
403b98: 90             nop
403b99: 8d b4 26 00 00 00 00 lea 0x0(%esi,%eiz,1),%esi
403ba0: 83 ec 0c         sub $0xc,%esp
403ba3: 8b 44 24 10      mov 0x10(%esp),%eax
403ba7: 85 c0          test %eax,%eax
403ba9: 74 0a          je 0x403bb5
403bab: 8b 80 14 01 00 00   mov 0x114(%eax),%eax
403bb1: 83 c4 0c         add $0xc,%esp
403bb4: c3          ret
403bb5: e8 56 01 00 00      call 0x403d10
403bba: c7 00 09 00 00 00   movl $0x9,(%eax)
403bc0: b8 ff ff ff ff      mov  $0xffffffff,%eax
403bc5: eb ea          jmp 0x403bb1
403bc7: 89 f6          mov %esi,%esi
403bc9: 8d bc 27 00 00 00 00 lea 0x0(%edi,%eiz,1),%edi
403bd0: 56             push %esi
403bd1: 53             push %ebx
403bd2: 83 ec 14         sub $0x14,%esp
403bd5: 8b 74 24 24      mov 0x24(%esp),%esi

```

403bd9:	8b 5c 24 20	mov	0x20(%esp),%ebx
403bdd:	85 f6	test	%esi,%esi
403bdf:	78 4f	js	0x403c30
403be1:	89 1c 24	mov	%ebx,(%esp)
403be4:	e8 57 ff ff ff	call	0x403b40
403be9:	85 f6	test	%esi,%esi
403beb:	74 37	je	0x403c24
403bed:	83 bb 10 01 00 00 ff	cmpl	\$0xffffffff,0x110(%ebx)
403bf4:	75 1b	jne	0x403c11
403bf6:	eb 2c	jmp	0x403c24
403bf8:	90	nop	
403bf9:	8d b4 26 00 00 00 00	lea	0x0(%esi,%eiz,1),%esi
403c00:	8b 83 10 01 00 00	mov	0x110(%ebx),%eax
403c06:	89 da	mov	%ebx,%edx
403c08:	e8 23 fc ff ff	call	0x403830
403c0d:	85 c0	test	%eax,%eax
403c0f: 74 13	je	0x403c24	
403c11:	8b 83 14 01 00 00	mov	0x114(%ebx),%eax
403c17:	83 c0 01	add	\$0x1,%eax
403c1a:	39 c6	cmp	%eax,%esi
403c1c:	89 83 14 01 00 00	mov	%eax,0x114(%ebx)
403c22:	7f dc	jg	0x403c00
403c24:	83 c4 14	add	\$0x14,%esp
403c27:	5b	pop	%ebx
403c28:	5e	pop	%esi
403c29:	c3	ret	
403c2a:	8d b6 00 00 00 00	lea	0x0(%esi),%esi
403c30:	e8 db 00 00 00	call	0x403d10
403c35:	c7 00 16 00 00 00	movl	\$0x16,(%eax)
403c3b:	83 c4 14	add	\$0x14,%esp
403c3e:	5b	pop	%ebx
403c3f: 5e	pop	%esi	
403c40:	c3	ret	
403c41:	90	nop	
403c42:	90	nop	
403c43:	90	nop	
403c44:	90	nop	
403c45:	90	nop	
403c46:	90	nop	
403c47:	90	nop	
403c48:	90	nop	
403c49:	90	nop	
403c4a:	90	nop	
403c4b:	90	nop	
403c4c:	90	nop	
403c4d:	90	nop	
403c4e:	90	nop	
403c4f: 90	nop		
403c50:	ff 25 20 82 40 00	jmp	*0x408220
403c56:	90	nop	
403c57:	90	nop	
403c58:	ff 25 1c 82 40 00	jmp	*0x40821c
403c5e:	90	nop	

403c5f:90	nop	
403c60:	ff 25 18 82 40 00	jmp *0x408218
403c66:	90	nop
403c67:	90	nop
403c68:	ff 25 14 82 40 00	jmp *0x408214
403c6e:	90	nop
403c6f:90	nop	
403c70:	ff 25 10 82 40 00	jmp *0x408210
403c76:	90	nop
403c77:	90	nop
403c78:	ff 25 0c 82 40 00	jmp *0x40820c
403c7e:	90	nop
403c7f:90	nop	
403c80:	ff 25 08 82 40 00	jmp *0x408208
403c86:	90	nop
403c87:	90	nop
403c88:	ff 25 04 82 40 00	jmp *0x408204
403c8e:	90	nop
403c8f:90	nop	
403c90:	ff 25 00 82 40 00	jmp *0x408200
403c96:	90	nop
403c97:	90	nop
403c98:	ff 25 fc 81 40 00	jmp *0x4081fc
403c9e:	90	nop
403c9f:90	nop	
403ca0:	ff 25 f8 81 40 00	jmp *0x4081f8
403ca6:	90	nop
403ca7:	90	nop
403ca8:	ff 25 f4 81 40 00	jmp *0x4081f4
403cae:	90	nop
403caf:90	nop	
403cb0:	ff 25 f0 81 40 00	jmp *0x4081f0
403cb6:	90	nop
403cb7:	90	nop
403cb8:	ff 25 ec 81 40 00	jmp *0x4081ec
403cbe:	90	nop
403cbf:90	nop	
403cc0:	ff 25 e8 81 40 00	jmp *0x4081e8
403cc6:	90	nop
403cc7:	90	nop
