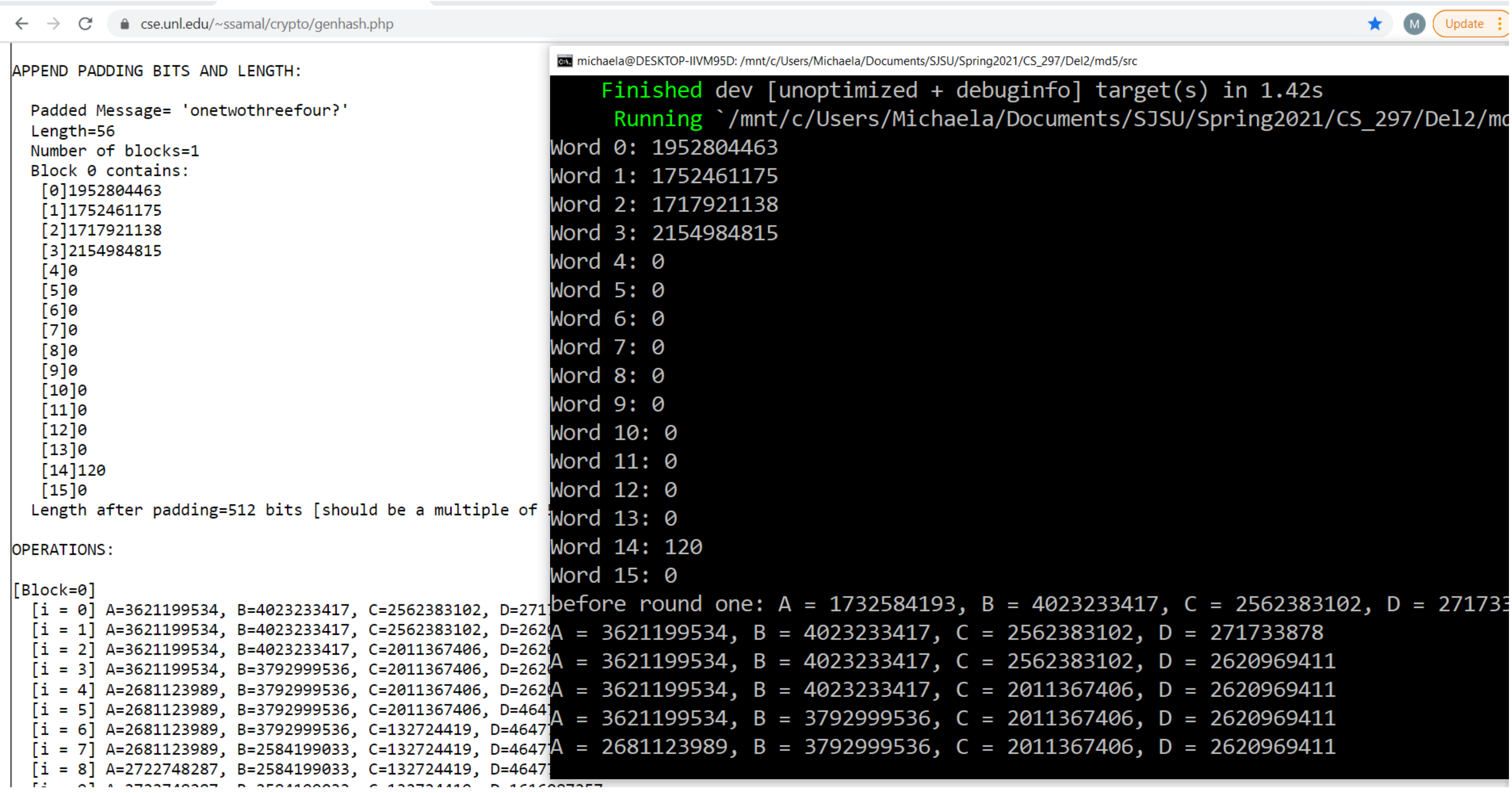
Fixed md5

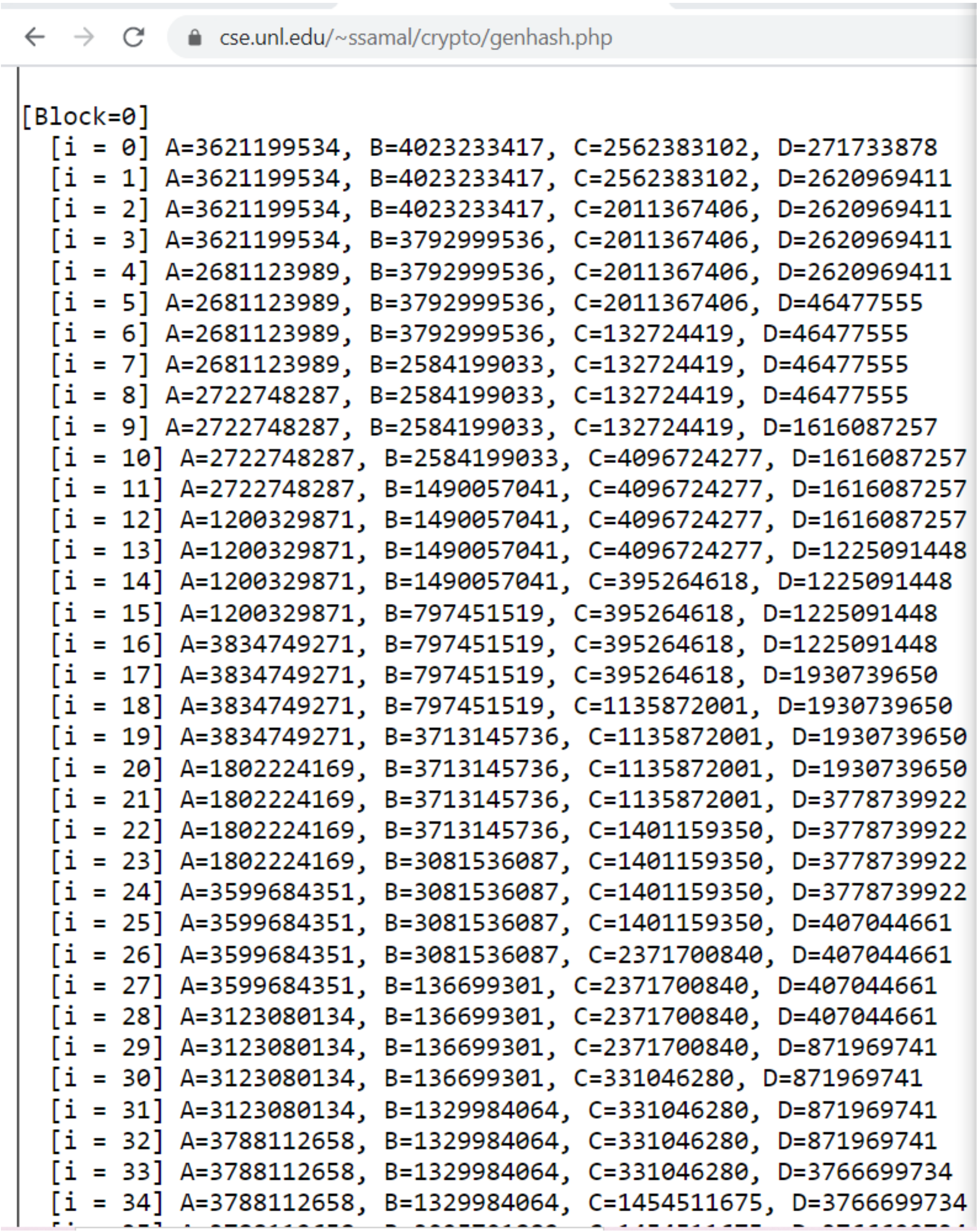
- initial values of registers were wrong
