11.5 Question 5

11.5.A S/MIME provides authentication, confidentiality, compression, and email compatibility. Which ones of the following statements about these four services are true and which ones are false? Justify.

S/MIME uses public key cryptography for content encryption in order to ensure confidentiality.

False, the key used is a symmetric key, which is only used once. For each message this key is generated from anew and encrypted with the use of the receiver's public key.

S/MIME requires that the signing is done first followed by the message encryption.

True, as can be seen on slide 25 of the lecture.

S/MIME uses X.509 public-key certificates.

True, as on slide 31 of the lecture it can be seen that S/MIME uses public-key certificates that conform to version 3 of X.509.

Lossy compression can be applied in any order with respect to the signing and message encryption operations.

False, as lossy compression leads to the need to perform the compression first and then the signing.

S/MIME provides 7-bit encoding for converting a stream of 8-bit octets to a stream of ASCII characters while some electronic mail systems accept only blocks of ASCII characters.

False, S/MIME provides the service of converting a raw 8-bit binary stream to a stream of printable ASCII characters. This service is called 7-bit encoding.