Assignment 8

The due date for submitting this assignment has passed. As per our records you have not submitted this assignment.

In this assignment you need to implement mutual information analysis attack (discussed in the course).

Once again, we supply an almost complete code snippet in python and you are asked certain gaps to get the correct answer for the following questions. The trace file for answers is also supplied.

1) In line number 81, the correct expression will be:
   
   a. btemp^ct_temp
   b. hw(btemp)
   c. hw(btemp^ct_temp)
   d. None

   No, the answer is incorrect.
   Score: 0
   Accepted Answers:
   a.

2) In line number 105, the correct expression will be:

   a. l_range/iter_val
   b. l_range/count
   c. count/l_range
   d. count/iter_val

   2 points
3) In line number 119, the correct expression will be:
   
   a. sec_count/O_range*L_range
   b. sec_count/O_range
   c. sec_count/count
   d. sec_count/L_range

No, the answer is incorrect.
Score: 0
Accepted Answers:
c.

4) In line number 131, the correct expression will be:
   
   a. P_O_L[i][j]*temp_2
   b. P_O_L[i][j]/temp_2
   c. P_O_L[i][j]/O_range*L_range
   d. None

No, the answer is incorrect.
Score: 0
Accepted Answers:
a.

5) The correct key value will be:
   
   a. 0
   b. 18
   c. 177
   d. 234

No, the answer is incorrect.
Score: 0
Accepted Answers:
c.