Homework 1

Written Assignment

due by Saturday, September 19, 11:59pm

(submission using Blackboard)

Problem 1

For the Protocols 1, 2, 3, and 4, given below, determine which of the following five security services are being implemented and which are not implemented.
In each case, explain why. Answers without justification will receive a 50% penalty.

Services:

C – Confidentiality,
AS – Authentication of the Sender,
AR – Authentication of the Receiver,
NS – Non-repudiation of the Sender, and
NR – Non-repudiation of the Receiver.

Protocol 1

1. A sends to B

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

2. B sends to A

   B, $h(M \| A \| B)$, A

Protocol 2

1. A sends to B

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

2. B sends to A

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

Protocol 3

1. A sends to B

   A, $E(PU_B, K)$, $E(K, M)$, $E(PR_A, h(M \| A))$, B

2. B sends to A

   B, $E(PR_B, K \| M \| B)$, A

Protocol 4

1. A sends to B

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

2. B sends to A

   B, $h(M \| B)$, A

Notation:
X represents a unique name of the user X, where X=A or B
M means a message
V || W means V concatenated with W
K_{AB} means a secret key shared in advance by A and B
K means a session key, generated at random as a part of a given protocol
$E(PU_Y, Z)$ means Z encrypted using a public key of Y
$E(PR_Y, Z)$ means Z encrypted using a private key of Y
E(K, Z) means Z encrypted using a secret key K

Problem 2

Demonstrate that the following constructions for Message Authentication Codes (MACs) do not fulfill the security requirements of MACs, by describing an efficient (computationally inexpensive) attack against each scheme.

The description of each attack should contain the equations for m' and $MAC_K(m')$, such that $m' \neq m$, and $MAC_K(m')$ can be calculated by an attacker without the knowledge of the secret key K, based on just one valid pair $\{m, MAC_K(m)\}$. Do your best to make m' as much different from m as allowed by the given MAC scheme.

Assume that all underlying cryptographic transformations (i.e., secret key ciphers and hash functions) are strong, i.e., they fulfill all security requirements specific to the given class of cryptographic transformations.

Notation:
$m_1, m_2, ..., m_N$ = blocks of message m
$c_1, c_2, ..., c_N, k_1, k_2, ..., k_N, X$ = intermediate variables
IV = initialization vector (a constant sent in clear in the header of the message)
K = a key known only to the sender and receiver
$E_K(X)$ = encryption of X with the key K
h(y) = hash value of the message y
|| represents concatenation; $\oplus$ represents an XOR operation
for i=1..N means for each integer i between 1 and N

a) $X = h(m_1 \oplus m_2 \oplus m_3 \oplus \ldots \oplus m_N)$
   $MAC_K(m) = E_K(X)$

b) $MAC_K(m) = E_K(h(m_1 \oplus m_2)) \oplus E_K(h(m_3 \oplus m_4)) \oplus \ldots \oplus E_K(h(m_{N-1} \oplus m_N))$
   Assume that N is an even integer.

c) $MAC_K(m) = E_K(h(m_1||m_2) \oplus h(m_2||m_3) \oplus h(m_3||m_4) \oplus \ldots \oplus h(m_{N-1}||m_N) \oplus h(m_N||m_1))$

d) $k_i = E_K(IV+i-1)$ for i=1..N
$c_i = m_i \oplus k_i \oplus i$ for i=1..N
$MAC_K(m) = h(c_1 \oplus c_2 \oplus \ldots \oplus c_{N/2}) \,||\, h(c_{N/2+1} \oplus c_{N/2+2} \oplus \ldots \oplus c_N)$
Assume that N is an even integer.

e) $c_0 = IV$
$c_i = m_i \oplus k_i \oplus i$ for i=1..N
$k_i = E_K(c_{i-1})$ for i=1..N
$MAC_K(m) = c_1 \oplus c_2 \oplus \ldots \oplus c_N$

Recommended Reading Assignment
(including material covered during the next lecture)

W. Stallings, *Cryptography and Network Security: Principles and Practice*,

8th edition:

- Chapter 15 Cryptographic Key Management and Distribution

or

7th edition:

- Chapter 14 Key Management and Distribution.