- had to reverse the bytes of the input
- bitshift left was not circular
- had to move mods inside parentheses



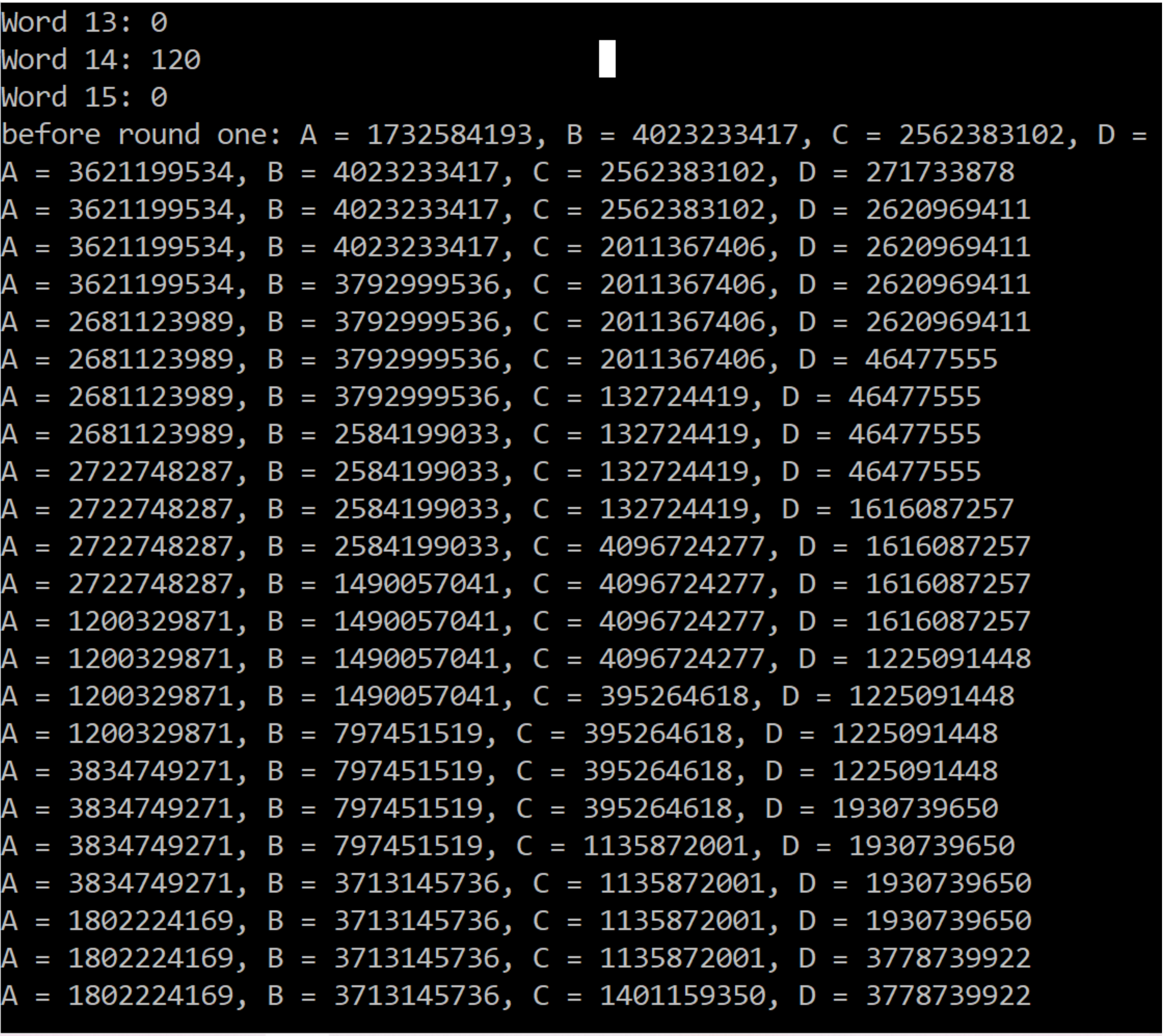
```
APPEND PADDING BITS AND LENGTH:

  Padded Message= 'onetwothreefour?'
