Universidad de Alcalá

Nombre:

Fecha: 9 de mayo de 2012

DEPARTAMENTO DE AUTOMÁTICA
ARQUITECTURA Y TECNOLOGÍA DE COMPUTADORES

Grado en Ingeniería Informática

REDES DE COMPUTADORES

Prueba de bloque 4, grupo tarde

- **Cada afirmación correctamente contestada vale 0,05 puntos y cada fallo descuenta 0,025.**
- **El problema debe resolverse en el espacio reservado para ello y vale 0,25 puntos.**

1. Marque cada una de las siguientes afirmaciones como verdadera (V) o falsa (F):

   a) Si dos usuarios comparten la clave secreta k_s, y uno le envía al otro un mensaje m, junto con $H(m||k_s)$, donde H es una función resumen, entonces se puede garantizar la autenticación pero no la integridad de los datos.

   V, F.

   b) La técnica CBC se emplea en los cifradores de flujo para proteger mejor los datos cifrados.

   V, F.

   c) El uso de un MAC garantiza total protección frente a los ataques por repetición.

   V, F.

   d) El correcto funcionamiento de IPsec exige que los routers frontera compartan una clave secreta.

   V, F.

   e) El sistema de correo electrónico seguro PGP utiliza la infraestructura de clave pública.

   V, F.

2. Supongamos que Alicia y Benito han iniciado una sesión SSL y están intercambiando paquetes de datos. Eva (el enemigo) introduce un paquete falso para Benito, fabricado en tal manera que todos los datos de la cabecera TCP e IP (direcciones, longitudes, números de puerto, etc.) son correctas.

   a) ¿Aceptará Benito ese paquete? Justificar la respuesta.

   b) Indicar si es posible que Eva pueda llegar a añadir un paquete falso con éxito y cómo lo haría.