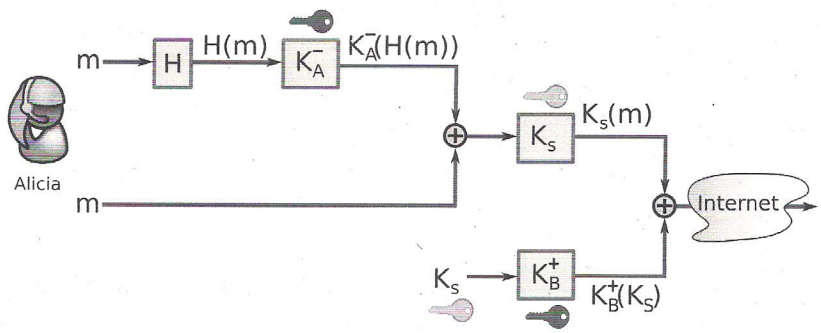
Redes de comunicaciones 2

5 de mayo de 2014

Nombre: _____ Apellidos: _____

Preguntas	1	2	3	Total
Puntos	40	40	20	100
Puntuación				

1. Dado el siguiente esquema de transmisión desde Alice hacia Bob, donde H es una función de hash, K_A^- es la clave privada de Alice, K_s es una clave simétrica y K_B^+ es la clave pública de Bob. [40]



A. Dibuje y explique el diagrama de bloque del procedimiento que debe utilizar Bob para leer el mensaje

B. Explique razonadamente qué propiedades de la seguridad de la información están soportadas por el esquema

2. Trudy está intentando leer los mensajes que intercambian Alice y Bob. Sabe que Alice y Bob están utilizando para codificar los mensajes que intercambian cifrado por bloques, con bloques de 3 bits. Además, ha logrado descubrir el texto en claro de un mensaje que ha interceptado: [40]

   Mensaje interceptado = 111010111001001110000110100010001001011000011110
   Texto en claro: 'Alicia'

   Con este conocimiento, logra interceptar y decodificar el siguiente mensaje: 111110010001011000011110.

   Reproduzca el razonamiento de Trudy y descubra el significado del segundo mensaje interceptado.

3. Necesitamos el numero de paquetes recibidos por UDP en un nodo que se administra utilizando SNMP. [20]

   A. ¿Cómo es el identificador ANS.1 para esta petición?

   B. ¿Qué mensaje SNMP tenemos que mandar para obtener estos datos?

   C. ¿Qué mensaje SNMP vamos a recibir como respuesta a esta petición?