W06 Feb 19 (D2) Napoleon's cipher: Data path

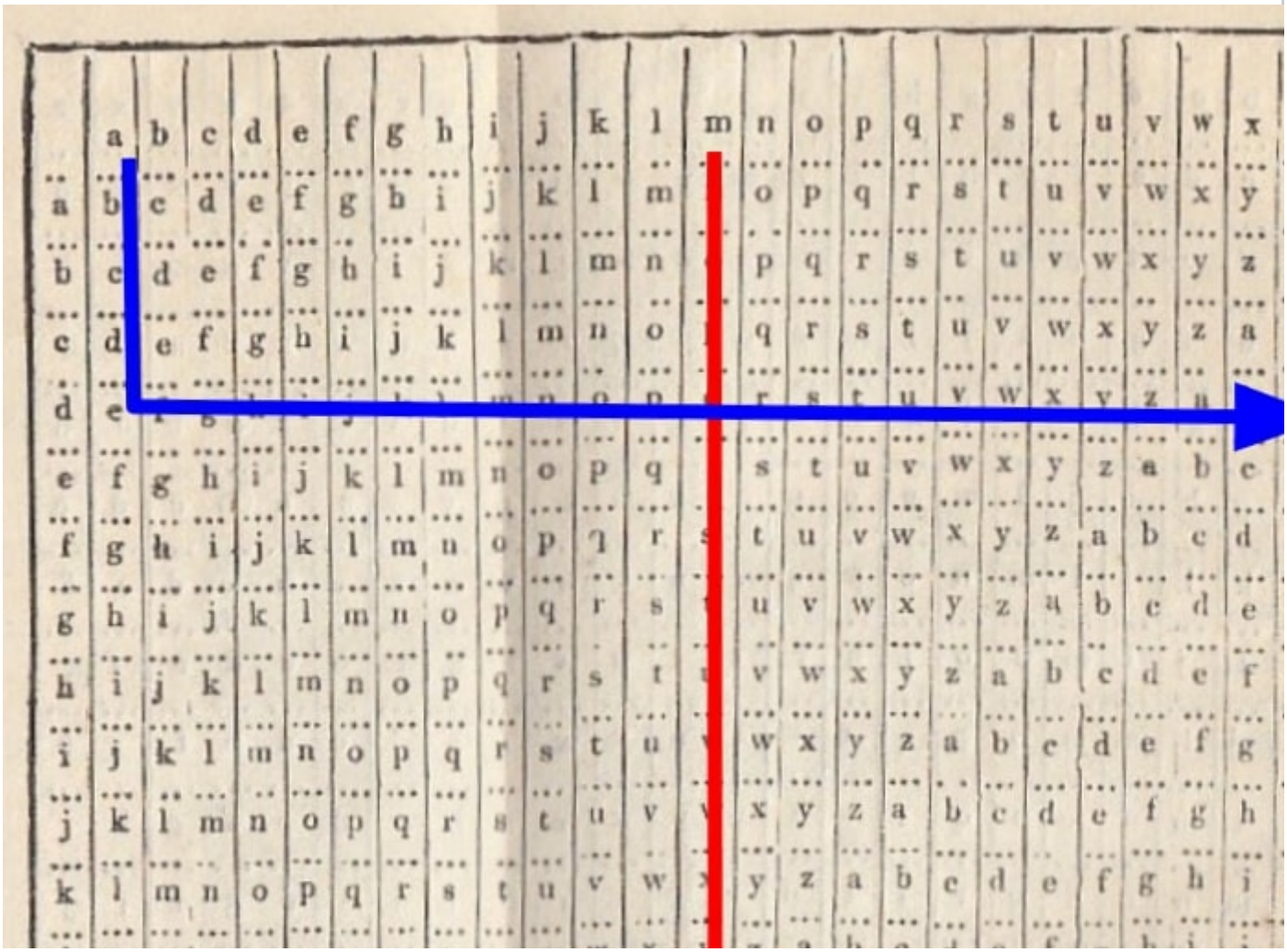
Jose Ferreira

