Security Services in Multistep Protocols Exercise

Problem 1

Which of the following five security services are implemented by Protocol 1 given below? Please explain why.

Services:

C - Confidentiality

AS - Authentication of the Sender

AR - Authentication of the Receiver

NS - Non-repudiation of the Sender

NR - Non-repudiation of the Receiver

Protocol:

1. A sends to B

   (A, $E(PU_B,\ (M \| A))$, B)

2. B sends to A

   (B, $E(PU_A,\ (M \| B))$, A)

X represents a unique name of user X, where X=A or B

M means a message (the same in both transfers)

(M || X) means M concatenated with X

$E(PU_Y, Z)$ means Z encrypted using a public key of Y

Test for Security Services in a Two-Step Protocol

Confidentiality: Can C access M?

Authentication of the Sender:

Can C perform step 1 of the protocol?

Authentication of the Receiver:

Can C perform step 2 of the protocol?

Non-Repudiation of the Sender:

Can C or B perform step 1 of the protocol?

Non-Repudiation of the Receiver:

Can C or A perform step 2 of the protocol?

Answer:

C – Confidentiality	YES
AS - Authentication of the Sender	NO
AR - Authentication of the Receiver	YES
NS - Non-repudiation of the Sender	NO
NR - Non-repudiation of the Receiver	NO

Problem 2

Which of the following five security services are implemented by Protocol 1 given below? Please explain why.

Services:

C - Confidentiality

AS - Authentication of the Sender

AR - Authentication of the Receiver

NS - Non-repudiation of the Sender

NR - Non-repudiation of the Receiver

Protocol:

1. A sends to B

   A, $E(PU_B, K_{AB})$, $E(K_{AB}, M)$, $E(PR_A, M \| A)$, B

2. B sends to A

   B, $h(K_{AB} \| M \| B)$, A

X represents a unique name of user X, where X=A or B
M means a message (the same in both transfers)
(M || X) means M concatenated with X
$E(PU_Y, Z)$ means Z encrypted using a public key of Y
$E(PR_Y, Z)$ means Z encrypted using a private key of Y
$E(K_{AB}, Z)$ means Z encrypted using a secret key KAB
h(M) means a hash value of M.

Test for Security Services in a Two-Step Protocol

Confidentiality: Can C access M?

Authentication of the Sender:

Can C perform step 1 of the protocol?

Authentication of the Receiver:

Can C perform step 2 of the protocol?

Non-Repudiation of the Sender:

Can C or B perform step 1 of the protocol?

Non-Repudiation of the Receiver:

Can C or A perform step 2 of the protocol?

Answer:

C – Confidentiality	NO
AS - Authentication of the Sender	YES
AR - Authentication of the Receiver	YES
NS - Non-repudiation of the Sender	YES
NR - Non-repudiation of the Receiver	NO

Test for Security Services in a Two-Step Protocol

No Authentication of the Sender ⇒
No Non-Repudiation of the Sender

No Authentication of the Receiver ⇒
No Non-Repudiation of the Receiver

No use of private key of the Sender ⇒
No Non-Repudiation of the Sender

No use of private key of the Receiver ⇒
No Non-Repudiation of the Receiver