  Length=56
  Number of blocks=1
  Block 0 contains:
   [0]1952804463
   [1]1752461175
   [2]1717921138
   [3]2154984815
   [4]0
   [5]0
   [6]0
   [7]0
   [8]0
   [9]0
   [10]0
   [11]0
   [12]0
   [13]0
   [14]120
   [15]0
  Length after padding=512 bits [should be a multiple of 

OPERATIONS:

[Block=0]
  [i = 0] A=3621199534, B=4023233417, C=2562383102, D=271
  [i = 1] A=3621199534, B=4023233417, C=2562383102, D=262
  [i = 2] A=3621199534, B=4023233417, C=2011367406, D=262
  [i = 3] A=3621199534, B=3792999536, C=2011367406, D=262
  [i = 4] A=2681123989, B=3792999536, C=2011367406, D=262
  [i = 5] A=2681123989, B=3792999536, C=2011367406, D=464
  [i = 6] A=2681123989, B=3792999536, C=132724419, D=4647
  [i = 7] A=2681123989, B=2584199033, C=132724419, D=4647
  [i = 8] A=2722748287, B=2584199033, C=132724419, D=4647
  [i = 9] A=2722748287, B=2584199033, C=132724419, D=1616987257
```

michaela@DESKTOP-IIVM95D: /mnt/c/Users/Michaela/Documents/SJSU/Spring2021/CS_297/Del2/md5/src

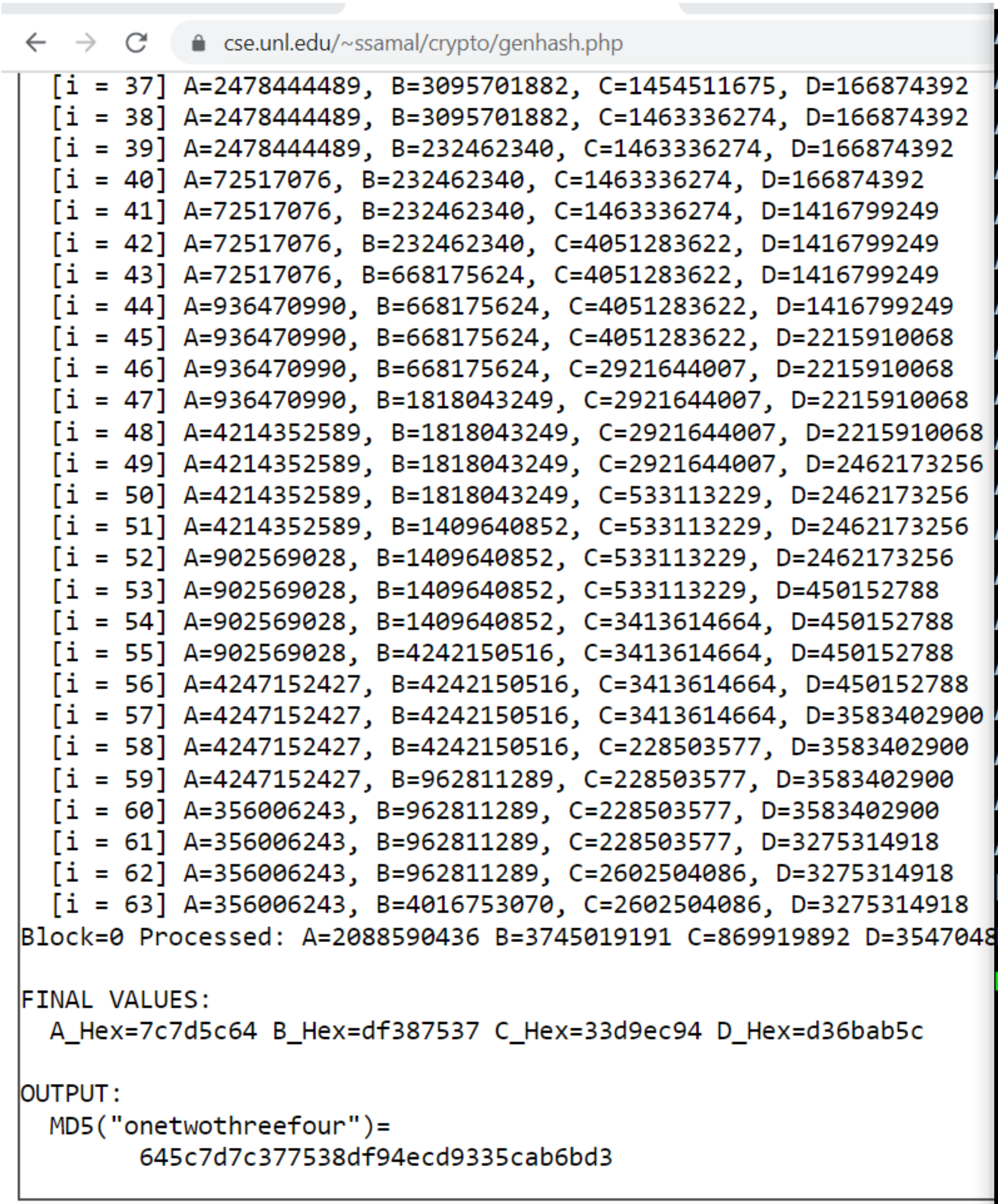
```
    Finished dev [unoptimized + debuginfo] target(s) in 1.42s
     Running `/mnt/c/Users/Michaela/Documents/SJSU/Spring2021/CS_297/Del2/md
Word 0: 1952804463
Word 1: 1752461175
Word 2: 1717921138
Word 3: 2154984815
Word 4: 0
Word 5: 0
Word 6: 0
Word 7: 0
Word 8: 0
Word 9: 0
Word 10: 0
Word 11: 0
Word 12: 0
Word 13: 0
Word 14: 120
Word 15: 0
before round one: A = 1732584193, B = 4023233417, C = 2562383102, D = 271733
A = 3621199534, B = 4023233417, C = 2562383102, D = 271733878
A = 3621199534, B = 4023233417, C = 2562383102, D = 2620969411
A = 3621199534, B = 4023233417, C = 2011367406, D = 2620969411
A = 3621199534, B = 3792999536, C = 2011367406, D = 2620969411
A = 2681123989, B = 3792999536, C = 2011367406, D = 2620969411
```



