UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE INGENIERIA

DEPARTAMENTO DE COMPUTACIÓN

75.06 – ORGANIZACIÓN DE DATOS

LIC. SERVETTO

PROGRAMA ANALÍTICO

AGOSTO 2006

Índice General

Módulo – Organización de Archivos 3
Módulo – Sistemas de recuperación total de textos.....4
Módulo – File Systems.....5
Módulo – Compresión.....6
Módulo – Criptografía y Archivos Multimediales.....7

Módulo – Organización de Archivos

1. **Introducción: Principios conceptuales y procedimentales. Organización de archivos: registros físicos y lógicos. Definición lógica y física de registros. Acceso secuencial y relativo a registros. Caso de estudio. Metadatos e independencia lógica de datos.**

2. **Organización secuencial de archivos: Índices de identificación y de clasificación de registros. Organización secuencial indexada de archivos. Arboles B+.**

3. **Organización indexada de archivos: Árboles B y B*.**

4. **Resolución de consultas con múltiples índices: Organización directa de archivos. Índices directos.**

Módulo – Sistemas de recuperación total de textos

1. **Introducción: Estado del arte. Concepto de término y documento.**

2. **Índices Invertidos: Compresión de números de documentos. *Modelos Globales:* códigos unarios, códigos gamma, códigos delta, modelo global tipo Bernoulli, códigos de golomb, forma vectorial de los códigos y modelo global de frecuencia observada. *Modelos Locales:* modelo local tipo Bernoulli, modelo local de frecuencia observada y batching. *Almacenamiento de los términos:* términos de longitud fija, concatenación de términos, front coding y hashing perfecto y mínimo. *Construcción de Índices invertidos:* inversión por transposición de matrices e inversión por sort.**

3. **Signature-Files: Construcción de signature files. Bit Slices.**

4. **Optimizaciones: Case folding. Stop words. Stemming.**

5. **Resolución de consultas: Consultas Booleanas. Wildcards: N-gramas y léxico rotado. *Consultas ranqueadas*: coordinate matching, producto interno, producto interno mejorado y modelos de espacios vectoriales (método del coseno). Phrase queries: Los índices nextword. Consultas por proximidad.**

Módulo – File Systems

1. **Organización del espacio en disco: Identificación y localización de archivos. Seguridad y auditoria de accesos. Casos de estudio.**

2. **Buffering y optimizaciones.**

Módulo – Compresión

1. **Introducción: Estado del arte. Datos e Información. Codificación. Desigualdad de Kraft Códigos Prefijos. Entropía**

2. **Compresores Estadísticos: *Huffuman*: Representación de bits en bytes. Huffman dinámico. Códigos de Shannon Fano. Manejo eficiente del árbol. Half coding. *Compresión aritmética*: Aritmética de enteros. Descompresión en aritmético. Implementación con números binarios. Utilización de contextos. *PPMC*: Inicio de la compresión. Descompresión**

3. **Compresión no estadística: LZ77. Lz78 – LZW: Caso particular. Clearing. Implementación eficiente de la tabla. LZHUFF. LZP.**

4. **Localidad en archivos: Localidad. Move to Front. Block Sorting. Descompresión. Implementación. Modelos que aprovecha la transformación BS + MTF: Modelo de Shannon. Modelo aritmético. Modelo Estructurado. Half coding.**

Módulo – Criptografía y Archivos Multimediales

1. **Conceptos básicos sobre Criptografía: Objetivos de la criptografía. Criptosistema. Definición y tipos de criptoanálisis. Relación entre criptosistema y criptoanálisis.**

2. **Criptografía clásica: Cifrado por bloque. Modos de cifrado por bloque. Cifrados por sustitución. Sustitución simple o monoalfabéticos. Cifrado Afin. Cifrado Homofónico. Cifrado Polialfabético (Vigenere). Cifrado Poligráfico (Hill y PlayFair). Cifrado por transposición. Cifrado por producto. Cifrado por Flujo. One Time Pad.**

3. **Criptografia de clave privada: Fundamentos. Data Encrytion Standard (DES). Triple DES. Advanced Encryption Standard (AES). Criptoanálisis diferencial y lineal.**

4. **Criptografía de clave pública: Fundamentos matemáticos. Criptosistema RSA. Criptoanálisis de RSA (Factorización de n, Seguridad del algoritmo). Vulnerabilidades de RSA. Algoritmo de Merkle-Hellman (knapsack).**

5. **Firmas Digitales: Firma de clave privada. Firma de clave pública. Función resumen. Diferencias y similitudes entre la firma manuscrita y la firma digital.**

6. **Administración de claves públicas: Certificados digitales.**

7. **Pretty Good Privacy (PGP): Introduction. Esquema de encriptación y desencriptación. Esquema de firma digital. Certificados digitales.**

8. **Protocolos criptográfico: ejemplos de aplicación.**

9. **Archivos Multimediales: Aplicaciones de los temas anteriores de la materia a archivos multimediales y sistemas multimedios. Compactación de datos.**