Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UNIVERSIDAD CARLOS III DE MADRID |

PRESENTATION PART 3

The third part studies mechanisms to provide message integrity and authentication, and also includes four modules.

- In Module 9, hash functions are studied. Hash functions take as input a message of any length and provide as output a digest of a fixed length. The digest represents and characterizes the input message. The module first defines the concept of hash functions and the properties this type of functions must satisfy. This is followed by the introduction of the Merkle-Damgard structure, used by many hash functions, and the main features and current status of the MD5, SHA-2, and SHA-3 hash functions.

- In Module 10, message authentication codes (a.k.a., MAC) are studied. These functions compute an authentication tag for a message taking as additional input a secret key shared among the parties. The tag is attached to the message, and it allows the receiver to authenticate the sender of a message and verify that the message has not been altered. The module explains the general model of this type of mechanisms and the properties they must satisfy. The two main types of MAC are introduced next: those based on hash functions, explaining in detail the HMAC algorithm, and those based on block ciphers. Finally, the main characteristics of authenticated encryption are studied, which allows to encrypt several blocks of data and generate an authentication tag for the message.

- In Module 11, digital signature schemes are studied. This type of mechanism uses public key cryptography to generate a digital signature for a message. The signature allows to authenticate the signer and verify that the message has not been altered, as well as preventing the signer from denying having generated the signature. To generate a signature, the signer uses his private key, and the receiver uses the signer's public key to verify the signature. The module first defines digital signature schemes, their properties and the different types that exist. Later, the RSA and El Gamal signature algorithms are detailed.

- In Module 12, public key infrastructures (a.k.a., PKI) are studied. PKIs are a set of entities, services and protocols that allow to authenticate the owner of a certain public key using public key certificates, and provide mechanisms to manage their life cycle.

Associated material

The material associated with this topic includes lecture notes slides and a collection of proposed exercises on the aspects covered in these modules with their solution. In addition, a set of objective answer quizzes are offered, with solutions, which allow students to verify their learning in these modules.