Universidad de Granada
Departamento de Teoría de la Señal,
Telemática y Comunicaciones

SEGURIDAD EN REDES DE COMUNICACIÓN

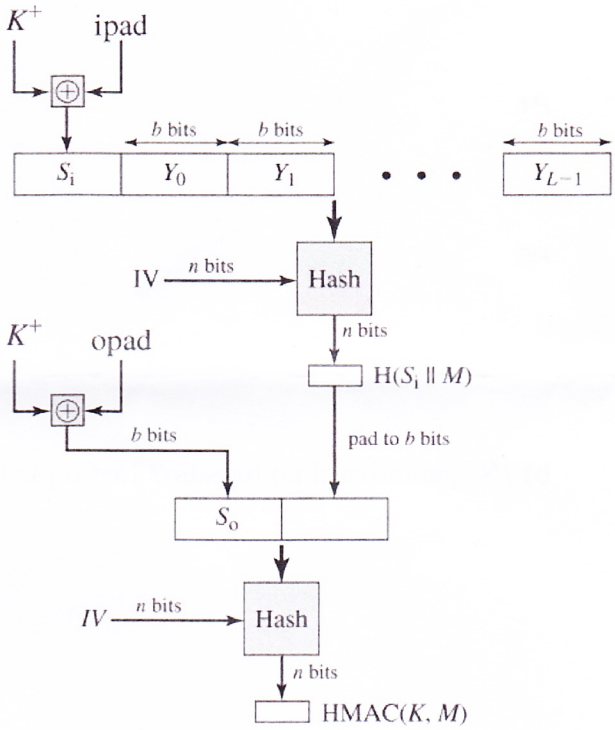
– 3er. curso Grado en Ingeniería de Tecnologías de Telecomunicación –

Examen de teoría[1] – Junio 2015

Apellidos: _____ **Nombre:** _____

1. *(1 pto. = 4×0,25)* Dado el esquema H-MAC adjunto (RFC 2104), responda a las siguientes cuestiones:

a) ¿Qué servicios de seguridad se proporcionan? ¿En base a qué elementos del esquema?



b) ¿Cómo se deriva K^+ de la clave K?

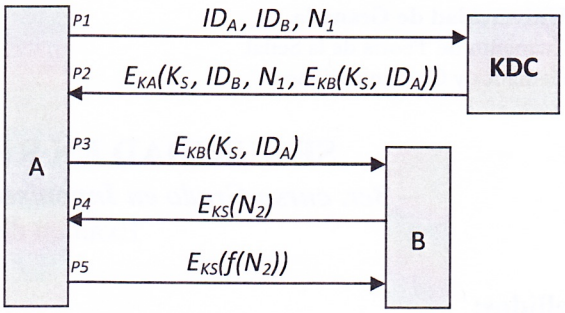
c) Obtenga la expresión de la salida generada, HMAC*(K,M)*, siendo $M = Y_{L-1}, \ldots, Y_0$ el mensaje de entrada.

d) ¿Cuál es la longitud en bits de la salida HMAC*(K,M)*, si la de M es 1.240 bytes?

[1] Esta parte de la asignatura se evaluará sobre un máximo de 6 puntos, debiéndose responder a cada una de las preguntas/ejercicios en el espacio específico reservado para ello.

2. *(1 pto. =2×0,5)* Suponga el protocolo de autenticación esquematizado abajo:

a) Explique el procedimiento en cuestión seguido.



P1.

P2.

P3.

P4.

P5.

b) ¿Se garantiza el no repudio? Justifique la respuesta.

3. *(0,5 ptos.)* Cuando se usan conjuntamente las cabeceras de encapsulado y autenticación en IPsec, primero se aplica ESP y después AH. ¿Por qué no hacerlo al contrario; primero AH y después ESP?

4. *(1,5 ptos.=2×0,75)* Dadas dos entidades finales que desean llevar a cabo entre sí un servicio seguro sobre SSL/TLS:

a) Explique el procedimiento global seguido en la comunicación, en base a los protocolos constitutivos de SSL/TLS y la funcionalidad asociada.

b) Establecido el canal SSL/TLS, indique los procesos involucrados en el transporte de la información del servicio de aplicación. Señale, en su caso, las diferencias entre SSL y TLS.

5. *(0,5 ptos.)* Dado el seudocódigo adjunto correspondiente a un *malware.exe*, indique:

Vector de infección:

Disparo:

Carga:

```
...
if (fecha==15 mayo) {
  busca y borra ficheros '.txt' del disco duro;
  for (i=0; i<#contactos_agenda_mail;i++) {
     envía email con 'malware.exe' como
                          adjunto a contacto[i];
  };
};
...
```

6. *(1 pto.=2×0,5)* Explique los procesos de *Exploración* (a) y *Vulnerabilidades* (b) habituales en una intrusión. De los siguientes procedimientos/herramientas, ¿cuáles podrían usarse para llevar a cabo cada una de las etapas anteriores?: (*i*) instalación de *backdoor*; (*ii*) uso de *Metasploit*; (*iii*) *port scan*; (*iv*) instalación de *rootkit*; (*v*) consulta de CVE.

7. *(0,5 ptos.=5×0,1)* Seleccione la respuesta correcta a cada una de las siguientes cuestiones:

a)	**El algoritmo de Diffie-Hellman**	
	Es de tipo asimétrico	☐
	Precisa el conocimiento a priori de la clave	☐
	A diferencia de RSA, basa su potencia en la teoría de los números primos	☐
	Todas las respuestas anteriores son incorrectas	☐
b)	**La cabecera AH de IPSec en modo túnel se encapsula como sigue:**	
	Cabecera_IP2 + AH + Cabecera_IP1 + Datos	☐
	Cabecera_IP + AH + Datos	☐
	AH + Cabecera_IP1 + Cabecera_IP2 + Datos	☐
	Cabecera_IP1 + Cabecera_IP2 + AH + Datos	☐
c)	**El protocolo PPTP**	
	Permite el control del túnel sobre TCP	☐
	Se complementa con el encapsulado de las tramas PPP mediante GRE	☐
	Contempla mensajes de control de llamada y de control de conexión	☐
	Todas las respuestas anteriores son correctas	☐
d)	**Una técnica de detección de cualquier *malware* es**	
	Detección de actividades normales en el entorno	☐
	Determinación de una tasa de paquetes servidor→cliente elevada	☐
	Uso de firmas/patrones identificativos	☐
	Generación de reglas de reenvío en el cortafuegos	☐
e)	**Las técnicas de *watermarking***	
	Son tecnologías denominadas ERM/IRM, donde se trata de controlar el recurso distribuido	☐
	Implican una autenticación *online* del usuario	☐
	A diferencia de las técnicas de *fingerprinting*, incorporan datos del consumidor del producto	☐
	Todas las respuestas anteriores son incorrectas	☐