3° Certamen Tiempo 90 min.

Cada pregunta tiene igual puntaje.

1. ¿En qué consiste la encriptación mono-alfabética? Mencione dos estrategias para descubrir el diccionario mono-alfabético.

La encriptción mono-alfabética consiste en reemplazar cada símbolo del mensaje por su símbolo correspondiente en el diccionario. Es mono-alfabética cuando usamos un único diccionario para cada símbolo del mensaje.

Una estrategia para descubrir el diccionario es estudiando la estadística de los símbolos en varios mensajes. Como se conoce la estadística de los símbolos en determinado lenguaje, se puede obtener el diccionario usado.

Otra estrategia es estudiar mensajes codificados cuyo contenido es conocido o sospechable; por ejemplo, el protocolo para acceder a un servidor web es conocido por ello se puede anticipar el contenido de algunos mensajes. Al ver su versión encriptada se puede obtener el alfabeto.

2. Un ingeniero dice: “La confidencialidad es la propiedad de las comunicaciones donde sólo el emisor y receptor esperado pueden acceder al contenido del mensaje”.
¿Está usted de acuerdo?

Sí estoy de acuerdo.

Si el mensaje fuera alterado en su tránsito ¿Sigue siendo confidencial? Explique.

Sí sigue siendo confidencial. La confidencialidad se pierde cuando el contenido llega a manos no deseadas, pero no se pierde si por dañarse el receptor no lo puede acceder.

¿Es posible tener confidencialidad y no integridad? Explique.

Sí. el contenido es alterado, se perderá la integridad, pero no la confidencialidad pues el atacante no pudo acceder al contenido.

¿Es posible tener integridad en un mensaje y no confidencialidad? Explique.

Sí, el mecanismo de firma digital es un ejemplo. Se consigue integridad pero no es confidencial.

3. Las entidades certificadoras emiten certificados firmados con su clave privada, así podemos saber si la clave pública de un servidor, por ejemplo, corresponde realmente a ese servidor. Pero ¿cómo sabe la aplicación cuál es la clave pública de la entidad certificadora?

Ésta viene integrada al software que usamos para acceder a esos servicios.

¿Por qué al conectarse desde un computador nuevo a aragorn vía ssh, éste envía un mensaje de advertencia?

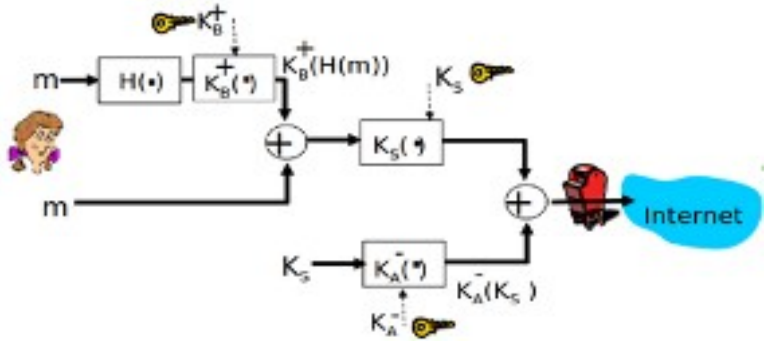
Porque aragorn envía su clave pública y nuestro cliente no tiene cómo verificar que es la correcta. Cuando el usuario indica que sí es la correcta, el cliente ssh la guarda como válida y no vuelve a consultar al usuario hasta que algo cambie en el servidor (MAC, versión de S.O, etc)

4. ¿Por qué el encriptar con clave privada el hash de un mensaje es más conveniente como firma digital que encriptar todo el mensaje con la clave privada?.

Porque el tiempo tomado para calcular la función hash y luego encriptarla con la clave privada es menor que encriptar todo el mensaje con la clave privada. La firma digital busca proveer autenticación

de la fuente, luego es mejor no encriptar todo el mensaje para que el receptor lo pueda ver tan pronto llega y el paralelo el software verifica que la firma es correcta.

5. Para proveer confidencialidad, autenticación e integridad de mensajes alguien propone el esquema de la figura adjunta para su envío. ¿Se logra cada una de estas propiedades? Explique.



NO. El esquema propuesto no garantiza ninguna de las propiedades.
Como la clave simétrica fue encriptada con la clave privada de Alicia, puede ser desencriptada por cualquiera, luego cualquiera puede tener acceso al contenido del mensaje.
La integridad se pierde pues cualquiera puede obtener la clave simétrica, el intruso usando su mensaje puede obtener su hash y luego encriotarlo con la clave pública de Bob. Luego encripta todo con la clave simétrica creada por Alicia y concatenar la misma versión encriptada de la clave simétrica que envió Alicia.
Se pierde autenticación pues no se puede asegurar que el mensaje haya sido creado por Alicia. El caso previo muestra cómo Bob no puede reconocer mensajes enviados por Alicia y el intruso..

6. ¿Por qué SSL utiliza un mensaje especial para el cierre de la conexión si TCP ya cuenta con los mensajes para el cierre de conexión?
Porque así los extremos de la comunicación SSL pueden diferenciar el cierre generado por un atacante que inyecta un mensaje FIN de TCP de aquel enviado luego de un cierre deseado de la conexión SSL. De esta forma se reconoce el ataque generado por envío prematuro de un FIN.

7. ¿ Por qué en una conexión SSL es mejor intercambiar dos claves simétricas por cada lado (para Código de Autenticación de Mensaje y de encriptación) y no ocupar una mecanismo de clave pública/privada en reemplazo de una de esas claves?
Porque el mecanismo de clave pública/privada es mucho más lento de aplicar. Si se usara se consumiría más recursos y la comunicación sería más lenta. La encriptación simétrica es mucho más veloz.

8. Se le encarga la tarea de detectar y evitar ataques SYN (se inicia la conexión pero no se concluye) a un servidor WEB, ¿Describa la protección más simple que usted puede sugerir?
Habría que poner un cortafuegos con estado. Ante la llegada de un SYN habría que detectar si llegan datos posteriores; si no los hay, se podría enviar un mensaje RESET (o FIN) al mismo servidor para que éste libere los recursos reservados.