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

January, 2023
Duration 50 minutes

Maximum number of points that can be obtained is 5.5.

Problem 1 (2.0 pts.)

In this exercise, $\langle \_, \_ \rangle$ represents concatenation, $[\![\_]\!]_\_$ represents a symmetric encryption scheme, $sign\_\{ \_ \}$ a digital signature, $pr(u)$ is the inverse secret key associated to $pk(u)$. Consider the following protocol:

$$\begin{array}{llll} 1. & A & \rightarrow & B \quad : g^X \ mod \ p \\ 2. & B & \rightarrow & A \quad : \langle g^Y \ mod \ p, \quad [\![\ sign_{pr(B)}\{ \ \langle g^Y \ mod \ p, g^X \ mod \ p \rangle \ \} \ ]\!]_{(g^{XY} \ mod \ p)} \rangle \\ 3. & A & \rightarrow & B \quad : [\![\ sign_{pr(A)}\{ \ \langle g^X \ mod \ p, \ g^Y \ mod \ p \rangle \ \} \ ]\!]_{(g^{XY} \ mod \ p)} \end{array}$$

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, $k = g^{xy} \ mod \ p$ 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.

We assume that the parties have agreed on a $(g; p)$ pair for Diffie-Hellman key exchange, that each user has keys for digital signatures and that they have agreed on a symmetric encryption scheme for use in subsequent encryption. Furthermore, $[\![\ m \ ]\!]_{sk}$ denotes the (symmetric) encryption of a message m using the key sk and $sign_{pr(A)}\{ \_ \}$ and $sign_{pr(B)}\{ \_ \}$ denote A's and B's signature operations, respectively. 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. Are A and B successfully authenticated to each other after a protocol session ?

Problem 2 (2.0 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:

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

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. 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 3 (1.5 pts.)

1. What risks arise when using the same key to encrypt both directions of a communication channel, that aren't present if using different keys for the different directions?
   (a) Message tampering by flipping bits in the ciphertext.
   (b) Reflection attacks.
   (c) Hash collisions.

(d) Eavesdropping attacks.

(e) Denial-of-service.

(f) None of the above.

2. Which of the following properties must a cryptographic hash function provide?

   (a) Key revocation.

   (b) Collision resistance.

   (c) A deterministic mapping from input to output.

   (d) One-to-one mapping of input to output.

   (e) Difficulty of finding an input that matches a given hash.

   (f) None of the above.

3. Which of the following equations/properties must a cryptographic hash function h provide in a Tamarin encoding?

   (a) $x1 = x2 \Rightarrow h(x1) = h(x2)$.

   (b) $h(x1) = h(x2) \Rightarrow x1 = x2$.

   (c) $h(x, y) = h(y, x)$.

   (d) No equation at all.

   (e) None of the above.