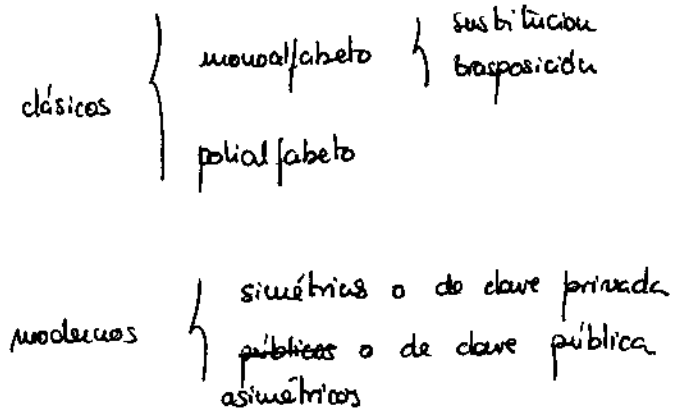
Nino

Protección y Seguridad de la Información

Junio 2001

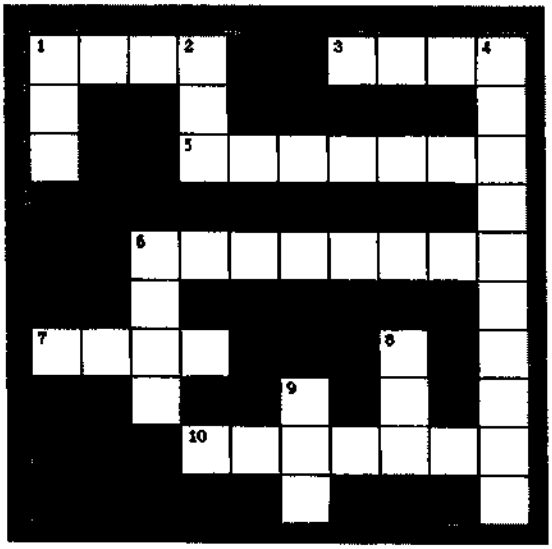
Nombre: Apellidos:

1. Métodos criptográficos clásicos y modernos. Haga un esquema con todos los métodos que conozca.



Nombre: Apellidos:

2. HORIZONTALES. 1. Mecanismo de seguridad en el almacenamiento en disco.// 3. Ley Orgánica de Protección de Datos.// 5. Padre de los fundamentos de la teoría de la información.// 6. Ataque desde el exterior que utiliza como dirección origen las internas a la organización.// 7. Puerto 80.// 10. Nombre de un emperador romano al que se le atribuye un método clásico de cifrado. VERTICALES. 1. Método de cifrado asimétrico.// 2. Puerto 53.// 4. Impedir una comunicación, una respuesta, causar un repudio de usuarios.// 6. Puerto 25.// 8. Método de cifrado simétrico.// 9. Mecanismo para cifrar datos enviados. Ampliamente utilizado en el correo electrónico.



Nombre: Apellidos:

3. Métodos criptográficos clásicos y modernos. Haga un esquema con todos los métodos que conozca.

Nombre: Apellidos:

4. Definiciones cortas

a) SSL

b) huella digital

c) encriptar

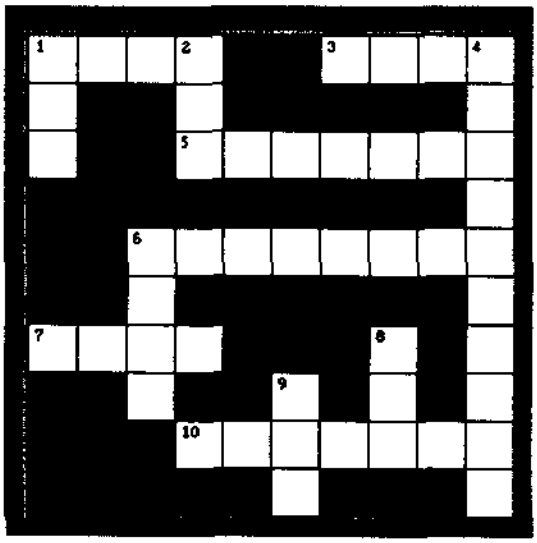
d) SAI

e) homófono

f) IDS

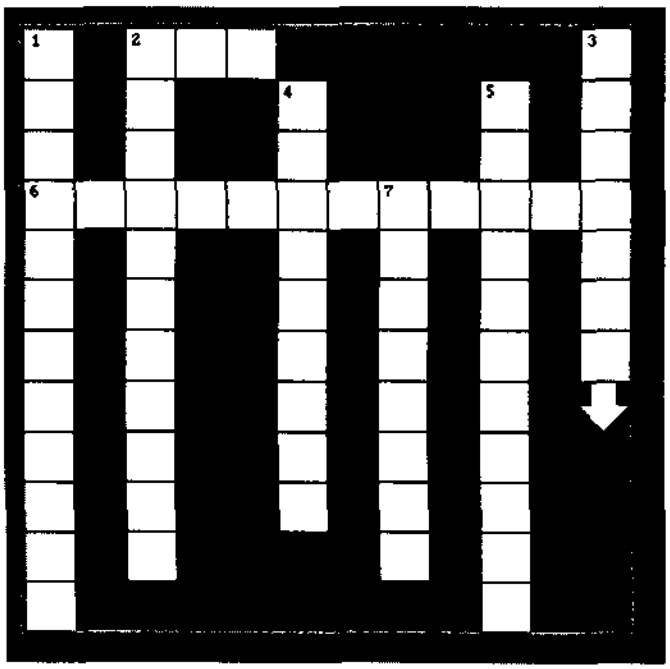
Nombre: Apellidos:

6. HORIZONTALES. 1. Mecanismo de seguridad en el almacenamiento en disco.// 3. Ley Orgánica de Protección de Datos.// 5. Padre de los fundamentos de la teoría de la información.// 6. Ataque desde el exterior que utiliza como dirección origen las internas a la organización.// 7. Puerto 80.// 10. Nombre de un emperador romano al que se le atribuye un método clásico de cifrado. VERTICALES. 1. Método de cifrado asimétrico.// 2. Puerto 53.// 4. Impedir una comunicación, una respuesta, causar un repudio de usuarios.// 6. Puerto 25.// 8. Método de cifrado simétrico.// 9. Mecanismo para cifrar datos enviados. Ampliamente utilizado en el correo electrónico.