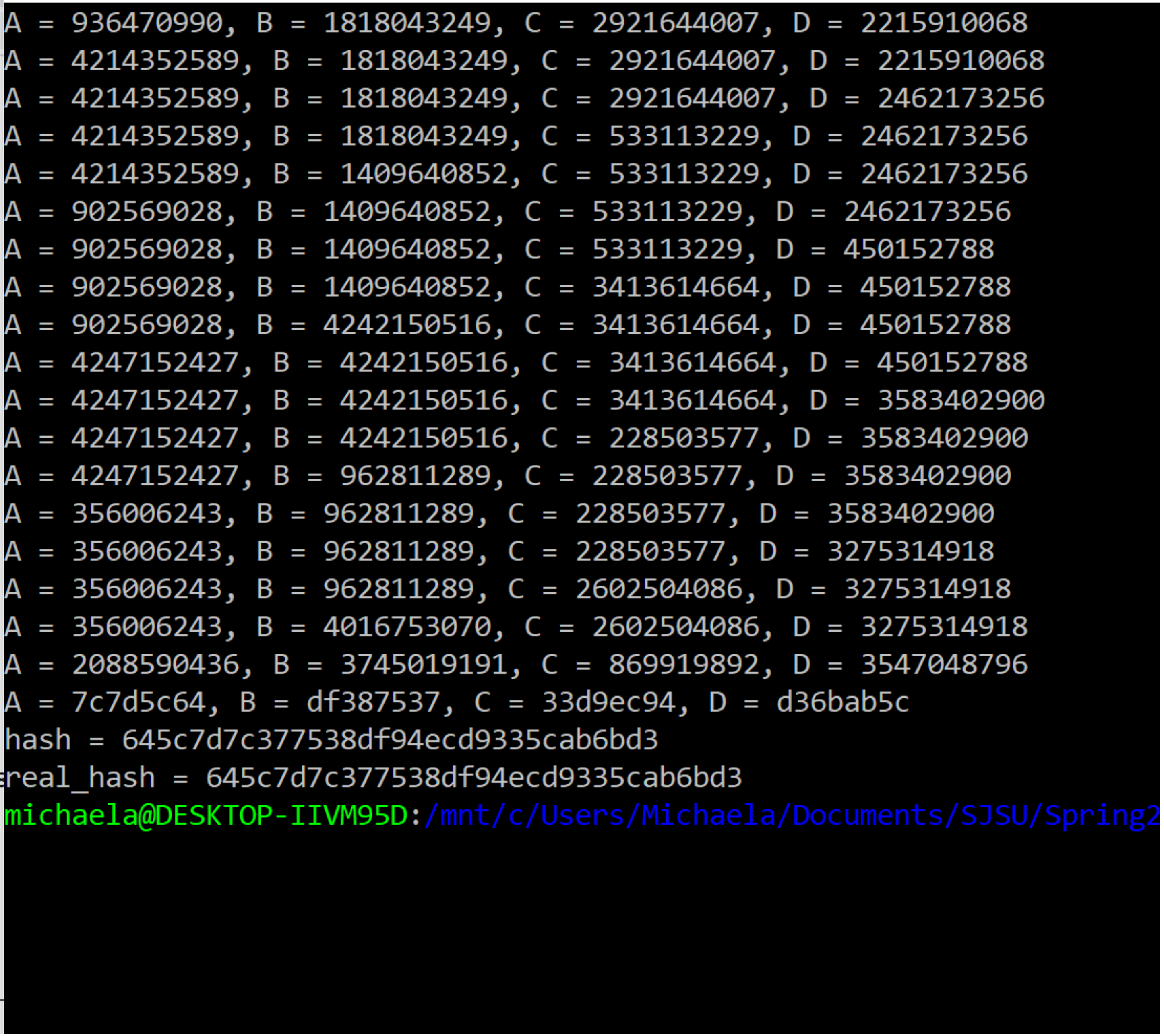
```
[Block=0]
  [i = 0] A=3621199534, B=4023233417, C=2562383102, D=271733878
  [i = 1] A=3621199534, B=4023233417, C=2562383102, D=2620969411
  [i = 2] A=3621199534, B=4023233417, C=2011367406, D=2620969411
  [i = 3] A=3621199534, B=3792999536, C=2011367406, D=2620969411
  [i = 4] A=2681123989, B=3792999536, C=2011367406, D=2620969411
  [i = 5] A=2681123989, B=3792999536, C=2011367406, D=46477555
  [i = 6] A=2681123989, B=3792999536, C=132724419, D=46477555
  [i = 7] A=2681123989, B=2584199033, C=132724419, D=46477555
  [i = 8] A=2722748287, B=2584199033, C=132724419, D=46477555
  [i = 9] A=2722748287, B=2584199033, C=132724419, D=1616087257
  [i = 10] A=2722748287, B=2584199033, C=4096724277, D=1616087257
  [i = 11] A=2722748287, B=1490057041, C=4096724277, D=1616087257
  [i = 12] A=1200329871, B=1490057041, C=4096724277, D=1616087257
  [i = 13] A=1200329871, B=1490057041, C=4096724277, D=1225091448
  [i = 14] A=1200329871, B=1490057041, C=395264618, D=1225091448
  [i = 15] A=1200329871, B=797451519, C=395264618, D=1225091448
  [i = 16] A=3834749271, B=797451519, C=395264618, D=1225091448
  [i = 17] A=3834749271, B=797451519, C=395264618, D=1930739650
  [i = 18] A=3834749271, B=797451519, C=1135872001, D=1930739650
  [i = 19] A=3834749271, B=3713145736, C=1135872001, D=1930739650
  [i = 20] A=1802224169, B=3713145736, C=1135872001, D=1930739650
  [i = 21] A=1802224169, B=3713145736, C=1135872001, D=3778739922
  [i = 22] A=1802224169, B=3713145736, C=1401159350, D=3778739922
  [i = 23] A=1802224169, B=3081536087, C=1401159350, D=3778739922
  [i = 24] A=3599684351, B=3081536087, C=1401159350, D=3778739922
  [i = 25] A=3599684351, B=3081536087, C=1401159350, D=407044661
  [i = 26] A=3599684351, B=3081536087, C=2371700840, D=407044661
