

```

1 804841c; movzx edx, byte ptr [ebp+var_D]; //k1
2 8048420; movzx eax, byte ptr [ebp+var_C]; //k2
3 8048424; add eax, edx;
4 8048426; mov byte ptr [ebp+var_B], al;
5 8048429; movzx edx, byte ptr [ebp+var_C]; //k2
6 804842d; movzx eax, byte ptr [ebp+var_A]; //k3
7 8048431; sub edx, eax;
8 8048433; mov eax, edx;
9 8048435; mov byte ptr [ebp+var_9], al;
10 8048438; movzx eax, byte ptr [ebp+var_B];
11 804843c; cmp al, byte ptr [ebp+var_9];
12 804843f; jb 0x8048451;
13 8048441; sub esp, 0xc;

```

a. Execution Trace

```

1 var_D = k1;  edx = zeroext(k1)
2 var_C = k2;  eax = zeroext(k2)
3 eax = zeroext(k1) + zeroext(k2);  edx = zeroext(k1)
4 var_B = k1 + k2
5 var_C = k2;  edx = zeroext(k2)
6 var_A = k3;  eax = zeroext(k3)
7 eax = zeroext(k3);  edx = zeroext(k2) - zeroext(k3)
8 eax = zeroext(k2) - zeroext(k3)
9 var_9 = k2 - k3
10 eax = k1 + k2
11 CF = (k1 + k2) > (k2 - k3)
12 Formula: k1 ≤ k3
13 esp = C1 - 0xc

```

b. Symbolic Execution