Examen-Septiembre-2018-RESUELTO.pdf

Juandf03

Seguridad de la Información

3º Grado en Ingeniería Informática

Escuela Técnica Superior de Ingeniería Informática
Universidad de Málaga

Parte 1

1. Explicar los conceptos de confusión y de difusión y cómo se usan en los algoritmos de cifrado en bloque.

* Confusión: La relación entre el mensaje cifrado y la clave debe ser lo más complicada posible.
* Difusión: Cada caracter del mensaje cifrado debe depender de alguna parte de la clave.

Un algoritmo de cifrado en bloque divide el mensaje M en subcadenas -bloques- que va cifrando, de forma que el resultado final -mensaje cifrado- es la concatenación de dichos bloques. La confusión aparece al final, como su propia definición indica, observando que no exista una relación evidente entre el mensaje cifrado y la clave; la difusión aparece en el interior del algoritmo, ya que en algunos algoritmos, para cifrar dichos bloques se generan subclaves de la clave original.

2. Ventajas de los algoritmos de clave pública respecto a los algoritmos simétricos. Justificar la existencia/uso de los criptosistemas híbridos.

Cuando 2 usuarios se comunican, no necesitan aclarar una clave a priori; lo que implica que no resulte problemático que estén lejanos físicamente; y por último, el número de claves se reduce de _*(n * (n-1) / 2)*_ en los algoritmos simétricos a _*2*n*_ en los algoritmos asimétricos, donde _*n*_ es el número de usuarios de la comunicación.

Los criptosistemas híbridos combinan algoritmos simétricos con asimétricos, y se usan debido a su bajo rendimiento: 2 usuarios usan un algoritmo asimétrico para el intercambio de una clave que usarán posteriormente para cifrar su comunicación mediante un algoritmo simétrico. Se usa el más pesado (asimétrico) una sola vez, para asegurar una comunicación con el cifrado más ligero (simétrico).

3. Definir qué es el cifrado producto y explicar su funcionamiento.

El cifrado producto consiste en aplicar sucesivamente algoritmos de cifrado (normalmente, diferentes) a un mensaje _*M*_, para lograr un nivel de seguridad complejo mediante sistemas sencillos.

Funciona de la siguiente manera: _*E₃ (E₂ (E₁ (M)))*_, donde al mensaje _*M*_ se le aplica el cifrado _*E₁*_, al resultado de eso, el cifrado _*E₂*_, y por último, a todo eso el cifrado _*E₃*_.

4. Describir las características principales de una función hash criptográfica.

Una función hash transforma un bloque de información _M_ de longitud variable en un bloque de información hash _h_ de longitud fija (huella digital de _M_): la función es unidireccional, ya que con _h_, no puede obtenerse _M_; y también libre de colisiones, porque es imposible que 2 mensajes _M_ y _M'_ distintos produzcan el mismo _h_.

5. Sean los servicios de confidencialidad, autenticación e integridad:

1. Defínelos.

* Autenticación: asegurarse de que la entidad con la que me comunico es realmente quien dice ser.
* Confidencialidad: protección de los datos frente a aquellos que no deben acceder a ellos.
* Integridad: asegurarse de que los datos que recibo son realmente los que se han enviado.

2. Justifica en qué capas del modelo OSI puede alojarse cada uno.

* Autenticación:
* Confidencialidad:
* Integridad:

3. Indica qué mecanismos se usan para su implementación para cada uno.

* Autenticación: autenticación por entidad y del origen de datos.
* Confidencialidad: confidencialidad en conexión, sin conexión, de campos seleccionados y del tráfico de datos.
* Integridad: integridad de la conexión con recuperación, sin recuperación, con campos seleccionados, integridad sin conexión e integridad sin conexión de campos seleccionados.

Parte 2

1. Modela el algoritmo Otway-Rees e indica cuáles fueron los motivos por los cuales se mejoró el algoritmo Needham-Schroeder.

```
1. A -> B : I, A, B, Eat(I, A, B, Na)
2. B -> T : I, A, B, Eat(I, A, B, Na), Ebt(I, A, B, Nb)
3. T -> B : I, Eat(Kab, Na), Ebt(Kab, Nb)
4. B -> A : I, Eat(Kab, Na)
```