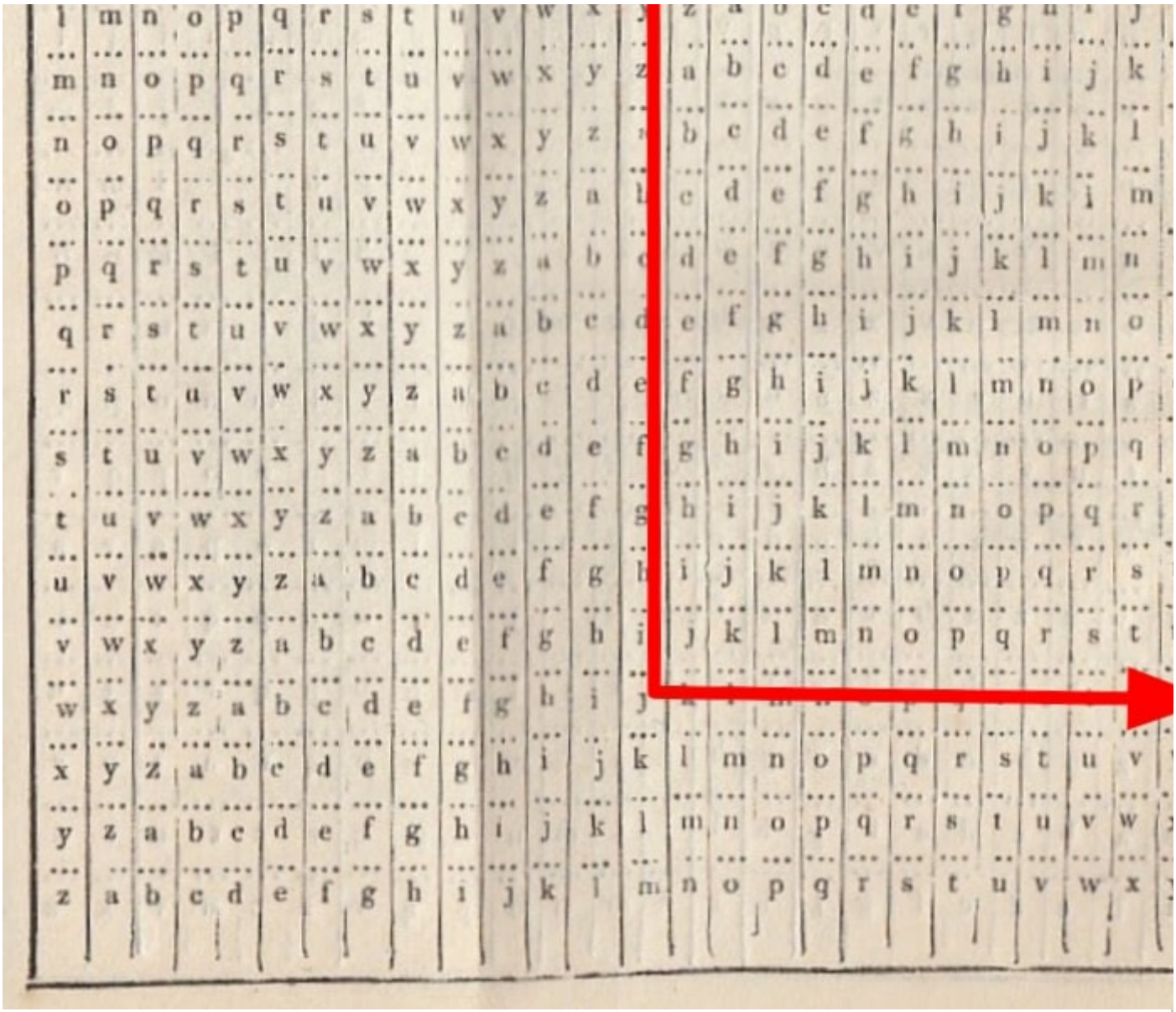
All Sections

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.



