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 mañana

- **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. Contestar las siguientes cuestiones marcando V (verdadero) o F (falso):

   a) En un sistema de clave secreta con n usuarios, hacen falta $O(n)$ mensajes para distribuir a todos los usuarios una clave nueva.
   Nota: $O(n)$ significa «del orden de n».

   V, F.

   b) Los sistemas de clave pública no son susceptibles de recibir ataques al texto en claro elegido.

   V, F.

   c) La propiedad de resistencia a colisiones de una *función resumen* significa que no existen dos mensajes que vayan a parar al mismo resumen.

   V, F.

   d) En IPsec, la base de datos SAD indica qué sistema criptográfico se ha de usar para cada conexión IPsec activa.

   V, F.

   e) Los *sistemas cortafuegos* regulan el tráfico mediante listas de reglas de acceso.

   V, F.

2. Supongamos un sistema RSA con los siguientes parámetros públicos: $n = 77$, $e = 11$. Eva está espiando y consigue capturar el criptograma $c = 51$, cifrado con esa clave pública.

   a) Tratar de vulnerar el sistema y obtener el mensaje en claro, *m*, correspondiente a *c*.

   b) ¿Cuál es el exponente de descifrado *d*?

   Nota: Se puede usar la calculadora, pero hay que consignar todos los pasos realizados: no vale dar solo los resultados finales de las operaciones.