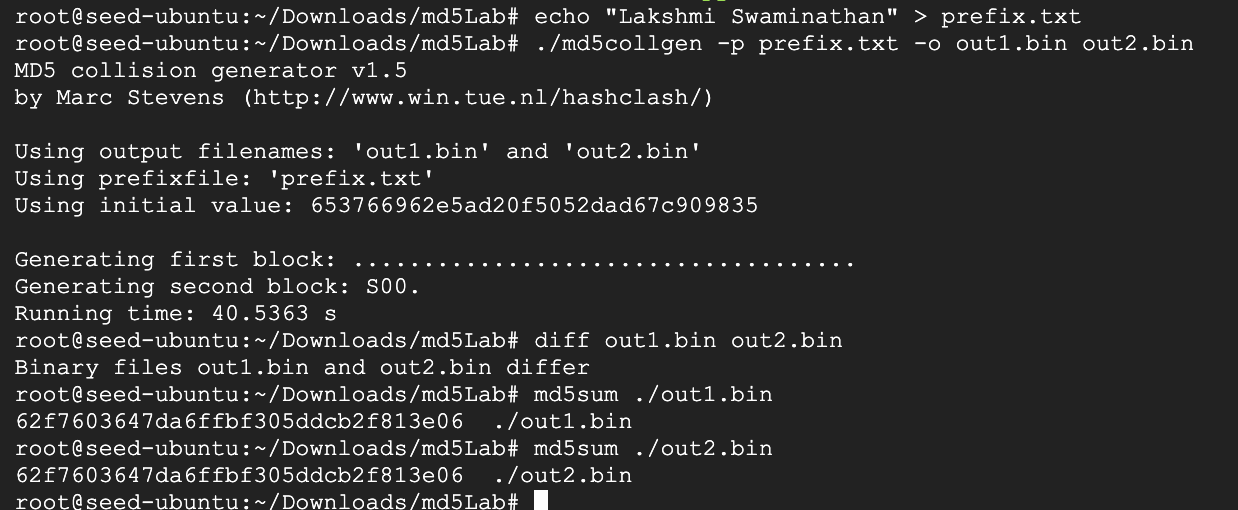
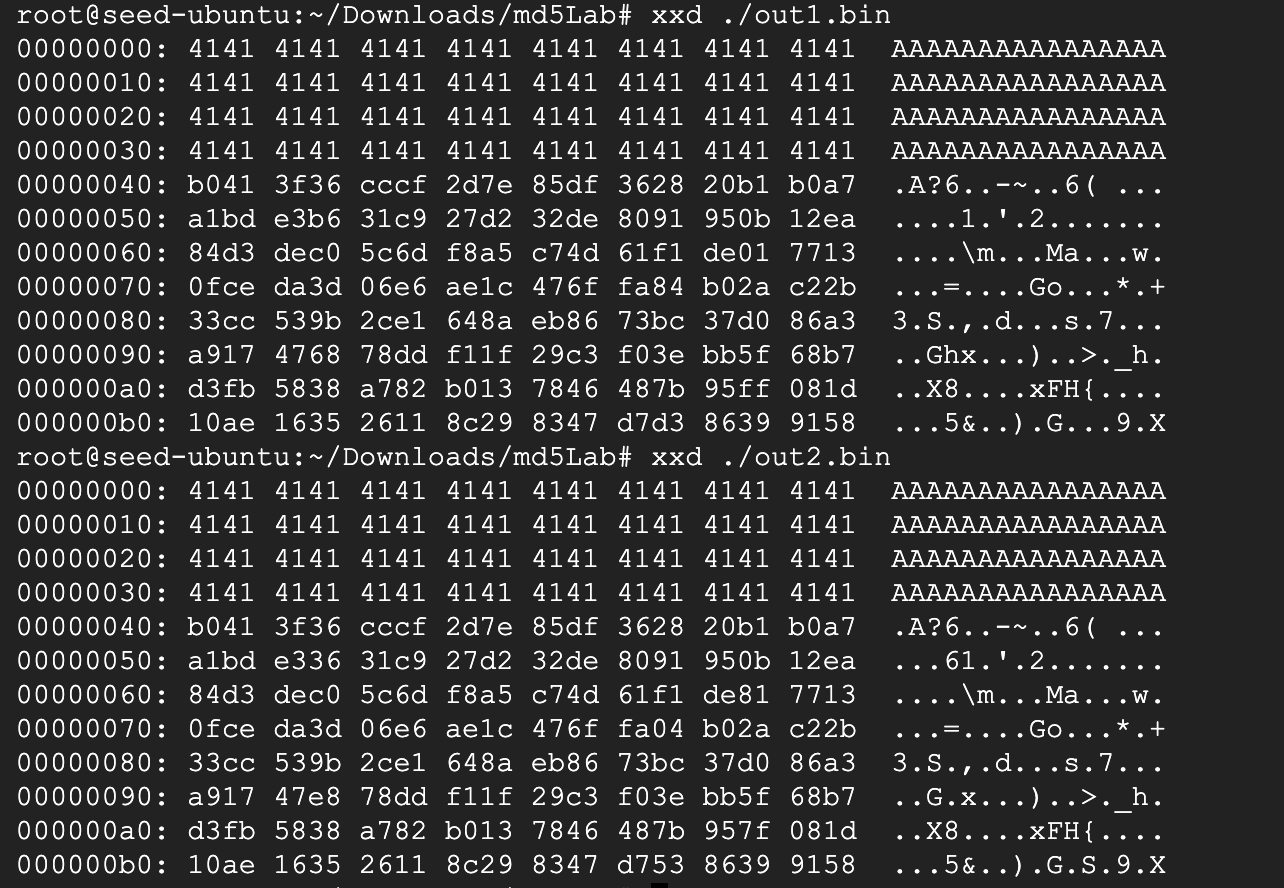
