Secure MAC Theory

The first task is to create a fixed length MAC. A fixed length MAC would take in a message of a fixed size and create a tag that would ensure that we get to know if the message is tampered with. The fixed length MAC involves computing the PRF where a key is used to randomise the message and generate a tag. This tag is used to check the sanctity of the message.
The tag is verified by computing the tag over the same message, given the same key. If the tag produced and the tag received are the same, we can be sure that the message was not tampered with. The verification process can be seen as doing the same process twice and checking if the results are the same.

The second task is to create a variable length MAC. A variable length MAC takes in a an input limited only by the block size of the message in bits. For this, the message is broken down into blocks of n/4 bits each. The final block is padded with 0s to account for remainders. Each block is appended by a random initialised bit string of size n/4, the number of blocks encoded in n/4 bits, the index of the particular block encoded in n/4 bits and the message itself. Thus it is $< r, d, i, m_i >$. Each of this string is then passed through the fixed length MAC to produce tags t_i. These tags together form $< t_1, t_2, ..., t_d >$. The random initialised bit string is appended at the beginning to complete the tag: $< r, t_1, t_2, ..., t_d >$.
This tag is also similarly verified by passing the message and the tag to the variable length MAC again, and comparing the produced tag with the given tag.