Problem 1

Implemented services:

• Confidentiality – because any third party C does not know either B’s private key necessary to decrypt the ciphertext sent in step 1 of the protocol, or A’s private key necessary to decrypt the ciphertext in sent step 2 of the protocol. Thus, C cannot get access to the message M.

• Authentication of the Receiver – because the third party C cannot execute step 2 of the protocol (it does not know the message M, decrypted by B after step 1 of the protocol).

Not implemented services:

• Authentication of the sender – because everybody with access to the public key of B can execute step 1 of the protocol.

• Non-repudiation of the sender – because everybody with access to the public key of B could execute step 1 of the protocol.

• Non-repudiation of the receiver – because step 2 can be executed by A, without any participation of B.

Problem 2

A. Invalid MAC, because MAC(m) does not depend on message blocks $m_1..m_{N-1}$. It depends only on the number of message blocks, $N$, and the last block of the message, $m_N$.

B. Valid MAC. It depends on the entire message M and the key K. There are also no straightforward attacks against this construction.

C. Invalid MAC, because MAC(m) does not depend on message blocks $m_1..m_{N-1}$. It depends only on the number of message blocks, $N$, and the last block of the message, $m_N$. This is because $MAC(m) = f_K(m_N, IS_N)$, and $IS_{i+1}$ does not depend on $m_i$.

D. Invalid MAC, because MAC(m) does not depend on the key K.

E. Valid MAC. It depends on the entire message M and the key K. There are also no straightforward attacks against this construction.