403cc8:	ff 25 e4 81 40 00	jmp *0x4081e4
403cce:	90	nop
403ccf:90	nop	
403cd0:	ff 25 e0 81 40 00	jmp *0x4081e0
403cd6:	90	nop
403cd7:	90	nop
403cd8:	ff 25 dc 81 40 00	jmp *0x4081dc
403cde:	90	nop
403cdf:90	nop	
403ce0:	ff 25 d8 81 40 00	jmp *0x4081d8
403ce6:	90	nop
403ce7:	90	nop
403ce8:	ff 25 d4 81 40 00	jmp *0x4081d4

403cee:	90	nop
403cef:90		nop
403cf0:ff 25 cc 81 40 00		jmp *0x4081cc
403cf6:90		nop
403cf7:90		nop
403cf8:ff 25 c8 81 40 00		jmp *0x4081c8
403cfe:90		nop
403cff: 90		nop
403d00:	ff 25 bc 81 40 00	jmp *0x4081bc
403d06:	90	nop
403d07:	90	nop
403d08:	ff 25 b4 81 40 00	jmp *0x4081b4
403d0e:	90	nop
403d0f:	90	nop
403d10:	ff 25 ac 81 40 00	jmp *0x4081ac
403d16:	90	nop
403d17:	90	nop
403d18:	ff 25 a8 81 40 00	jmp *0x4081a8
403d1e:	90	nop
403d1f:	90	nop
403d20:	ff 25 a0 81 40 00	jmp *0x4081a0
403d26:	90	nop
403d27:	90	nop
403d28:	ff 25 9c 81 40 00	jmp *0x40819c
403d2e:	90	nop
403d2f:	90	nop
403d30:	ff 25 94 81 40 00	jmp *0x408194
403d36:	90	nop
403d37:	90	nop
403d38:	ff 25 80 81 40 00	jmp *0x408180
403d3e:	90	nop
403d3f:	90	nop
403d40:	ff 25 7c 81 40 00	jmp *0x40817c
403d46:	90	nop
403d47:	90	nop
403d48:	ff 25 78 81 40 00	jmp *0x408178
403d4e:	90	nop
403d4f:	90	nop
403d50:	ff 25 74 81 40 00	jmp *0x408174
403d56:	90	nop
403d57:	90	nop
403d58:	ff 25 70 81 40 00	jmp *0x408170
403d5e:	90	nop
403d5f:	90	nop
403d60:	ff 25 6c 81 40 00	jmp *0x40816c
403d66:	90	nop
403d67:	90	nop
403d68:	ff 25 68 81 40 00	jmp *0x408168
403d6e:	90	nop
403d6f:	90	nop
403d70:	ff 25 64 81 40 00	jmp *0x408164
403d76:	90	nop
403d77:	90	nop

403d78:	ff 25 60 81 40 00	jmp	*0x408160
403d7e:	90	nop	
403d7f:	90	nop	
403d80:	ff 25 5c 81 40 00	jmp	*0x40815c
403d86:	90	nop	
403d87:	90	nop	
403d88:	ff 25 58 81 40 00	jmp	*0x408158
403d8e:	90	nop	
403d8f:	90	nop	
403d90:	ff 25 54 81 40 00	jmp	*0x408154
403d96:	90	nop	
403d97:	90	nop	
403d98:	ff 25 50 81 40 00	jmp	*0x408150
403d9e:	90	nop	
403d9f:	90	nop	
403da0:	ff 25 4c 81 40 00	jmp	*0x40814c
403da6:	90	nop	
403da7:	90	nop	
403da8:	ff 25 48 81 40 00	jmp	*0x408148
403dae:	90	nop	
403daf:	90	nop	
403db0:	ff 25 44 81 40 00	jmp	*0x408144
403db6:	90	nop	
403db7:	90	nop	
403db8:	ff 25 40 81 40 00	jmp	*0x408140
403dbe:	90	nop	
403dbf:	90	nop	
403dc0:	ff 25 3c 81 40 00	jmp	*0x40813c
403dc6:	90	nop	
403dc7:	90	nop	
403dc8:	ff 25 8c 81 40 00	jmp	*0x40818c
403dce:	90	nop	
403dcf:90	nop		
403dd0:	ff 25 88 81 40 00	jmp	*0x408188
403dd6:	90	nop	
403dd7:	90	nop	
403dd8:	66 90	xchg	%ax,%ax
403dda:	66 90	xchg	%ax,%ax
403ddc:	66 90	xchg	%ax,%ax
403dde:	66 90	xchg	%ax,%ax
403de0:	55	push	%ebp
403de1:	89 e5	mov	%esp,%ebp
403de3:	5d	pop	%ebp
403de4:	e9 57 d5 ff ff	jmp	0x401340
403de9:	90	nop	
403dea:	90	nop	
403deb:	90	nop	
403dec:	90	nop	
403ded:	90	nop	
403dee:	90	nop	
403def:	90	nop	
403df0:	ff	(bad)	
403df1:	ff	(bad)	

```
403df2:      ff          (bad)
403df3:      ff e0      jmp    *%eax
403df5:      3d 40 00 00 00      cmp    $0x40,%eax
403dfa:      00 00          add    %al,(%eax)
403dfc: ff          (bad)
403dfd:      ff          (bad)
403dfe:      ff          (bad)
403dff: ff 00          incl   (%eax)
403e01:      00 00          add    %al,(%eax)
...
```