  [i = 27] A=3599684351, B=136699301, C=2371700840, D=407044661
  [i = 28] A=3123080134, B=136699301, C=2371700840, D=407044661
  [i = 29] A=3123080134, B=136699301, C=2371700840, D=871969741
  [i = 30] A=3123080134, B=136699301, C=331046280, D=871969741
  [i = 31] A=3123080134, B=1329984064, C=331046280, D=871969741
  [i = 32] A=3788112658, B=1329984064, C=331046280, D=871969741
  [i = 33] A=3788112658, B=1329984064, C=331046280, D=3766699734
  [i = 34] A=3788112658, B=1329984064, C=1454511675, D=3766699734
```



```
Word 13: 0
Word 14: 120
Word 15: 0
before round one: A = 1732584193, B = 4023233417, C = 2562383102, D =
A = 3621199534, B = 4023233417, C = 2562383102, D = 271733878
A = 3621199534, B = 4023233417, C = 2562383102, D = 2620969411
A = 3621199534, B = 4023233417, C = 2011367406, D = 2620969411
A = 3621199534, B = 3792999536, C = 2011367406, D = 2620969411
A = 2681123989, B = 3792999536, C = 2011367406, D = 2620969411
A = 2681123989, B = 3792999536, C = 2011367406, D = 46477555
A = 2681123989, B = 3792999536, C = 132724419, D = 46477555
A = 2681123989, B = 2584199033, C = 132724419, D = 46477555
A = 2722748287, B = 2584199033, C = 132724419, D = 46477555
A = 2722748287, B = 2584199033, C = 132724419, D = 1616087257
A = 2722748287, B = 2584199033, C = 4096724277, D = 1616087257
A = 2722748287, B = 1490057041, C = 4096724277, D = 1616087257
A = 1200329871, B = 1490057041, C = 4096724277, D = 1616087257
A = 1200329871, B = 1490057041, C = 4096724277, D = 1225091448
A = 1200329871, B = 1490057041, C = 395264618, D = 1225091448
A = 1200329871, B = 797451519, C = 395264618, D = 1225091448
A = 3834749271, B = 797451519, C = 395264618, D = 1225091448
A = 3834749271, B = 797451519, C = 395264618, D = 1930739650
A = 3834749271, B = 797451519, C = 1135872001, D = 1930739650
