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 2

The second part studies the mechanisms to provide message confidentiality, also including four modules.

- In Module 5, symmetric block ciphers are studied. Symmetric cryptosystems allow a message to be encrypted and decrypted, using the same key for both operations. This key must be known by both the sender and the receiver of the message. Block ciphers allow you to encrypt a block of data of a certain size each time by mixing it with the key. This module illustrates the Feistel scheme, a typical structure for symmetric block cryptosystems, and then the operation modes that can be used if multiple blocks need to be encrypted. The DES and AES algorithms are studied in detail next.

- In Module 6, stream symmetric ciphers are studied. These ciphers allow to encrypt and decrypt a series of data elements of a small length compared to the length of blocks processed by symmetric block ciphers. From the symmetric key shared between the sender and receiver of the message, a keystream is derived with elements of similar length to those of the data stream to be encrypted. This module first defines the model of this type of cryptosystems and then the concept of keystream. Next, pseudo-random bit generators used to generate keystreams are studied, specifically those based on linear feedback shift registers. Finally, the RC4 algorithm is briefly studied.

- In Module 7, asymmetric cryptosystems are studied. This module introduces one of the major milestones of modern cryptography, asymmetric or public key cryptography. In this case, two communicating parties do not share the same key to encrypt and decrypt the messages, but rather each party has a pair of keys called public and private key. The public key is made public and therefore it is assumed that everyone knows it. The private one is kept private, only known by its owner. The receiver's public key is used to encrypt a message. Only the receiver will be able to decrypt the message with his private key. These types of algorithms are based on trapdoor one-way functions, that is, calculating the private key is very difficult if only the public one is known. In this module, in addition to defining the asymmetric cryptosystem model, the RSA and El Gamal encryption algorithms are studied in detail.

- In Module 8, key distribution and establishment is studied. The previous modules assume that both parties share a secret key or know the receiver’s public key in advance. This situation does not have to occur in all cases, so it is necessary to introduce mechanisms that allow key distribution and establishment, such that guarantees are provided about who knows the shared keys or who owns them. This module introduces the basic mechanisms to distribute symmetric keys using symmetric cryptosystems, symmetric keys using asymmetric cryptosystems (better known as hybrid cryptosystems), public keys using asymmetric cryptosystems, and finally, the Diffie-Hellman key exchange algorithm is studied in detail.

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.