Solutions

Mohammad Mahzoun

February 26, 2020

1 Exercise 1

Authenticity: The message is signed by A so B can verify that the message she received is indeed sent by A because in order to sign a message as A, adversary needs to forge the signature scheme.
Confidentiality: Since the messages are authenticated, in order to know the m, one has to find ek which is equivalent to breaking the security of $penc$. mac can be used to check if the message is not changed in the network.

2 Exercise 2

let $GEN() = randomBytes\ 16$

let $A\ (pk_B : pub\_key)\ (sk_A : sig\_key)\ (m : bytes) : (C : bytes) =$
let private $ek = GEN()$ in
let private $mk = GEN()$ in
let $C_1 = penc\ pk_B\ (concat\ ek\ mk)$ in
let $C_2 = sign\ sk_A\ C_1$ in
let $C_3 = sym\_enc\ ek\ m$ in
let $C_4 = mac\ mk\ C_3$ in
$concat\ C_2\ C_4$

let $B\ (pk_A : verif\_key)\ (sk_B : priv\_key)\ (C : bytes) : (m : bytes) =$
let $C_1\ C_2 = splitC$ in
if $verif\ pk_A\ C_1\ = 1$ then
let $M_1 = pke\_dec\ sk_B\ C_1$ in
let $ek\ mk = split\ M_1$ in
let $Cipher\ MAC =\ split\ C_2$ in
let $m = sym\_dec\ ekC$ in
if $mac\ Cipher\ mk = MAC$ then m

3 Exercise 3