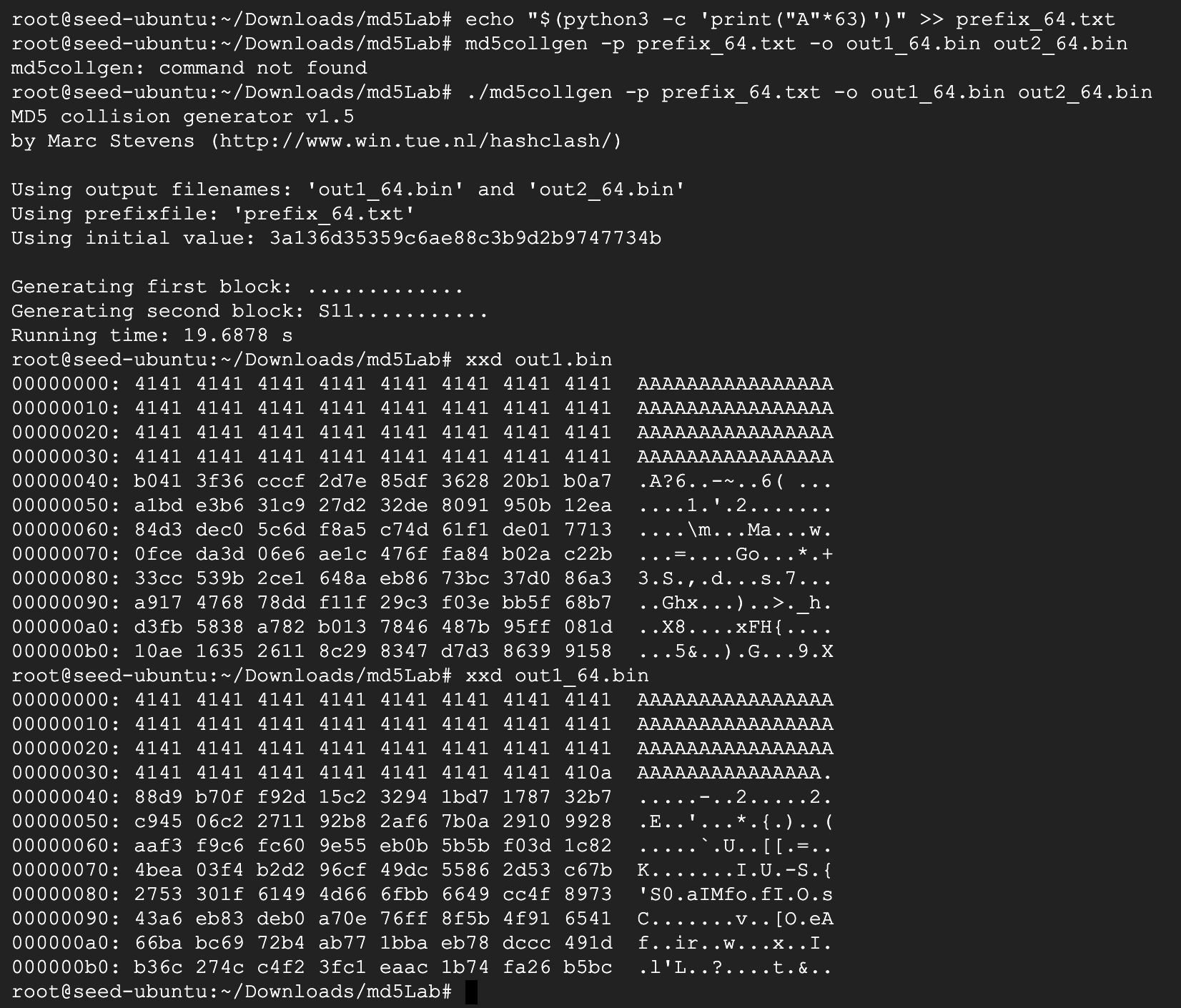
Task 1:



