Comp7402 - Lab #1

Objective: Cryptanalysis of a Book Cipher. You may work in groups of two.

- Consider the following message that contains a set of numerals that has been intercepted from someone who is suspected of sending secret information:

  228 4 8 229 49 7 61 14 5 66 1 6 30 9 12 113 24 10 201 1 11 229 41 2 30 21 10 179 47 2 30 9 3 124 3 9 200 8 5

- There is good data to suggest that this is a book cipher. Your task is to attempt to discover the key and decrypt the message.

- Field agents have a very good hunch about the identity of the sender, using some surveillance techniques have provided you with the following information that may be of help:

  - The agent is known to be a keen classics scholar (especially the **history** of the Roman Empire) and in particular is an avid reader of classic historians of the Roman Empire such as **Tacitus** and **Thucydides**.

  - A covert search of the suspected agent's hotel room did not reveal any copies of books. However long-range visual surveillance has shown that the agent reads a lot of online material. It may very well be possible that online books are preferred to physical copies.

  - It is also very unlikely that the agent keeps any electronic copies or is in possession of any crypto applications. In other words, his tradecraft is impeccable.

- Your task is to make an intelligent guess at the possible keys (books) and determine the exact one being used as quickly as possible.