

Tema 5: Seguridad en redes

Sesión A13: Seguridad en redes. Criptografía de clave simétrica

Lectura previa:

- Kurose2010 secciones 1.6, 8.1, 8.2-intro y 8.2.1

Conceptos:

- Seguridad en la red [8.1]
 - Ataques a las redes [1.6]
 - Propiedades en una comunicación segura
 - Confidencialidad
 - Autenticación del punto terminal
 - Integridad del mensaje
 - Seguridad operacional
- Principios de criptografía [8.2]
 - Conceptos de texto claro, texto cifrado y algoritmo de cifrado
- Criptografía de clave simétrica [8.2.1]
 - Cifrado de César
 - Cifrado monoalfabético y polialfabético
 - Cifrado de bloque
 - Encadenamiento de bloques cifrados
 - Vector de inicialización

Sesión A14:

Criptografía de clave pública. Integridad de los mensajes. Firma digital. Autenticación. Conexiones TCP seguras

Lectura previa:

- Kurose2010, secciones 8.2.2, 8.3 y 8.5

Conceptos:

- Criptografía de clave pública [8.2.2]
 - Funcionamiento
 - RSA
 - Clave de sesión
- Integridad de los mensajes [8.3 - intro]
 - Funciones hash criptográficas [8.3.1]
 - Código de autenticación del mensaje [8.3.2]
 - Firmas digitales [8.3.3]
 - Certificación de clave pública
 - Autoridad de certificación
 - Autenticación del punto terminal [8.3.4]
 - Ataques por reproducción y números distintivo
- Capa SSL [8.5]
- Panorámica general [8.5.1]
 - Fase de acuerdo
 - Deducción de las claves
 - Transferencia de datos
 - Registro SSL
- Algún detalle más [8.5.2]
 - Fase de acuerdo
 - Cierre de la conexión

