Assignment #1
Due: Friday, September 21, 2018 (before 16:00, to be submitted to Brightspace)

1. Chose a plaintext of at least 18 alphabetic letters and a key appropriate for the Hill cipher with $m = 3$. Demonstrate encryption, decryption, and a successful cryptanalytic attack of the form discussed in class. [4 marks]

2. Consider the rotor system shown in the figure below. Assume that the first 20 characters of a plaintext string have already been encrypted. Choose the next 10 letters of plaintext and show the output from the 3rd rotor for each of these input letters. [4 marks]

[Note: for both questions, your plaintext should be chosen independently by you. For question #1, your key should also be chosen independently by you.]

Figure 2.7 Three-Rotor Machine With Wiring Represented by Numbered Contacts