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

January, 2024
Duration 45 minutes

Maximum number of points that can be obtained for this part is 5 (your grade is calculated as min(ex1 + ex2, 5)). Hence you do not need to succesfully answer to all questions to reach the maximal grade.

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:

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

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, $|\cdot|$ denotes the length of a bitstring, $\overline{x}$ is the bitwise complement of x (e.g. $\overline{1101} = 0010$) and $\oplus$ denotes the usual bitwise xor over equal-length bitstrings, e.g. $0011 \oplus 1110 = 1101$. A one-way function is a function that is easy to compute but hard to invert. Formally, $f : \{0,1\}^* \mapsto \{0,1\}^*$ is a one-way function, if for all probabilistic polynomial-time families of adversaries $\mathcal{A}$ the following probability:

$$p(k) \stackrel{def}{=} Pr_{b \stackrel{R}{\leftarrow} [x \stackrel{R}{\leftarrow} \{0,1\}^k;\ y \leftarrow f(x);\ x' \stackrel{R}{\leftarrow} \mathcal{A}(y)\ :\ \text{return}\ \ f(x') = y]}(b = true)$$

(simpler written $p(k) \stackrel{def}{=} Pr[f(x') = y \mid x \stackrel{R}{\leftarrow} \{0,1\}^k;\ y \leftarrow f(x);\ x' \stackrel{R}{\leftarrow} \mathcal{A}(y)]$)
is a negligible function in k. That is, the probability that a probabilistic polynomial-time algorithm $\mathcal{A}$ is able to find a preimage x' for a given image $y = f(x)$ of an uniformly sampled x is negligible. In this exercise, we assume the existence of at least one such one-way function denoted by f_0.

For each of the assertions below, prove or disprove that they are valid for arbitrary one-way functions f and g (we assume that $\forall x \in \{0,1\}^*$, $|f(x)| = |g(x)|$). That is, if the assertion is valid give a proof by reduction. If it is not, give a counterexample of one-way functions f and g such that the obtained function is not a one-way function.

1. Let $CXor(f) : \{0,1\}^* \mapsto \{0,1\}^*$ be the function defined by $CXor(f)(x) = \overline{f(x)}$, i.e. $CXor(f)$ is the function that applies the function f to the argument and then computes the bitwise complement of the result.
   If f is a one-way function then $CXor(f)$ is also a one-way function.

2. Let $BXor(f,g) : \{0,1\}^* \mapsto \{0,1\}^*$ be the function defined by $BXor(f,g) = f(x) \oplus \overline{g(x)}$.
   If f and g are one-way functions then $BXor(f,g)$ is also a one-way function.