Corresponde al Anexo I de la Resolución N°: 208/00

ANEXO I

DEPARTAMENTO: MATEMÁTICA

ASIGNATURA: ORGANIZACIÓN DE COMPUTADORAS II

CARRERAS - PLAN: PROFESORADO EN COMPUTACIÓN – PLAN 98

CURSO: TERCER AÑO

RÉGIMEN: CUATRIMESTRAL (2º)

CARGA HORARIA: Teórico - prácticos: 6 HS. RELOJ POR SEMANA

CICLO LECTIVO: 2000

EQUIPO DOCENTE:

ING. PABLO GARCIA (PROFESOR ADJUNTO – DEDICACIÓN SIMPLE)
PROF. GUSTAVO J. ASTUDILLO (PROFESOR ADJUNTO – DEDICACIÓN SIMPLE)

OBJETIVOS Y/O ALCANCES DE LA ASIGNATURA

- Manejar los fundamentos teóricos de un sistema operativo.
- Resolver problemas de concurrencia mediante la aplicación de semáforos, monitores e intercambio de mensajes.
- Comprender los conceptos principales de los sistemas operativos distribuidos.
- Analizar el modelo por capas de las redes de computadoras.
- Discutir los conceptos clásicos de la teoría de la información.
- Analizar el concepto de encriptación en el actual contexto de desarrollo de la tecnología.
- Comprender los conceptos matemáticos para una encriptación segura.
- Implementar algoritmos concretos de encriptación
- Discutir las ideas principales del criptoanálisis.
- Exponer las principales metodologías utilizadas por los hackers en sus ataques informáticos.
- Proponer un plan integral para la seguridad de la información.

Corresponde al Anexo I de la Resolución N°: 208/00

- Exponer los conceptos teóricos de la compactación de información.
- Asegurar que los alumnos manejen correctamente los programas de compactación más difundidos.

ANEXO II

ASIGNATURA: ORGANIZACIÓN DE COMPUTADORAS II

CICLO LECTIVO: 2000

PROGRAMA ANALITICO

Unidad 1: Sistemas Operativos (S.O.)

- **Introducción.** Evolución histórica de los S.O.: Generaciones. Conceptos de S.O.: procesos, archivos, intérprete de comandos. Llamadas al sistema: manejo de procesos, señalación, manejo de archivos, manejo de directorios, protección, manejo del tiempo. Estructura de un S.O.: sistemas monolíticos, sistemas en estratos, máquinas virtuales, modelo Cliente - Servidor.
- **Procesos.** Modelo. Implementación. Comunicación entre procesos: condiciones del concurso, secciones críticas, exclusión mutua. Bloqueo y desbloqueo. Semáforos, contadores de eventos, monitores, transmisión de mensajes. Equivalencia de primitivas. Problemas clásicos de concurrencia. Planificación de un proceso.
- **Entrada/salida (E/S).** Hardware: Dispositivos de E/S. Controladores de dispositivos. Software: Objetivos del software de E/S, manejadores de interrupciones, drivers de dispositivos. Estancamientos: recursos, modelado, detección, recuperación y prevención. Discos: hardware y software. Relojes: hardware y software.
- **Administración de la memoria.** Monoprogramación. Multiprogramación con particiones fijas y variables. Intercambio. Administración de la memoria con mapas de bits, listas enlazadas y sistema compañero. Distribución del espacio para el intercambio. Análisis de sistemas de intercambio. Memoria virtual: paginación y segmentación. Algoritmos de sustitución de páginas.
- **Sistemas de archivo.** Aspectos básicos. Directorios. Diseño de un sistema de archivos: manejo del espacio en disco, almacenamiento en archivos, estructura del directorio, archivos compartidos, confiabilidad, rendimiento.

Unidad 2: Sistemas Operativos Distribuidos. (S.O.D.)