Nombre: Apellidos:

7. HORIZONATALES. 2. Mecanismo para cifrar sesiones.// 6. Categoría de ataques en la que se encuadra el borrado de registros. VERTICALES. 1. Categoría de ataques que incide sobre la integridad.// 2. Técnica criptográfica que sustituye un carácter del texto en claro por otro en el texto cifrado.// 3. Forma básica de chequeo de puertos abiertos.// 4. Autor de un tratado sobre criptografía militar que propone que "un sistema debe mantener su impenetrabilidad, aún cuando el criptoanalista conozca con detalle la manera en que se cifra el mensaje, con tal de que no se conozca la clave utilizada...".// 5. Unión de la criptografía y el criptoanálisis.// 7. Método de sustitución poligráfico en el que la clave es una matriz de 5x5.//



Nombre: Apellidos:

8. Definiciones cortas

1. Métodos de sustitución

2. criptología

3. encriptar

4. RSA

9. Definiciones cortas

1. Sniffing

2. firma digital

3. algoritmo mixto JERG

4. certificado digital

Nombre: Apellidos:

10. Diferencias entre PROTECCIÓN y SEGURIDAD de la información

PROTECCIÓN Y SEGURIDAD DE LA INFORMACIÓN

Curso 2001-2002

Nombre: Apellidos:

1. Se dispone de una idea genérica sobre una pequeña empresa tecnológica con ámbito de actuación en la red Internet. Esta empresa proporcionará todo tipo de servicios en Internet (acceso a sistemas de información relacionados con la actividad principal de la empresa, web, email, gestión y resolución de nombres, etc.). Además deberá disponer de personal técnico cualificado, tanto para la administración como para la explotación –mínimo dos pequeños departamentos-. Como es lógico, la seguridad de la información deberá ser un punto primordial. También se valorará el grado de ajuste a las instalaciones y tecnologías de última generación.

Ustedes deciden poner a funcionar dicha idea. Para ello hablan con su profesor de PSI que, aunque podría plantear una empresa de teletrabajadores totalmente distribuida, les sugiere dada la propia naturaleza de la empresa la necesidad de un pequeño local. Además, el profesor de PSI les regala las viviendas 4ºC (80 m^2) y 5ºC (80 m^2) de un edificio que ha ganado jugando a las chapas en Ponferrada.

ACCIONES PREVIAS A RESOLVER:

-
-
-
-
-
-
-
-
-
-
-
-
-

Nombre: Apellidos:

2. La modificación es una categoría de ataque contra

   a) la confidencialidad
   b) la disponibilidad
   c) la integridad
   d) la austeridad

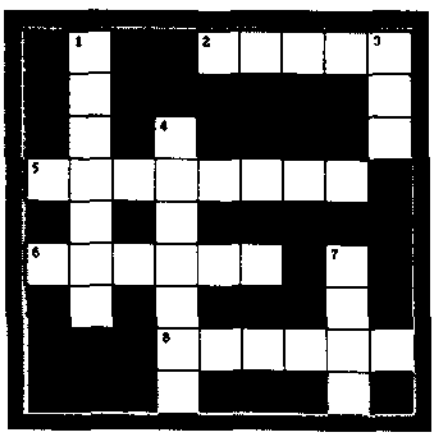
3. Un ataque por repetición es de tipo

   a) activo
   b) pasivo
   c) inverso
   d) mixto

4. ¿Qué técnica de "scanning" de puertos se conoce como "escaneo" de "media apertura" al no abrirse nunca una sesión TCP completa.

   a) TCP SYN scanning
   b) TCP connect() scanning
   c) TCP open() scanning
   d) TCP reverse ident scanning

5. HORIZONTALES. 2. Mecanismo que implica el cifrado, por medio de la clave secreta o privada del emisor, de una cadena comprimida de datos que se va a transferir.// 5. Elemento que centraliza la seguridad en una política de defensa perimetral.// 6. Herramienta para chequear la seguridad de los sistemas, sus servicios y puertos activos.// 8. Máquina de cifrado alemana de la segunda guerra mundial. VERTICALES. 1. Cifrador simétrico que utiliza bloques de 128 bits, clave de 128 bits y 16 vueltas.// 3. Listas de Acceso.// 4. Cifrador en el que en cada vuelta se cifra la mitad del bloque de información a cifrar y en cada vuelta se produce una permutación o intercambio de las dos mitades.// 7. Protocolo orientado a la gestión de redes.



Nombre: Apellidos:

GRÁFICO DE LA ESTRUCTURA FÍSICA DE LA RED Y ELEMENTOS:

GRÁFICO DE LA ESTRUCTURA LÓGICA DE LA RED Y ELEMENTOS:

Nombre: Apellidos:

ELEMENTOS HARDWARE

-
-
-
-
-
-
-

ELEMENTOS SOFTWARE

-
-
-
-
-
-
-
-
-
-
-
-
-

Nombre: Apellidos:

MECANISMOS DE SEGURIDAD Y ACCIONES (AGRUPAR SEGÚN NIVELES)

-
-
-
-
-
-