COM3190 Theory of Distributed Systems Assignment Part 1

Dean Knott

26th May 2020

1 Part A

1.1 Describe the flow of messages through the concurrent system, the possible synchronisations,and the possible sequences of messages. Identify any problems.

The messages flow through the keyboard which sends a character pressed through to the plugboard. When it reaches the plugboard, the character sent is checked to see if it is switched with another character of the alphabet and outputs that character. If the character is not switched then the output stays the same. The output is then sent to the first rotor. The first rotor then outputs a new character, depending on which rotor is used, which is then input into the second rotor. The second rotor outputs a new character, depending on what rotor is used second, which is then output to the third rotor. The third rotor takes this input and outputs a new char, depending on the rotor used third in the chain. This output is then sent through a reflector which changes the char and outputs a new char. This process is then in-versed, i.e. the chars are sent through rotor 3, rotor 2 then rotor 1. Once the process has finished the result is then presented to the user.

After each key press, the first rotor rotates, the second rotor rotates when the first rotor completes a full rotation, and the third rotor rotates when the second rotor completes a full rotation.

In the model, the keyboard sends a key press signal then an increment signal then waits for a lamp signal. This means that the rotor will increment, then this signal will be sent to the lamp which will light up the incremented character instead of the true character. This is a problem as it will output the incorrect key press which will cause inaccuracies when encoding and decoding messages.

2 Part B

2.1 Modify the model to make it a more accurate representation of the real Enigma system, and explain briefly how your version overcomes the problems you identified in (a).

To replicate the physical system, the key press signal needs to be sent through the keyboard, then the plugboard, then to the lamp to indicate which character has been pressed. This character should then be sent through the first rotor, then an increment signal is sent from the keyboard to the rotors. This means that the lamp will indicate what character has been input before the rotor increments. Doing this ensures the correct input is indicated by the lamp making the encoding and decoding process accurate.

The real system also incorporates an offset, a turnover and ring settings. The offset value effects the rotation of each rotor depending on the offset value i.e. it will shift the output value to a different character in the neighbouring rotor.
The turnover advances the rotation of the neighbouring rotors i.e. if a rotor has a turnover Q, when the Q character is passed, the neighbouring rotor is then advanced.
The ring settings rotate the wiring on a real system. If in a rotor, the A position normally encodes an A into an E, and the B position encodes B into a K, with a ring setting offset B the input A will be encoded into K.

These settings need to be produced within the rotor function to ensure they are used in the correct path and are executed at each necessary point of entry