3° Certamen Tiempo 90 min.

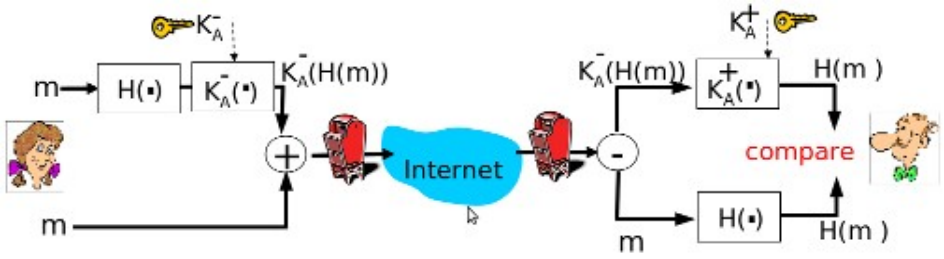
Cada pregunta tiene igual puntaje.

Escriba sus respuesta en forma clara y precisa.

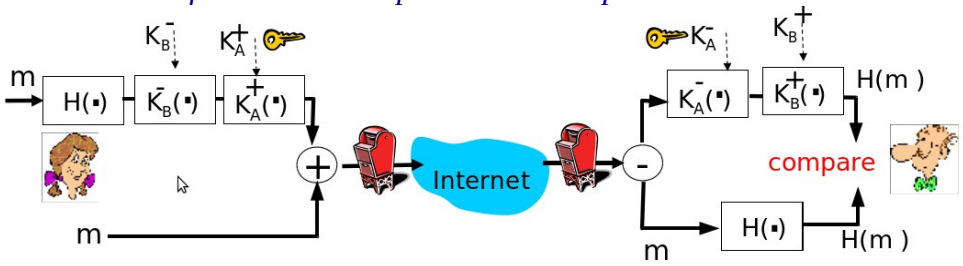
1.- Explique los siguientes conceptos: confidencialidad, autenticación, e integridad.
En el contexto de seguridad en redes de computadores tenemos:
Confidencialidad: El contenido del mensaje solo puede ser visto por el destinatario del mensaje.
Autenticación: La identidad del transmisor y receptor puede ser confirmadas. En mensajes debe ser verificable que el creador del mensaje es quien dice ser.
Integridad: Cualquier cambio o alteración del mensaje debe ser detectada por el receptor.

Nota en contexto de seguridad, la integridad procura detectar si el mensaje fue alterado por un atacante.

2.- Explique en qué consiste la no repudiación de un mensaje y describa un mecanismos eficiente que permita conseguirla.
La no repudiación consiste en que el transmisor no puede negar que el mensaje recibido fue generado por él.
Basta que el transmisor firme el mensaje, por ejemplo, cifrando un resumen del mensaje, H(m), con su clave privada K_A^- y adjuntarlo al mensaje.



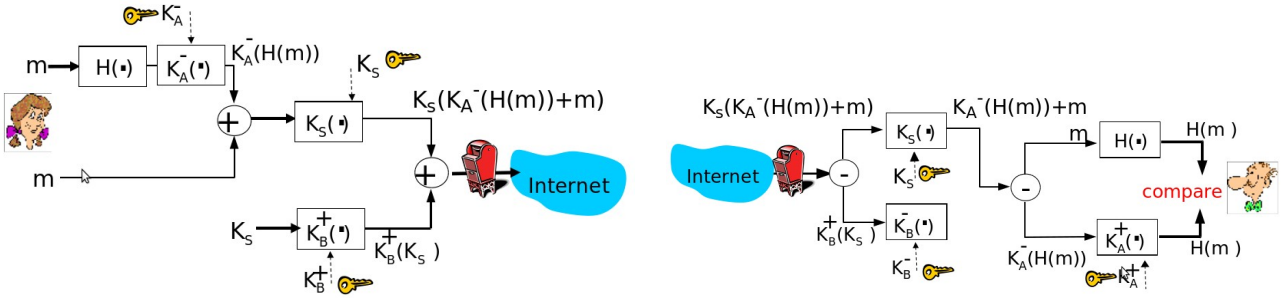
3.- Se desea enviar un mensaje de manera que el receptor sea el único que pueda verificar su integridad. Muestre un esquema **eficiente** para lograr este propósito en el lado del transmisor y receptor.
Nota: Use bloques rotulados para señalar las operaciones; por ejemplo, un bloque con H(.) indica obtención de función hash (o resumen).
Un esquema eficiente es aquel similar al previo pero en lugar de cifrar el resumen con la clave privada del transmisor se cifra con la clave pública del receptor.



