W07 Feb 26 (D1) Napoleon's cipher: Strength of the key

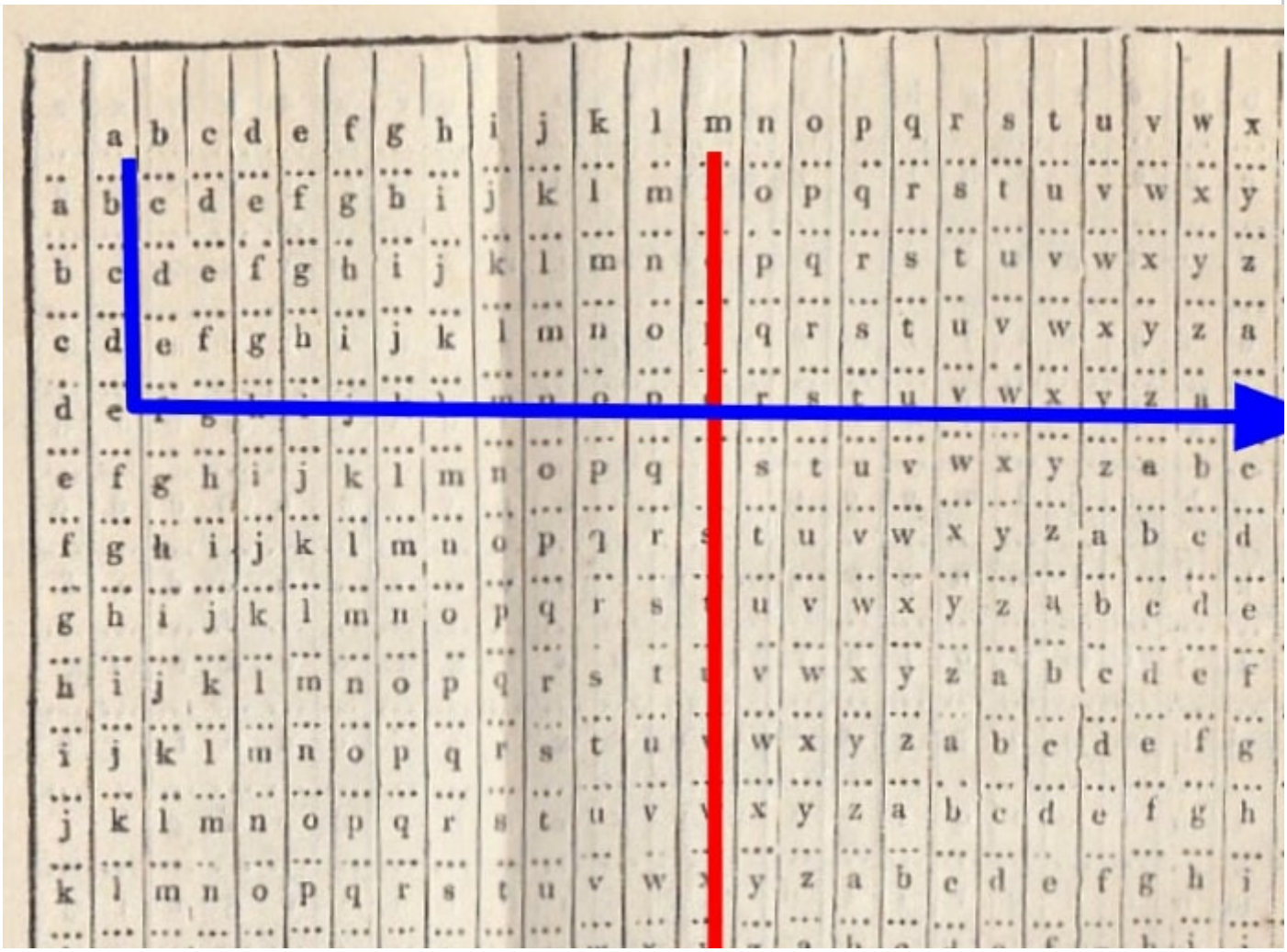
Jose Ferreira

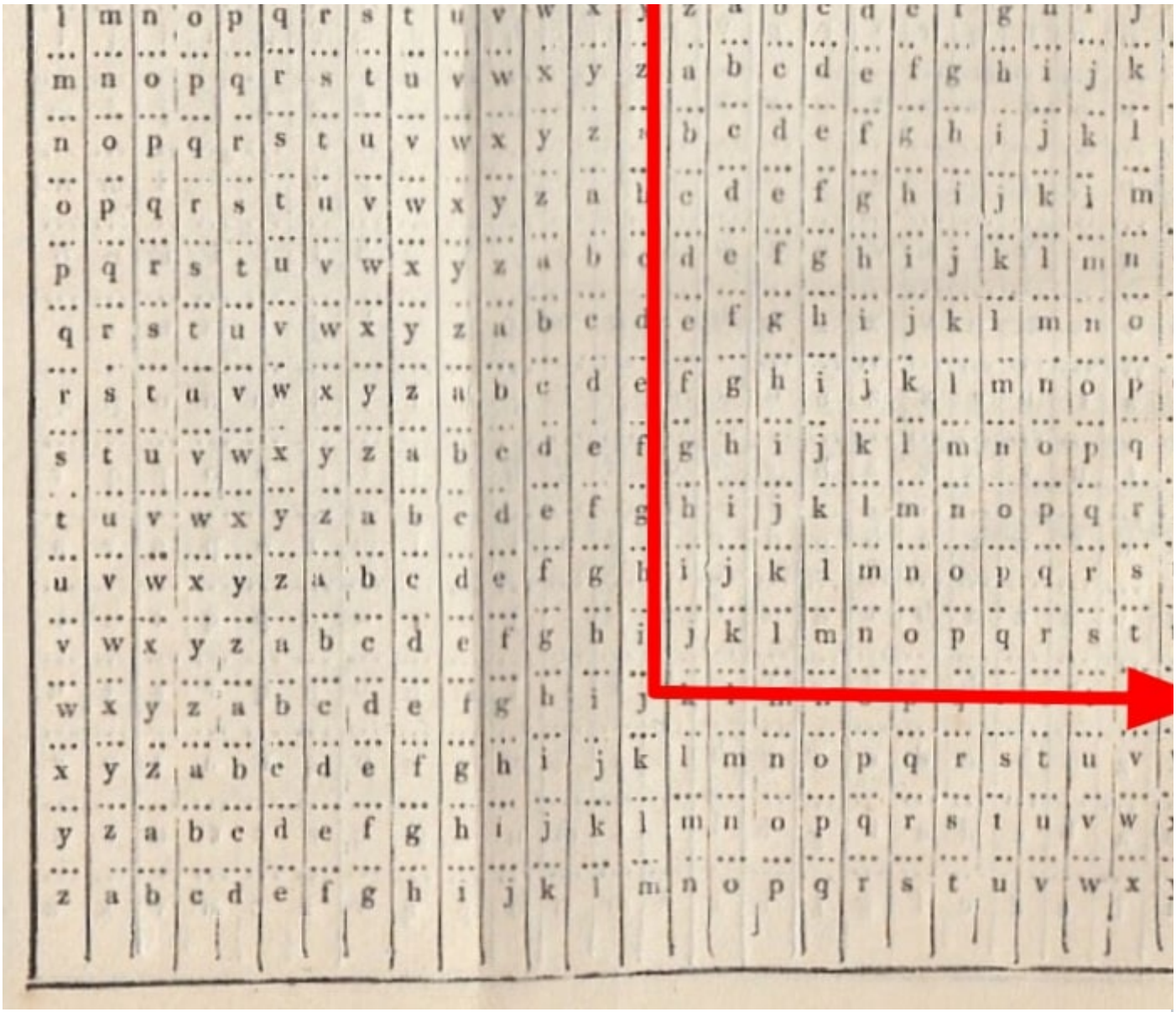
All Sections

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
```

1. Will the encryption method become weaker if the length of the key is reduced? Why?
2. What would be an acceptable length in the case of an FPGA implementation?

Search entries or author | Unread | Subscribe

Reply