Master M2 Cybersecurity
Course : Cryptographic Engineering
Cristian Ene's part

January, 2025
Duration 45 minutes

Problem 1 (4.0 pts.)

In this exercise, $\langle \_, \_ \rangle$ represents concatenation, $[\ \_\ ]_{\_}$ represents a symmetric encryption scheme, $\{\ \_\ \}_{\_}$ an asymmetric encryption scheme, $pr(u)$ is the inverse secret key associated to $pk(u)$ and $\oplus$ denotes the usual bitwise xor over equal-length bitstrings, e.g. $0011 \oplus 1110 = 1101$. Consider the following protocol:

$$\begin{array}{llcll}
1. & A & \rightarrow & B & : \{\ \langle \langle A, B \rangle, N_a \rangle\ \}_{pk(B)} \\
2. & B & \rightarrow & A & : \langle \{\ \langle K, N_b \rangle\ \}_{pk(A)}, [\ N_a \oplus B\ ]_K \rangle \\
3. & A & \rightarrow & B & : \{\ \langle \langle A, N_b \rangle, K \rangle\ \}_{pk(B)}
\end{array}$$

The goal of this protocol is to provide both secrecy and authentication: at the end of a session between two honest participants a and b, k **(the instantiation of the variable K in the specification of the protocol) should be a new shared secret value known only by a and b.** This target session between honest participants a and b may be part of a richer scenario containing other running sessions in parallel where the active adversary i can be involved.

1. Describe in details (as a list) A's and B's actions at receipt of messages 2 and 3 and what beliefs they have at that stage.
2. Show **(using the McAllester's Algorithm)** that k (the instantiation of the variable K in the specification of the protocol) remains secret in presence of a passive Dolev-Yao intruder.
3. What do you think about the correctness of the protocol in presence of an active Dolev-Yao intruder? If you think that the protocol is correct, then give a justification. Otherwise,
   - give an attack on the target session between honest participants a and b where the intruder i will learn k;
   - propose a correction of the protocol.

Problem 2 (2.0 pts.)

In this exercise, $\langle \_, \_ \rangle$ represents concatenation, $\{\ \_\ \}_{\_}$ represents an asymmetric encryption scheme, and $pk(u)$ is the public key associated to the user with identity u. All protocols in this exercise are intended to provide acknowledgement of the receipt of an encrypted message m by the intended receiver b, i.e. at the end of a session between honest participants a and b, a will think that she is talking to b and she is sharing a secret value m with b. For all following protocols, you should consider a target session between honest (uncorrupted) participants a and b, part of a richer scenario containing maybe other running sessions, and check if m (the instantiation of variable M in this session) remains secret in presence of an active Dolev-Yao intruder. For all protocols below, if you think that the protocol is not correct, give an attack on the target session between honest participants a and b where the intruder i will learn m (maybe using other sessions running in parallel where i can be involved), but if you think that the protocol is correct, then give a justification.

1. We start with a naive protocol:

$$\begin{array}{llcll}
1. & A & \rightarrow & B & : \langle A, \{\ M\ \}_{pk(B)} \rangle \\
2. & B & \rightarrow & A & : \{\ M\ \}_{pk(A)}
\end{array}$$

2. A more "elaborate" protocol:

$$\begin{array}{llcll}
1. & A & \rightarrow & B & : \{\ \langle A, M \rangle\ \}_{pk(B)} \\
2. & B & \rightarrow & A & : \{\ M\ \}_{pk(A)}
\end{array}$$

3. And a “very encrypted” protocol:

$$\begin{array}{lcccl} 1. & A & \rightarrow & B & : \{\, \langle A, \{\, M \,\}_{pk(B)} \rangle \,\}_{pk(B)} \\ 2. & B & \rightarrow & A & : \{\, M \,\}_{pk(A)} \end{array}$$