W08 Mar 04 (D1) Napoleon's cipher: Math formula

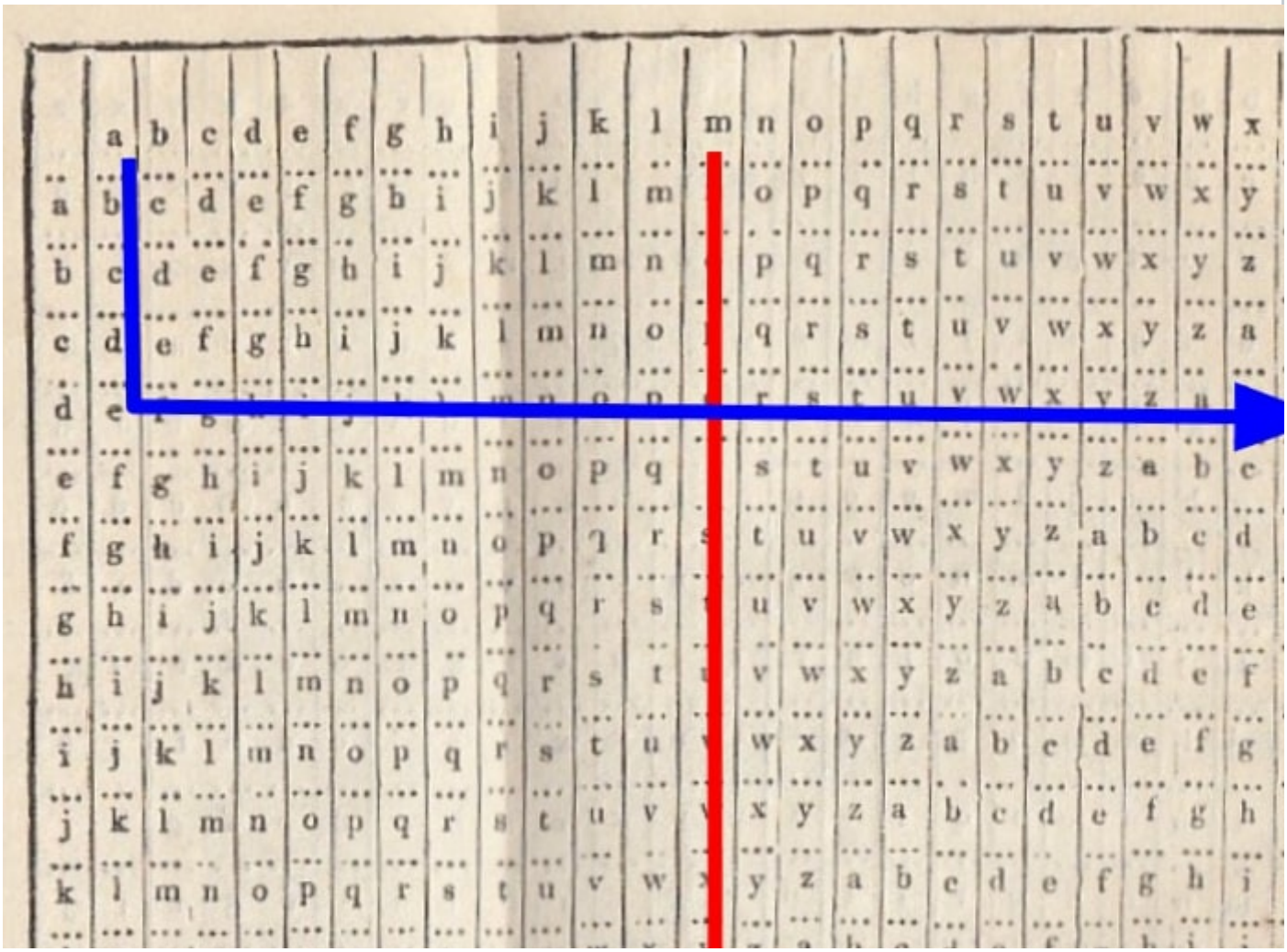
Jose Ferreira

