Lab 13

Q1

E_K(M_1)

Message M1 encrypted using E_K

M_1 is encrypted PU(B) and decrypted with PR(B)

It was encrypted with his public key and decrypted with his private key.

Q2

M_3 decrypted with PR(B)

The message M_3 would be decrypted with his private key

Q3

M_2 encrypted with PR(A)

She uses her private key to encrypt the message and this show she sent message.

Q4

M_2 decrypted with PU(A)

The message has to be decrypted by Alice's public key and this proves message wasn't changed by some one else.