Problem 7: Attacker/Attackee

Overview
We all make mistakes when trying to log in to a system. We may forget our passwords or we may have a typo in our user name or password or we may click to log in before completing the entry of our data. Still, in the long run, these things don’t happen all that often. If too many of the login attempts on a system are failing, that may very well be a symptom of a hacking attack. In this problem, we will consider the likelihood of such an attack.

Problem
We will work within a network of N computers, each of which may log in to any other, including itself. Computer A is considered to be attacking Computer B if more than a certain percentage of the log in attempts are failing; this percentage is called the threshold percentage. To prevent spurious reports from inactive systems, there must also be a certain number of attempts to log in before an attack is considered to be under way; this number is called the attack minimum. You are to report all instances of one computer attacking another. In addition, any computer whose overall thresholds (sum of all data) indicate that it is attacking others or being attacked shall be reported appropriately.

Input
The first line of input contains three positive integers P, M, and N, indicating the threshold percentage, the attack minimum, and the number of computers in the network. The maximum possible values for each will be 100. These values are followed by 2N lines of input, each containing N non-negative numbers separated by spaces. The first N lines indicate how many successful logins have taken place from one computer to the next; the second block of N lines describes total login attempts from one computer to the next. (All computers are numbered consecutively starting at zero.) Thus, assuming N=5 (as in the sample output), the second number on the fourth line (remember the initial line of the input!) indicates the number of successful logins from computer 2 to computer 1 (in this case eight good logins.) Similarly, the fourth number on the tenth line indicates the total number of login attempts from computer 3 to itself. (In this case there are ten such logins; you can also verify that – for this data set – all logins from computer 3 to itself were successful.) The data will be internally consistent; there will never be more successful logins than total login attempts for a given pair of computers. The total number of login attempts will be less than 1,000,000.

- over-

---

1 In other words, although one failure in one attempt would be a 100% failure rate, there just isn’t enough data to go on here.
Output

The output is a series of lines of text describing the attack, followed by a single line indicating that the report is complete. The lines describing the attack may be presented in any order, but must be formatted exactly as in the sample output. (No line has any leading or trailing spaces despite indentation and margin concerns in the printing of the sample output.)

Example (First nine lines of the output may be in any order)

Input

50 4 5
0 2 1 2 6
3 0 0 1 30
9 8 0 1 7
20 1 5 10 0
2 2 0 0 7
8 4 3 6 11
4 0 9 5 30
12 8 4 4 7
20 3 5 10 0
2 4 6 0 7

Output

Computer 0 is attacking computer 0.
Computer 0 is attacking computer 3.
Computer 1 is attacking computer 2.
Computer 1 is attacking computer 3.
Computer 2 is attacking computer 2.
Computer 2 is attacking computer 3.
Computer 4 is attacking computer 2.
Computer 0 is generally attacking the network.
Computer 2 is under general attack.
Report complete.