A = 3834749271, B = 3713145736, C = 1135872001, D = 1930739650
A = 1802224169, B = 3713145736, C = 1135872001, D = 1930739650
A = 1802224169, B = 3713145736, C = 1135872001, D = 3778739922
A = 1802224169, B = 3713145736, C = 1401159350, D = 3778739922
```



```
  [i = 37] A=2478444489, B=3095701882, C=1454511675, D=166874392
  [i = 38] A=2478444489, B=3095701882, C=1463336274, D=166874392
  [i = 39] A=2478444489, B=232462340, C=1463336274, D=166874392
  [i = 40] A=72517076, B=232462340, C=1463336274, D=166874392
  [i = 41] A=72517076, B=232462340, C=1463336274, D=1416799249
  [i = 42] A=72517076, B=232462340, C=4051283622, D=1416799249
  [i = 43] A=72517076, B=668175624, C=4051283622, D=1416799249
  [i = 44] A=936470990, B=668175624, C=4051283622, D=1416799249
  [i = 45] A=936470990, B=668175624, C=4051283622, D=2215910068
  [i = 46] A=936470990, B=668175624, C=2921644007, D=2215910068
  [i = 47] A=936470990, B=1818043249, C=2921644007, D=2215910068
  [i = 48] A=4214352589, B=1818043249, C=2921644007, D=2215910068
  [i = 49] A=4214352589, B=1818043249, C=2921644007, D=2462173256
  [i = 50] A=4214352589, B=1818043249, C=533113229, D=2462173256
  [i = 51] A=4214352589, B=1409640852, C=533113229, D=2462173256
  [i = 52] A=902569028, B=1409640852, C=533113229, D=2462173256
  [i = 53] A=902569028, B=1409640852, C=533113229, D=450152788
  [i = 54] A=902569028, B=1409640852, C=3413614664, D=450152788
  [i = 55] A=902569028, B=4242150516, C=3413614664, D=450152788
  [i = 56] A=4247152427, B=4242150516, C=3413614664, D=450152788
  [i = 57] A=4247152427, B=4242150516, C=3413614664, D=3583402900
  [i = 58] A=4247152427, B=4242150516, C=228503577, D=3583402900
  [i = 59] A=4247152427, B=962811289, C=228503577, D=3583402900