If the length of your prefix file is not a multiple of 64, the md5collgen program will pad the prefix to make its length a multiple of 64 bytes. This is because the MD5 algorithm processes data in 64-byte blocks.



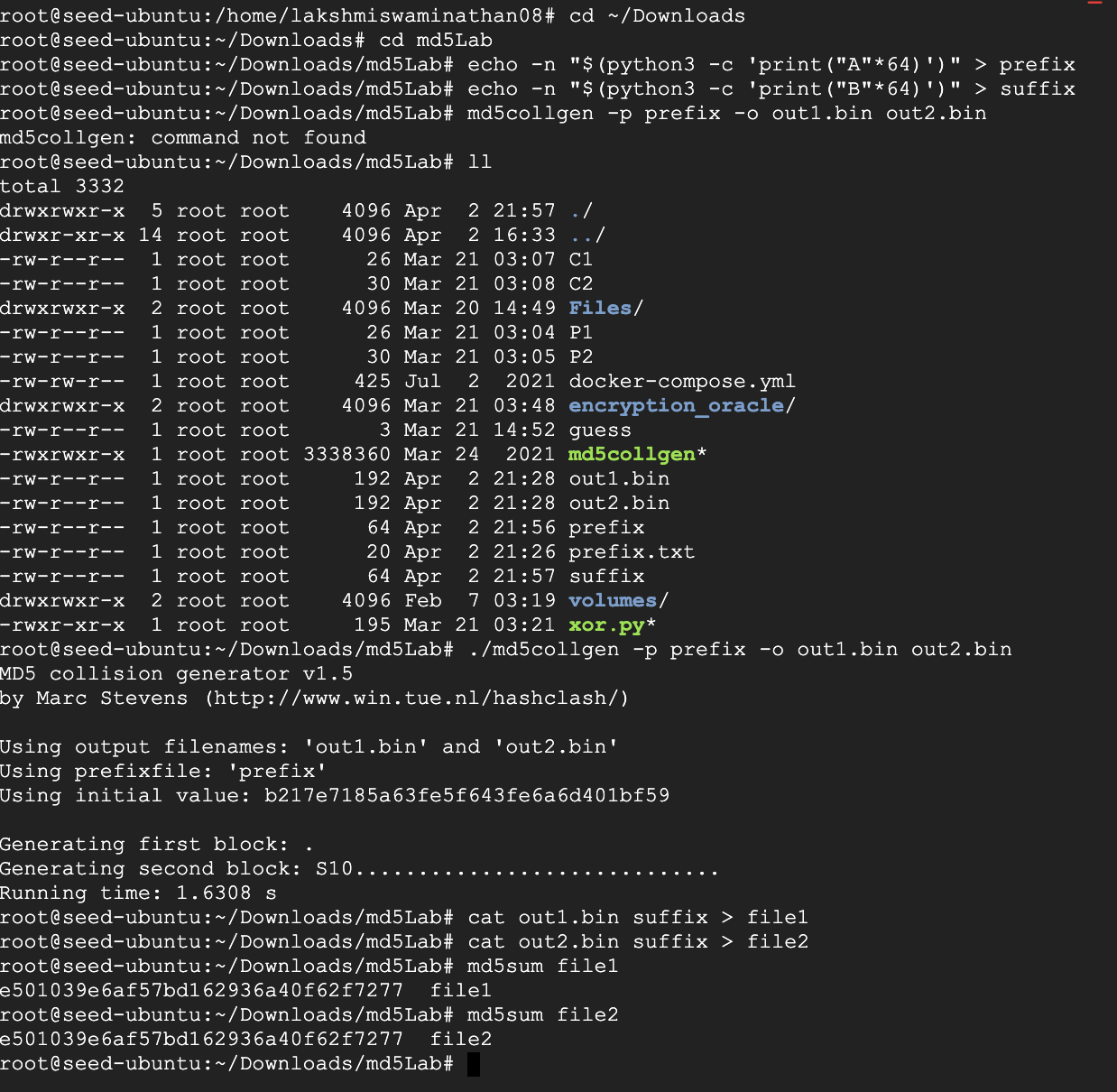
## Question 2 and Question 3



If the prefix file is exactly 64 bytes, the md5collgen program