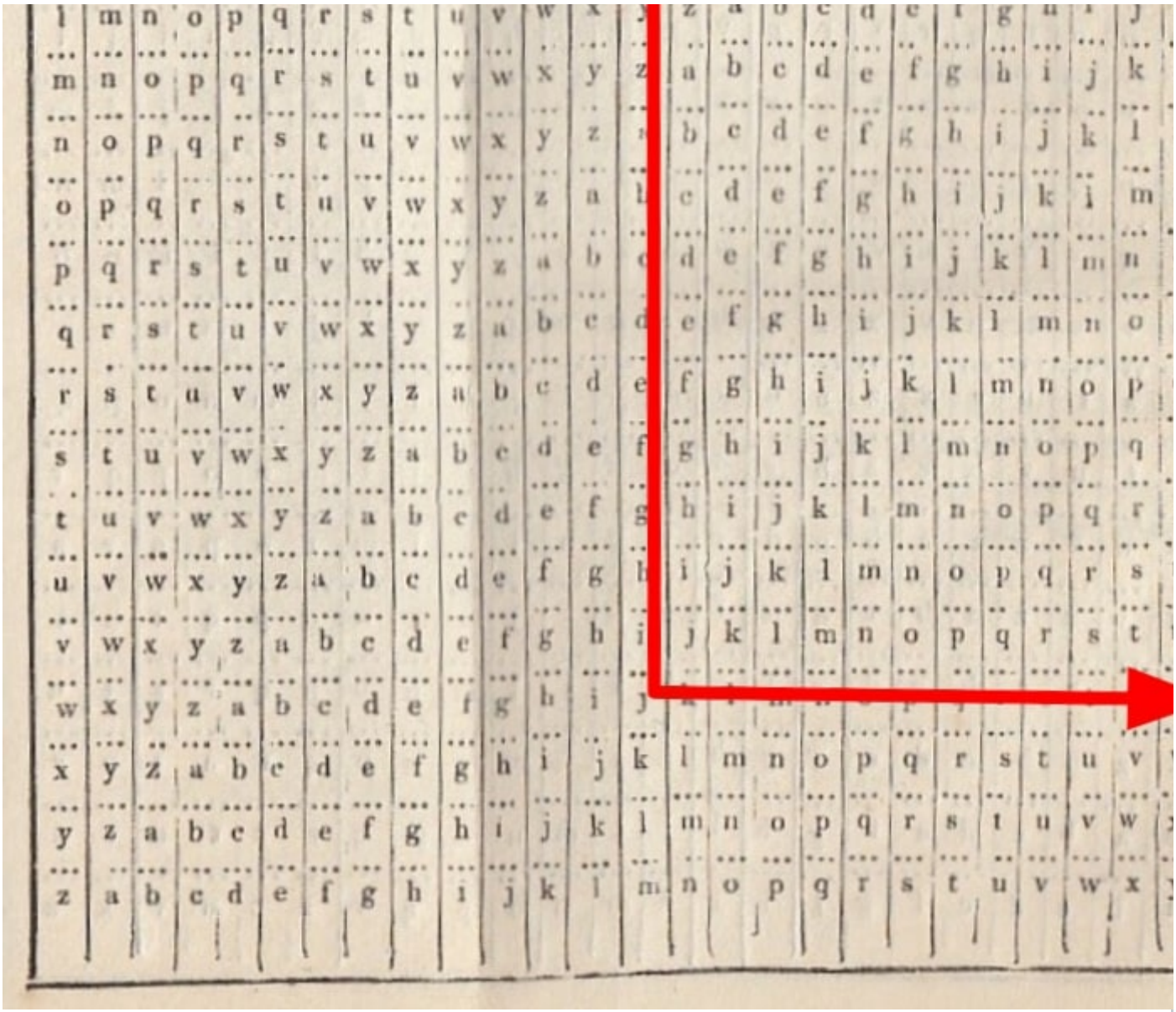
All Sections

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.



