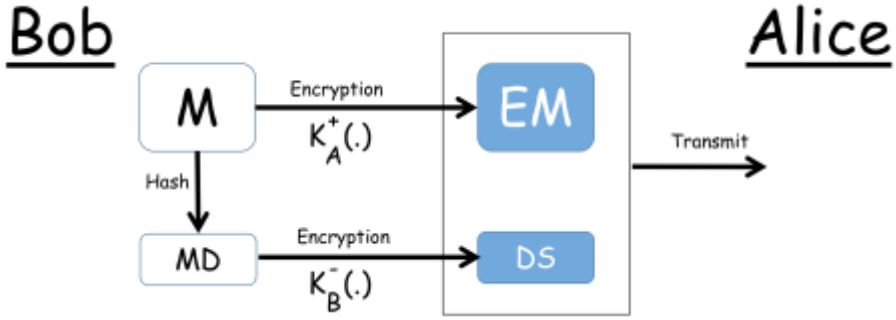
# TELE 3119: Trusted Networks
# Session 2, 2016: Quiz 2

**Question 1.** [10 points]
The following diagram depicts the Digital Signatures Concept using the public key encryption technique. The first part of the diagram is shown in which Bob sends the encrypted message and his digital signature. Complete the diagram by drawing the second part in which Alice decrypts the message and authenticates Bob as the true sender.




**M**: Original message
**EM**: Encrypted message
**MD**: Message Digest
**DS**: Digital Signature
$K_B^-$: Bob's private key
$K_A^+$: Alice's public key

**Question 2.** [10 pints]
Company xLtd has principals X, A1, A2, … , where X issues certificates for the Ai 's, and is their trust anchor. Company yLtd has principals Y, B1, B2, … , where Y issues certificates for the Bi 's, and is their trust anchor.
One day, xLtd acquires yLtd. You are to obtain a new PKI for the new xLtd. Note that parts **a** and **b** below are independent.

**a)** [5]

b-i. Modify the old PKIs to obtain a new PKI in which X is the sole trust anchor for all Ai 's, and Y is the sole trust anchor for all Bi 's; minimize the number of new certificates.

b-ii. Give the certificate chain that A1 needs to get the public key of B1 in the new PKI.

b-iii. Give the certificate chain that B1 needs to get the public key of A1 in the new PKI.

**b)** [5]

a-i. Modify the old PKIs to obtain a new PKI in which X is the sole trust anchor for all Ai 's and Bi 's; minimize the number of new certificates.

a-ii. Give the certificate chain that A1 needs to get the public key of B1 in the new PKI.

a-iii. Give the certificate chain that B1 needs to get the public key of A1 in the new PKI.