Nota: Rx es el único que puede verificar integridad, luego el hash debe ir encriptado por su clave pública. Para asegurar integridad, el mensaje debe ir además firmado, pues de otra manera

cualquiera podría crear un mensaje y encriptar el hash con la clave pública del destinatario consiguiendo así alternar el mensaje que va en texto plano.

4.- Se desea enviar un mensaje confidencial de forma que no pueda ser repudiado. ¿Qué esquema sugeriría para cifrar el mensaje y luego para descifrarlo?
A diferencia de la pregunta 2, esta vez el mensaje debe ser además confidencial. En mensaje debe ser encriptado con un secreto compartido el cual es enviado usado la clave privada del transmisor. Hay varios esquemas que permiten satisfacer este requerimiento, una solución es:



Nota existen sistemas más simples pero menos eficientes, por ejemplo encriptando todo con la clave privada del Tx y luego con la clave pública del Rx.

5.- Dé un ejemplo del problema que dio origen a las Autoridades Certificadoras. Explique cómo su problema se resuelve con la existencia de Autoridades Certificadoras.
Puedo encargar un libro o una pizza y junto con el encargo enviar mi clave pública para que descifren el mensaje. El problema aparece por que cualquiera puede enviar tal mensaje y pretender ser Agustín González.
Para evitar tal problema, el receptor de una clave pública debe poder validar que esa clave pública en efecto pertenece a quien dice ser. Para esto se han creado Autoridades Certificadoras (AC) las cuales registran las claves públicas de los interesados. Estas AC entregan un certificado, que incluye los datos del dueño y su clave pública, firmado con la clave privada de la AC.
Así el receptor del encargo del libro o pizza puede usar la clave pública de la AC para verificar que en efecto esa es la calve pública pertenece a quien hace la compra.

6.- Dé un ejemplo del problema que dio origen al uso de **números únicos**. Muestre cómo el número único resuelve el problema.
Un intruso puede grabar una copia del mensaje en que Agustín encarga un libro o una pizza. Al día siguiente, el intruso puede enviar nuevamente en mensaje y hacer creer al negocio que Agustín desea otro libro o pizza.
El número único evita el problema previo, pues al comprar un libro o pizza, primero el negocio hace llegar un número único a Agustín. Éste incluye tal número en la firma del mensaje. El negocio puede verificar así la unicidad del mensaje.
Con esta técnica el intruso no podrá repetir en el mensaje, pues el negocio verá que el número único no corresponde con la sesión del intruso y rechazará así el mensaje.

7.- Explique por qué el método de cifrado de bloques en cadena no puede ser usado para encriptar paquetes capa 2 en redes inalámbricas.
No se puede usar pues se espera que algunos paquetes de la capa 2 se pierdan y por lo tanto al usar cifrado de bloques en cadena no sería posible descifrar los paquetes restantes.

8.- Mencione una ventaja de los Sistemas de Detección de Intrusión respecto a los cortafuegos. Mencione una ventaja de los cortafuegos respecto a los Sistemas de Detección de Intrusión.

Ventaja de IDS respecto a cortafuegos: Los IDS monitorean el tráfico tomando copia de todo los paquetes y por lo tanto no aumentan los tiempo de procesamiento de cada paquete como sí lo hacen los cortafuegos.

Ventaja de cortafuegos respecto a los IDS: El cortafuego evita la ocurrencia de situaciones indeseadas, el IDS las detecta y la acción evasiva es de responsabilidad de otra parte del sistema.