- **Introducción**: ¿qué es un S.O.D.?. Ventajas y desventajas de los S.O.D. Conceptos de hardware: multiprocesadores y multicomputadoras, buses y conmutador. Conceptos de software: sistemas operativos de redes, sistemas realmente distribuidos y sistemas de
- multiprocesador con tiempo compartido. Aspectos del diseño: transparencia, flexibilidad, confiabilidad, desempeño y escalabilidad.
- **Comunicación en los sistemas distribuidos.** Protocolos con capas: física, de enlace de datos, de red, de transporte, de sesión, de presentación y de aplicación. Redes con modo de transferencia asíncrona. ATM. Modelo cliente – servidor. Direccionamiento. Primitivas con y sin bloqueo. Primitivas con y sin buffer. Primitivas confiables y no confiables. Llamada a un procedimiento remoto (RPC). Operación básica de RPC. Transferencia de parámetros. Conexión dinámica. Comunicación en grupo.
- **Sincronización en sistemas distribuidos.** Sincronización de relojes. Relojes lógicos y físicos. Algoritmos de sincronización de relojes. Exclusión mutua. Algoritmos de elección. Transacciones atómicas. Bloqueos en sistemas distribuidos.
- **Procesos y procesadores en sistemas distribuidos.** Hilos. Diseño e implementación de un paquete de hilos. Modelos de sistemas: estación de trabajo, pila de procesadores. Asignación de procesadores. Fallas: de componentes, de sistema. Redundancia. Sistemas distribuidos de tiempo real.

Unidad 3: Redes de Computadoras

- **Introducción.** Importancia e las redes informáticas en la sociedad moderna. Hardware: redes de área local, metropolitana, amplia, redes inalámbricas y multirredes. Software: Jerarquías de protocolos. Interfaces y servicios. Primitivas de servicios. Relación entre servicios y protocolos. Modelos de referencia: OSI, TCP/IP. Ejemplos de redes. Novell Netware, Internet. Estandarización de redes.
- **Capa física.** Bases teóricas de la comunicación de datos. Análisis de Fourier. Señales limitadas por el ancho de banda. Tasa de envío máximo de un canal. Medios de transmisión: magnéticos, par trenzado, cable coaxial de banda base, cable coaxial de banda ancha, fibra óptica. Transmisión inalámbrica. Estructura del sistema telefónico.
- **Capa de enlace de datos.** Enmarcado. Control de errores. Control de flujo. Códigos de corrección de errores. Códigos de detección de errores.
- **Capa de acceso al medio.** Problema de reparto de canal. Protocolos de acceso múltiple.

- **Capa de red.** Diseño. Servicios proporcionados a la capa de transporte. Organización interna de la capa de red. Algoritmos de enrutamiento. Algoritmos de control de congestionamiento. Interredes.
- **Capa de transporte.** Servicios que proporciona a las capas superiores. Calidad del servicio. Primitivas del servicio de transporte. Elementos de los protocolos de transporte. Direccionamiento. Establecimiento de una conexión. Liberación de una conexión. Control de flujo y buffers. Multiplexión. Recuperación de caídas.
- **Capa de aplicación.** Seguridad de la red. Sistema de nombres de dominio (DNS). Protocolo sencillo de administración de redes (SNMP). Correo electrónico. USENET. World Wide Web.

Unidad 4: Teoría de la Información

- Teoría de la Información. Nociones básicas de la información. Entropía y cantidad de la información entre variables discretas. . Entropía Condicionada. Criptosistema Seguro de Shannon. Redundancia. Desinformación y Distancia de Unicidad. Confusión y Difusión. Transmisión de la información. Transmisión de la información en canales sin ruido. Transmisión de la información en canales con ruido.
- Codificación. Detección y corrección de errores. Códigos lineales: Códigos de Reed-Muller, Hamming y perfectos. Códigos cíclicos: Códigos BCH, Reed-Solomon y Goppa. Códigos correctores.

Unidad 5: Técnicas de Encriptación y Compactación

- Encriptación: Introducción. Procedimientos clásicos de cifrado. Sustitución y transposición. Condiciones de secreto perfecto. Aplicación práctica del cifrado de flujo. Criptoanálisis elemental: Frecuencia de las letras. Cifrado de Vigenére. Distancia de unicidad. Secreto perfecto. Compresión de texto claro.
- Criptografía de clave secreta: Métodos de cifrado en flujo. Generadores seudoaleatorios de secuencia cifrante: período, distribución de ceros y unos, imprevisibilidad, facilidad de implementación. Estructuras básicas para la generación de secuencias cifrantes: generadores basados en congruencias lineales, registro de desplazamientos realimentados. Filtrado no lineal. Combinadores no lineales: generadores de Geffe, Beth – Piper, Cascada de Gollman, bilateral de control paso a paso, multivelocidad de Massey Rueppel.
- Criptografía de clave secreta: métodos de cifrado en bloque. Arquitectura del cifrado en bloque. Cifrados de Feistel. DES: estructura, involución, manipulaciones, expansión de

claves, propiedades, seguridad. Modos de implementación de los cifrados en bloque: encadenamiento de bloques cifrados, realimentación del texto cifrado, realimentación de salida. Cifrado múltiple: encuentro a medio camino, cifrado triple. IDEA. RC5. SKIPJACK. Ataques especializados a los cifrados en bloque: criptoanálisis diferencial, lineal y basado en fallos e hardware.

