Coursework 1 - Exercise 6

November 9, 2023

a) Given are two protocols in which the sender's party performs the following operation:

Protocol A:

$$c = \text{Enc}(k_1, H(k_2||x||\sigma_{pr}(x)))$$

where x is the message, H is a hash function, Enc is a symmetric-key encryption function, $||$ denotes simple concatenation, and k_1, k_2 are secret keys which are only known to the sender and the receiver.

Protocol B:

$$c = \text{Enc}(k_1, x||\sigma_{pr}(x))$$

where k is a shared key, pr is the private key of the receiver, and σ_{pr} denotes a digital signature using the key pr. Provide a step-by-step description (e.g. an itemized list) of what the receiver does upon reception of c for each protocol.

b) State whether the following security properties are fulfilled for each protocol given in the previous question:

- confidentiality
- integrity
- non-repudiation

(To get full marks, you need to justify your answer. A Yes/No answer will not be considered for marking)

Protocol A:

1. User receiver decrypts the message using the following equation:

$$d = \text{Dec}(k_1, c) = H(k_2||x||\sigma_{pr}(x))$$

2. User is now stuck and wont be able to retrieve the message since hash functions are not reversable

Protocol B:

1. User receiver decrypts the message with the following equation:

$$d = \text{Dec}(k_1, c) = x||\sigma_{pr}(x)$$

2. To obtain the original message x, the user deconcatenates d as follows:

$$x = \text{deconcatenate}(d) = \boxed{x}||\sigma_{pr}(x)$$

b)

We first go over the definition of the properties:

- **Confidentiality**: Information is available for reading only to authorized members.
- **Integrity**: Detect if data was modified from the source to the destination.
- **Non-repudiation**: Sender cannot claim she did not send the message

	Confidentiality	Integrity	Non-repudiation
Protocol A	Yes, since the key k_1 is needed to decrypt the message	Yes, since message is encrypted, if the message was modified, decryption wouldn't be possible	No, since sign is lost to hash
Protocol B	Yes, since the key k_1 is needed to decrypt the message	Yes, since message is encrypted	No, since sender did not sign the message