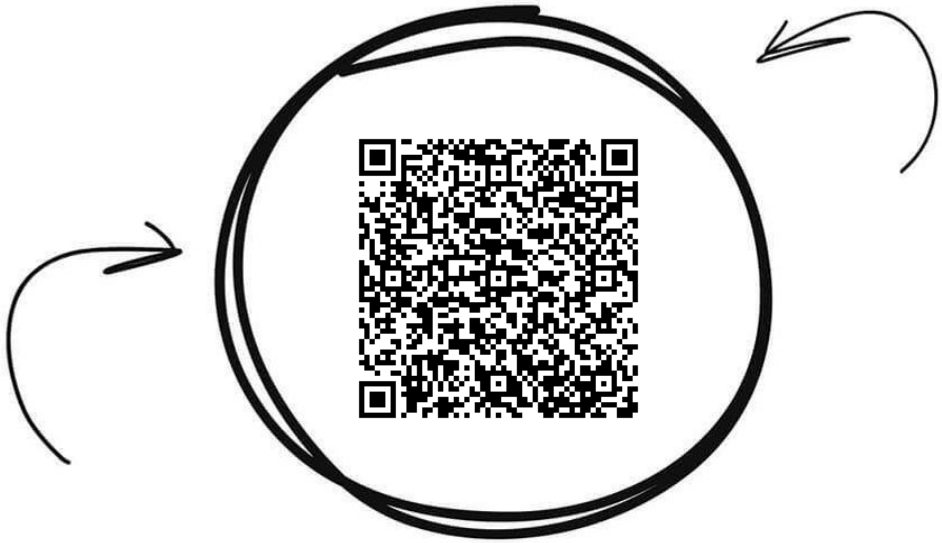
AUSSAR
TIENDA DE INFORMÁTICA ONLINE

¡Encuentra el portátil perfecto para la uni!

Tenemos justo lo que necesitas: equipos a medida, móviles, tablets y más. ¡De ofimática a servidores, y todo listo para ti!

¡Ofertas exclusivas para ti! Escanea el QR y descúbrelas ahora en aussar.es

Seguridad de la Información



Banco de apuntes de la

WUOLAH

Comparte estos flyers en tu clase y consigue más dinero y recompensas

1. Imprime esta hoja
2. Recorta por la mitad
3. Coloca en un lugar visible para que tus compis puedan escanar y acceder a apuntes
4. Llévate dinero por cada descarga de los documentos descargados a través de tu QR

El algoritmo Needham-Schroeder se mejoró porque tenía 3 fallos de seguridad que consistían en:
* La suplantación de _A_.
* Un ataque de repetición entre la conexión de _A_ a _B_.
* Un ataque DoS en el mismo punto.

Para ello, se añadió un nonce en todos los pasos del algoritmo y no solo en los 3 primeros (como anteriormente).

2. ¿Qué propiedad debe cumplirse en los protocolos de lanzamiento de moneda y de póker mental para que se pueda aplicar?

Ha de cumplirse el siguiente requisito, que siempre es válido en algunos pero no todos los algoritmos criptográficos:
$D_{K1}(E_{K2}(E_{K1}(M))) = E_{K2}(M)$

3.1. Modela el funcionamiento general del protocolo de división de secretos, suponiendo que el mensaje secreto M se quiere repartir entre 5 personas.

El protocolo de división de secretos consiste en la división de un mensaje _M_ cifrado, entre _n_ usuarios, donde se requiere a todos los usuarios para poder descifrar el mensaje original. Suponiendo que _n = 5_, el funcionamiento resulta:

1. Se generan _4_ cadenas aleatorias de bits (del mismo tamaño que _M_).
   * Cadenas generadas: _A_, _B_, _C_ y _D_.

2. Se opera _M_ con todas las cadenas usando XOR, obteniendo una cadena _R_.
   * _M (+) A (+) B (+) C (+) D = R_.

3. Se le otorga a cada usuario una de las cadenas.

Si se operan todas las cadenas usando XOR, se obtendrá _M_.
* _A (+) B (+) C (+) D (+) R = M_.

3.2. ¿Qué restricción presenta? Razonar la respuesta mediante un ejemplo.

La mayor restricción es que si una de las partes se pierde, ya no es posible recuperar el mensaje _*M*_.

4. Dibujar el esquema de operaciones que se llevan a cabo en SSL Record Protocol, teniendo en cuenta el orden de sus acciones.

1. Fragmenta los datos de la subcapa alta -y para cada fragmento-:
2. Lo comprime (opcional).
3. Le añade el MAC.
4. Lo cifra.
5. Le añade una cabecera.

El resultado final se transmite en un mensaje TCP.

5. Nombrar los servicios de seguridad que proporcionan tanto el protocolo SSL como TLS y explicar en qué consiste un suite de cifrado (SSL Cipher Suite).

6. Nombrar al menos tres mecanismos de privacidad explicando sus objetivos.

7. ¿Qué define una política de seguridad en IPsec?

Garantizar la protección de todas sus aplicaciones, necesiten seguridad o no.

8.1 Describe el protocolo IKE (fase 1 y fase 2) y dibuja el protocolo ISAKMP.

1. Establecer una SA ISAKMP previa a la SA de IPSec.
   * Dos modos posibles: principal y agresivo.

2. El SA ISAKMP se emplea para negociar y establecer los SAs de IPSec.

Modo principal de ISAKMP:
```
```

A ----- Crypto ofrecida ---> B
A <---- Crypto elegida ----- B
A ------- Ga mod (p) ------> B
A <------ Gb mod (p) ------- B K = Gab mod (p)
A --- K(A, prueba_A, Ma) --> B
A <-- K(B, prueba_B, Mb) --- B
```

**8.2. Dibuja el modo agresivo del protocolo ISAKMP.**

```
A -------- Ga mod (p), A, Crypto ofrecida -------> B
A <-- Gb mod (p), Crypto elegido, prueba_A, Mb --- B
A ------------------- prueba_A ------------------> B
```
```