- Gestión de claves. Tipos. Clave maestra y almacenamiento de claves. Generación de claves maestras. Redes de datos: centralizadas, horizontales. Gestión de claves simétricas. Plan integral de seguridad informática.
- Compactación. Codificación entrópica. Codificación por fuente. Ejemplos: JPEG, MPEG. Métodos de codificación utilizados por los compactadores más populares.

Corresponde al Anexo III de la Resolución N°: 208/00

ANEXO III

ASIGNATURA: ORGANIZACIÓN DE COMPUTADORAS II

CICLO LECTIVO: 2000

BIBLIOGRAFÍA

- **Fuster Sabater:** Técnicas Criptográficas de Protección de Datos – Alfaomega Grupo Editor.

- Lucena López, Manuel Jose**: Criptografía y Seguridad en Computadores. Segunda Edición. Septiembre de 1999. Departamento de Informática. Escuela Politécnica Superior. Universidad de Jaén.**

- **Tanembaun, Andrew:** Redes de Computadoras – Prentice Hall

- **Tanembaun, Andrew:** Sistemas Operativos – Diseño e Implementación – Prentice Hall

- **Tanembaun, Andrew:** Sistemas Operativos Distribuidos – Prentice Hall

Corresponde al Anexo IV de la Resolución N°: 208/00

ANEXO IV

ASIGNATURA: ORGANIZACIÓN DE COMPUTADORAS II

CICLO LECTIVO: 2000

PROGRAMA DE TRABAJOS PRÁCTICO

Trabajo Práctico 1
Resolución de ejercicios de concurrencia. Aplicación del método de semáforos.

Trabajo Práctico 2
Resolución de ejercicios de concurrencia. Aplicación del método de monitores.

Trabajo Práctico 3
Resolución de ejercicios de concurrencia. Aplicación del método de intercambio de mensajes.

Trabajo Práctico 4
Este práctico se refiere a sistemas operativos distribuidos. Incluye aplicación de los conceptos teóricos explicados en clase.

Trabajo Práctico 5
Redes. Se desarrollarán prácticas sobre computadoras, con aplicaciones de conceptos como protocolo, unidades compartidas, IRQ, etc. Se observarán los elementos de hardware necesarios para la implementación de redes locales (plaquetas de red, cables, conectores, etc.) y de redes amplias (módem).

Trabajo Práctico 6
Teoría de la información. Cálculo de entropías. Aplicación de códigos.

Trabajo Práctico 7
Criptografía. El práctico incluye la implementación de los algoritmos típicos de la criptografía clásica: César, Vigenere, Beaufort y Vernam.

Trabajo Práctico 8
Criptografía. Implementación de un algoritmo que utilice cifrado en bloque.

Corresponde al Anexo IV de la Resolución N°: 208/00

Trabajo Práctico 9

Manejo de los compactadores más populares. Implementación de un compactador que utilice alguno de los métodos expuestos en el teórico.

Corresponde al Anexo V de la Resolución N°: 208/00

ANEXO V

ASIGNATURA: ORGANIZACIÓN DE COMPUTADORAS II

CICLO LECTIVO: 2000

PROGRAMA DE EXAMEN

Unidad 1
Conceptos de sistemas operativos. Procesos. Concurrencia. Entrada – Salida. Memoria. Sistemas de archivos.

Unidad 2
Definición de sistema operativo distribuido. Ventajas y desventajas. Comunicación. Sincronización. Procesos y procesadores.

Unidad 3
Conceptos básicos sobre redes. Capa Física. Capa de enlace. Capa de acceso al medio. Capa de red. Capa de transporte. Capa de aplicación

Unidad 4
Teoría de la información. Entropía. Cantidad de Información. Transmisión de la información. Ruido. Códigos.

Unidad 5
Conceptos fundamentales de la encriptación. Sustitución. Transposición. Criptografía de clave secreta. Seguridad informática. Compactación: codificación entrópica y por fuente.