Question Number 10

Find the flaw in the following argument: Consider the following attack against one-time pad: upon seeing a ciphertext c, the eavesdropper tries every candidate key $k \epsilon \{0,1\}^n$ until she has found the one that was used, at which point she outputs the plaintext m. This contradicts the argument that the eavesdropper can obtain no information about m by seeing the ciphertext.

Solution. Solution is in notebook.