MAC then Encrypt? Or Encrypt then MAC?

When you need a system that needs both confidentiality and authentication, you need to use encryption and a MAC (Message Authentication Code). The MAC can be created by hashing an input. There are two realistic options for the order that you should perform these two actions. One is to first authenticate and then encrypt. The other is to encrypt first and then authenticate. It is more secure to use the latter option.

The first option is to authenticate then encrypt. This means that the sender computers the MAC of the plaintext, then encrypts both the plaintext and the MAC. This order of operations has one problem. This requires the receiver to decrypt the message, or at least parts of it, before the receiver can authenticate the message. This presents a vulnerability that attackers can exploit. If the attacker were able to get the ciphertext, they could alter the contents of the ciphertext to see how the receiver behaves. Since the receiver has to decrypt parts of the ciphertext before authentication, the attacker can figure out the plaintext one block at a time.

The second option is to encrypt and then authenticate. This means that the plaintext is encrypted first, then appends the MAC of the ciphertext. This way, the very first thing that the receiver does is authenticate the message. This prevents the trial and error method that would work on the previous option.

Basically, the very first thing that receiver does should always be the authenticate. Doing anything else before authenticating allows for different exploits that creative attackers could come up with.