will directly append the collision blocks to the prefix.

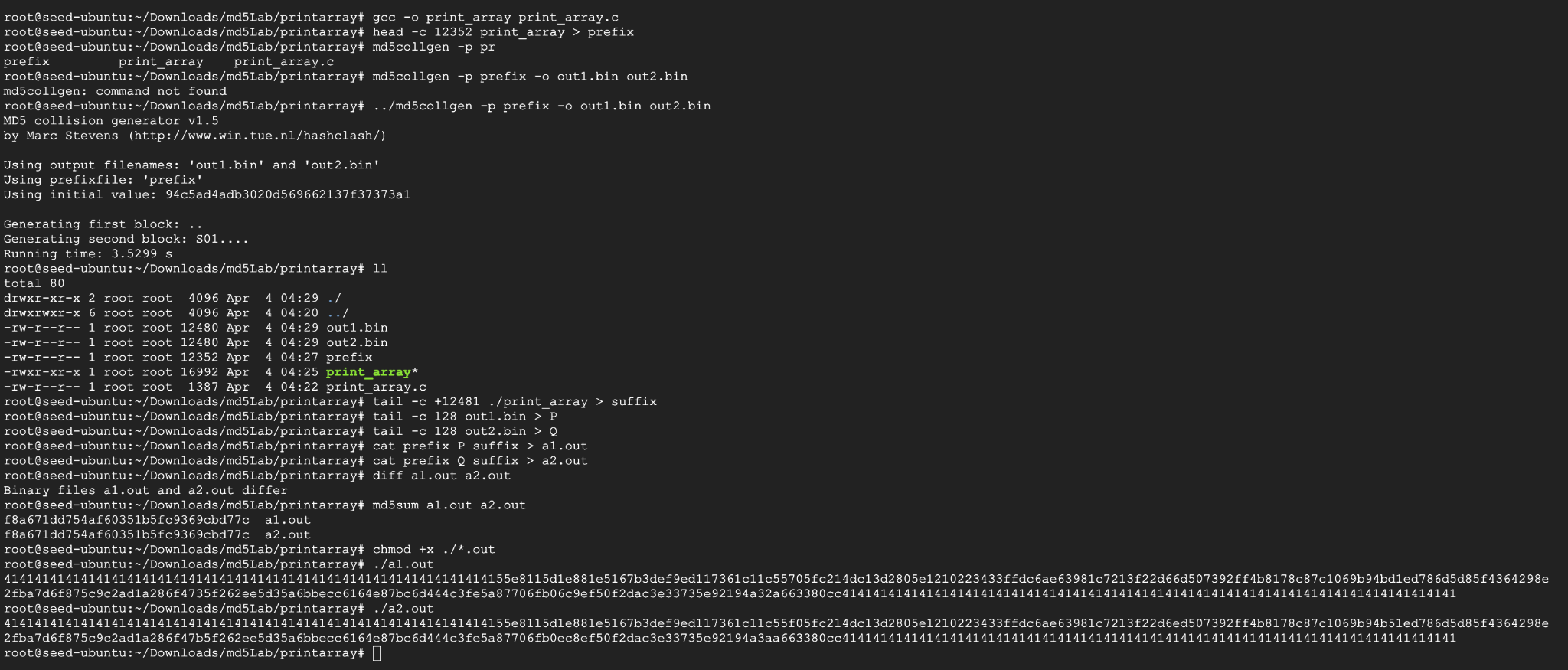
The data (128 bytes) generated by md5collgen are not completely different for the two output files. The first 64 bytes of the collision blocks (P and Q) are identical. The difference lies in the remaining 64 bytes.

Task 2



Task 3







Task 4