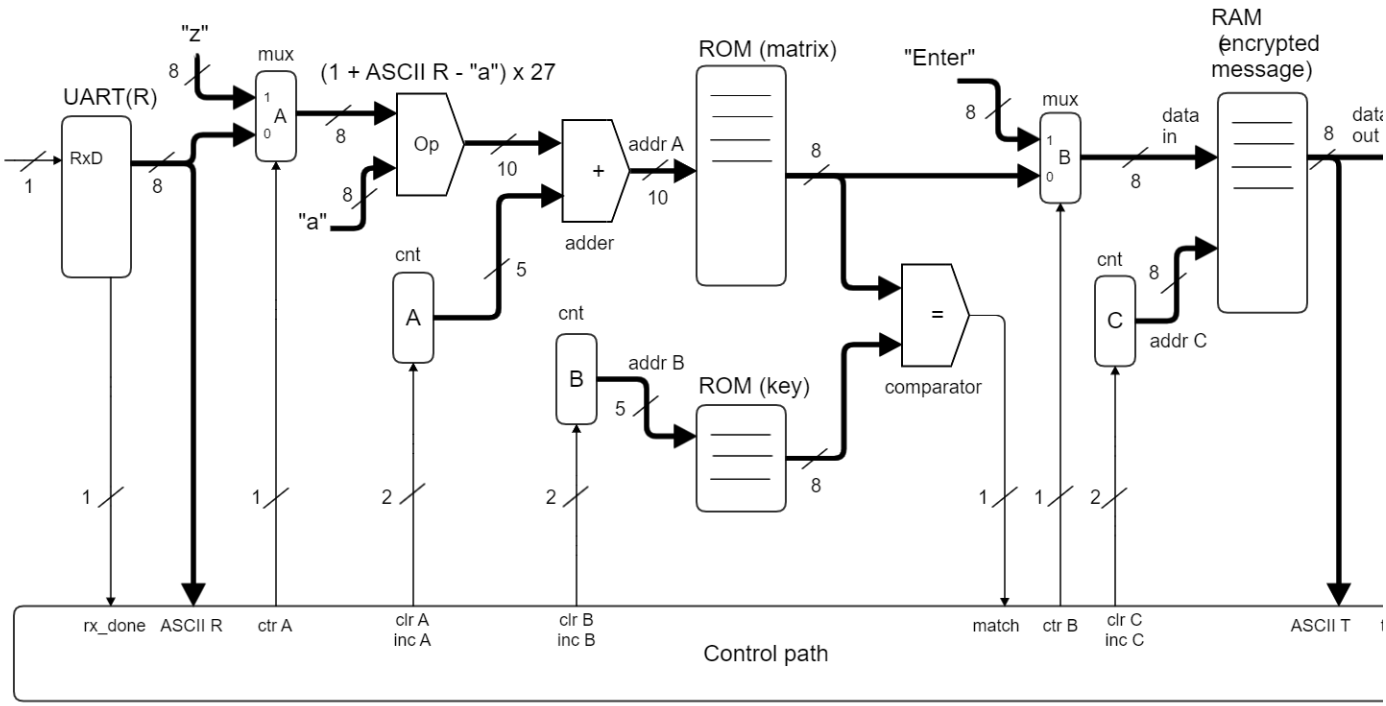


Example using the key “Jean-Jacques Rousseau”:

```
Make every day count
|||| ||||| ||| |||||
Jean Jacqu esR ousse
|||| ||||| ||| |||||
wdpi eexyv ars lfxek
```

The following data path represents a draft of a possible solution for encryption, where one ROM is used to store the original matrix, a second ROM is used to store the key, and a RAM is

used to store the encrypted messages -- the user will type in the message, which each letter being encrypted and stored in RAM as it is received, and the full encrypted message will be sent back to the PC when the ASCII code for the “Enter” code is received (pressing “Enter” marks the end of the message).



Note: If you have questions concerning the envisaged operation of the data path above, please do not hesitate to post them here.

1. Present an ASMD chart for the data path architecture shown above, including receive and transmit states.
2. Would it be possible to improve the solution presented above for the data path core (comprising the matrix ROM and the blocks to its left up to the receiving UART subsystem)?