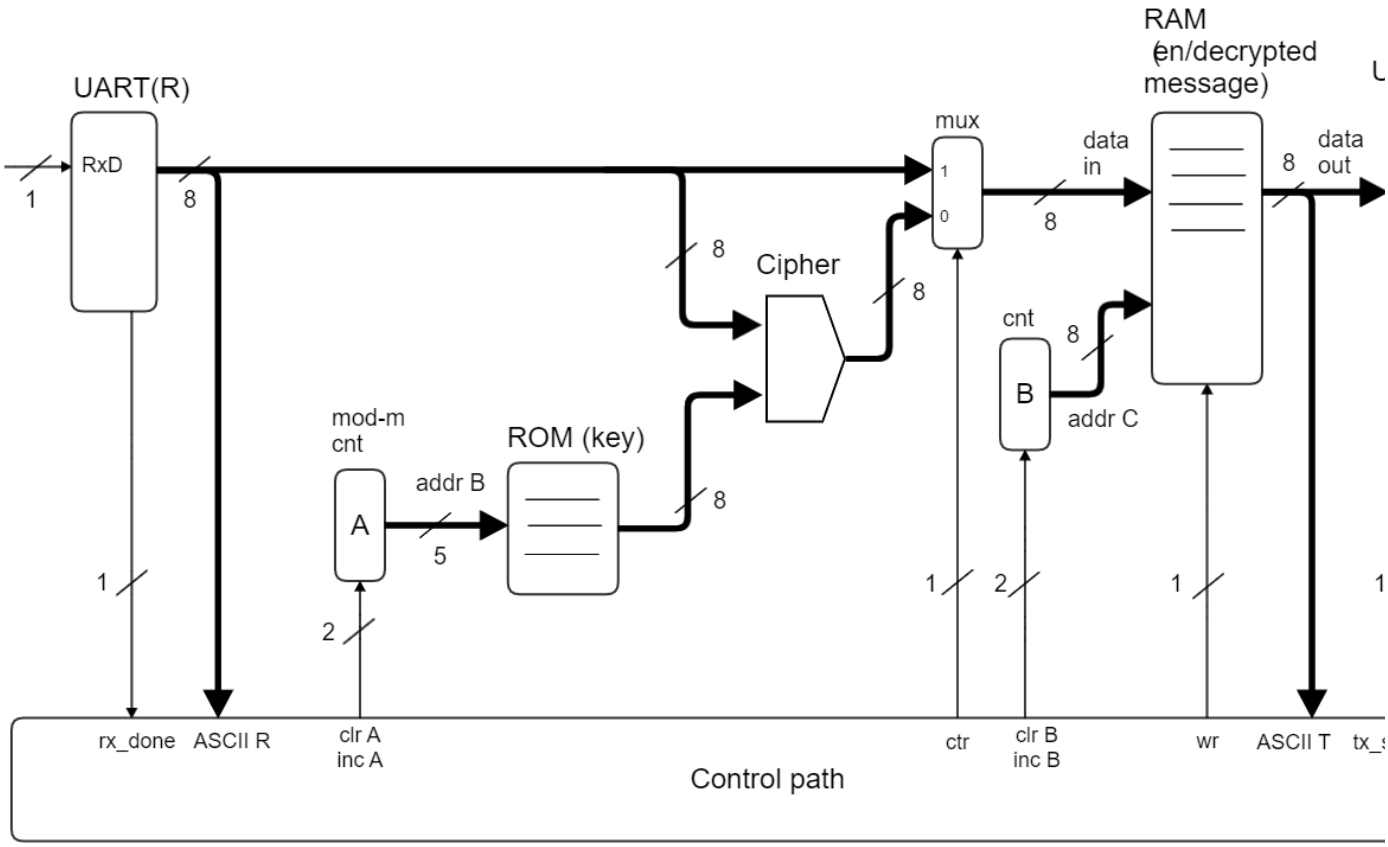


Example using the key “Jean-Jacques Rousseau”:

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

The following data path represents a draft of one possible solution, where the encryption/decryption operation is done by a (combinational) cipher block implementing a

mathematical formula, a ROM is used to store the key, and a RAM is used to store the encrypted/decrypted messages -- the full encrypted/decrypted message will be sent back to the PC when the ASCII code for the “Enter” key 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. Why are the two counters of different types (mod-m up counter for A, standard up counter for B)?
2. What factor will define the value of m? (limit of the mod-m counter)
3. What are the limitations imposed by the number of bits presented above for the two counters?
4. Present an ASMD chart that specifies the behaviour of the control path.