W07 Feb 26 (D2) Napoleon's cipher: Switch-defined key

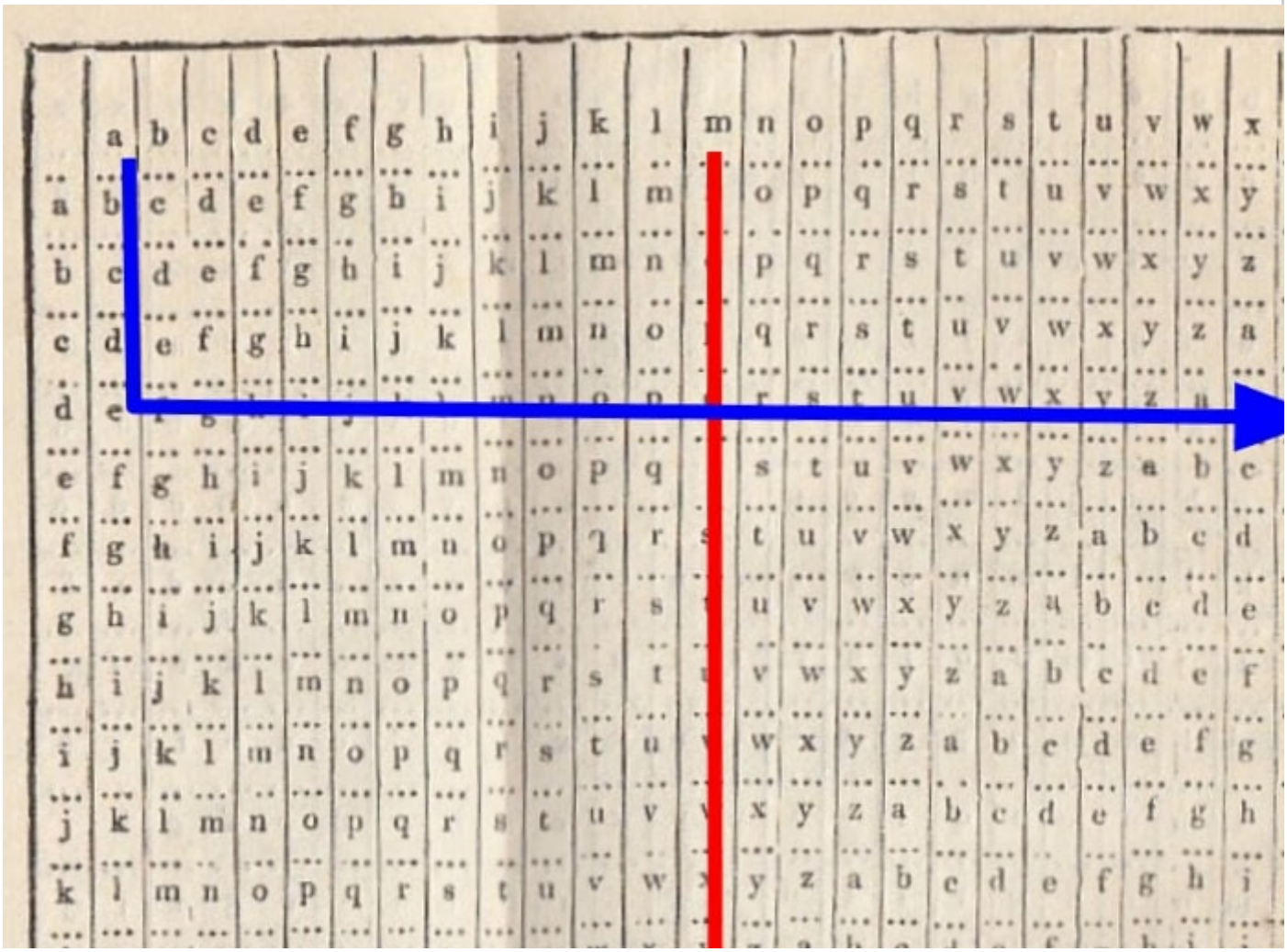
Jose Ferreira

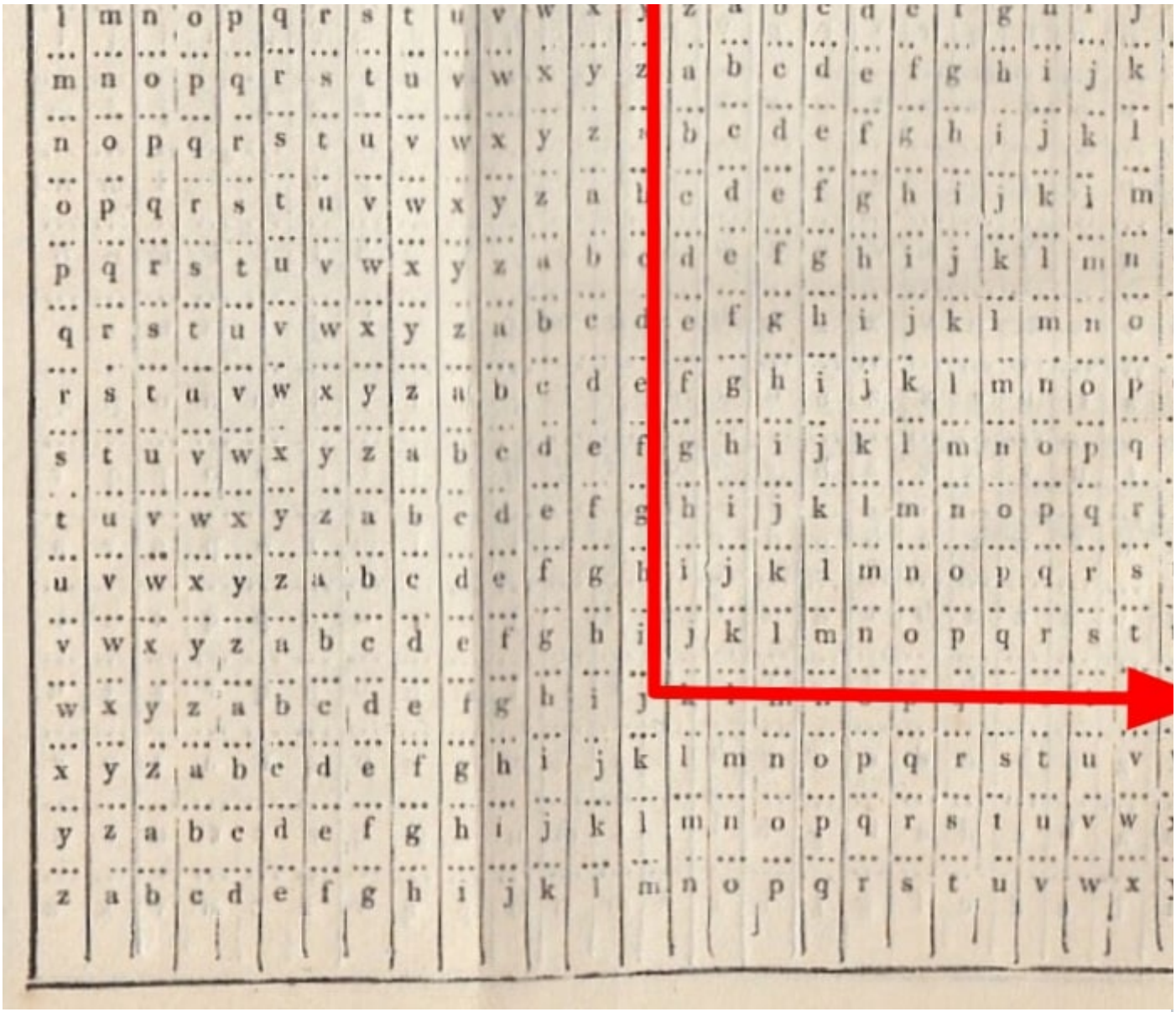
All Sections

These questions are presented under the following assumptions:

- They may be selected to be part of the final exam
- Responses must be posted by the students (not me)
- I will call your attention to any mistakes or wrong content posted in response

Consider an early Napoleon's cipher that uses a matrix with 27 lines and 27 columns, laying out the 26 letters as shown below. To encrypt a message, locate its first letter in the first line, proceed downwards until you find the first letter of your key, then proceed to the right until the last column where you'll find the letter to use in your ciphered message (shown in red below). Move on to the second letter and repeat the procedure (shown in blue). And likewise until the message is completely ciphered.





Example using the key “Jean-Jacques Rousseau”:

```
Make every day count

|||| ||||| ||| |||||

Jean Jacqu esR ousse

|||| ||||| ||| |||||

wdpi eexyv ars lfxek
```

Would it be possible to use as key the position of the 8 switches located in the Basys-3 board (instead of a sequence of ASCII codes as represented above)? In case your answer is yes,

would that solution provide a stronger cipher than the example key shown above?