  [i = 60] A=356006243, B=962811289, C=228503577, D=3583402900
  [i = 61] A=356006243, B=962811289, C=228503577, D=3275314918
  [i = 62] A=356006243, B=962811289, C=2602504086, D=3275314918
  [i = 63] A=356006243, B=4016753070, C=2602504086, D=3275314918
Block=0 Processed: A=2088590436 B=3745019191 C=869919892 D=3547048

FINAL VALUES:
  A_Hex=7c7d5c64 B_Hex=df387537 C_Hex=33d9ec94 D_Hex=d36bab5c

OUTPUT:
  MD5("onetwothreefour")=
        645c7d7c377538df94ecd9335cab6bd3
```



```
A = 936470990, B = 1818043249, C = 2921644007, D = 2215910068
A = 4214352589, B = 1818043249, C = 2921644007, D = 2215910068
A = 4214352589, B = 1818043249, C = 2921644007, D = 2462173256
A = 4214352589, B = 1818043249, C = 533113229, D = 2462173256
A = 4214352589, B = 1409640852, C = 533113229, D = 2462173256
A = 902569028, B = 1409640852, C = 533113229, D = 2462173256
A = 902569028, B = 1409640852, C = 533113229, D = 450152788
A = 902569028, B = 1409640852, C = 3413614664, D = 450152788
A = 902569028, B = 4242150516, C = 3413614664, D = 450152788
A = 4247152427, B = 4242150516, C = 3413614664, D = 450152788
A = 4247152427, B = 4242150516, C = 3413614664, D = 3583402900
A = 4247152427, B = 4242150516, C = 228503577, D = 3583402900
A = 4247152427, B = 962811289, C = 228503577, D = 3583402900
A = 356006243, B = 962811289, C = 228503577, D = 3583402900
A = 356006243, B = 962811289, C = 228503577, D = 3275314918
A = 356006243, B = 962811289, C = 2602504086, D = 3275314918
A = 356006243, B = 4016753070, C = 2602504086, D = 3275314918
A = 2088590436, B = 3745019191, C = 869919892, D = 3547048796
A = 7c7d5c64, B = df387537, C = 33d9ec94, D = d36bab5c
hash = 645c7d7c377538df94ecd9335cab6bd3
real_hash = 645c7d7c377538df94ecd9335cab6bd3
michaela@DESKTOP-IIVM95D:/mnt/c/Users/Michaela/Documents/SJSU/Spring2
```