



UNIVERSIDAD DE LAS PALMAS
DE GRAN CANARIA

GUÍA DOCENTE

CURSO: 2007/08

12724 - CRIPTOGRAFÍA

ASIGNATURA: 12724 - CRIPTOGRAFÍA

Vinculado a : (Titulación - Asignatura - Especialidad)

1801-Ingeniería en Informática - 12724-CRIPTOGRAFÍA - 00

CENTRO: Escuela de Ingeniería Informática

TITULACIÓN: Ingeniero en Informática

DEPARTAMENTO: INFORMÁTICA Y SISTEMAS

ÁREA: Ciencia De La Comp. E Intel. Artificial

PLAN: 10 - Año 1999**ESPECIALIDAD:**

CURSO: Cr. comunes cic**IMPARTIDA:** Primer semestre **TIPO:** Optativa

CRÉDITOS: 4,5

TEÓRICOS: 3

PRÁCTICOS: 1,5

Descriptores B.O.E.

Criptosistemas de Clave Secreta y Pública. Técnicas y Protocolos Criptográficos.

Temario

PROGRAMA

TEMA I

INTRODUCCIÓN A LA ARITMÉTICA MODULAR

1. Aritmética modular

1.1. Congruencias y aritmética modular.

1.1.2 Residuos. Conjunto completo de residuos.

1.1.3 Principio de la aritmética modular. Exponenciación modular. Algoritmo rápido de exponenciación.

1.1.4 Cálculo de inversos. Conjunto reducido de residuos. Función Totient de Euler. Cálculo de la función de Euler.

1.1.5 Teorema de Fermat. Generalización la función de Euler.

Resolución de ecuaciones diofánticas.

1.1.6 Algoritmo extendido de Euclides.

Temporización 3 horas

TEMA II

CRIPTOGRAFÍA: CONCEPTOS GENERALES

2.1. Criptografía : Conceptos generales.

2.1.1. Criptografía, texto original, texto cifrado, criptograma, cifrado o

encriptación, claves, cifrado de trasposición, cifrados de sustitución, cifrados de César, códigos, criptoanálisis, criptología.

2.1.2. Métodos de ataque según el conocimiento que se tenga de los textos original y cifrado.

2.1.3. Notaciones usuales.

2.1.4. Las grandes reglas del criptoanálisis.

2.1.5. Sistemas criptográficos. Definiciones.

Temporización 3 horas

TEMA III

CRIPTOGRAFIA CLASICA.: ALGORITMOS DE CIFRADO.

3.1. Sistemas monoalfabéticos.

3.1.1. Permutaciones de n-gramas. Cifrados de trasposición.

3.1.2. Sustituciones de letras. Sistemas de sustituciones.

3.1.3. Cifrados de sustitución simple. Cifrados de César..

3.1.5. Alfabetos standard mezclados.

3.1.6. Transformaciones afines. Sustitución afín de César

3.1.7. Transformaciones polinómicas. Análisis de la frecuencia.

3.1.8. Sustitución monoalfabética general.

3.1.9. Cifrados de sustitución poligrámica.

3.1.9.1. Cifrado Playfair. Criptoanálisis de un cifrado Playfair.

3.1.9.2. Cifrado Hill. Criptoanálisis de un cifrado Hill.

3.1.10. Cifrados de sustitución homofónica.

3.1.10.1. Definiciones y ejemplos.

3.1.10.2. Cifrados de Beale.

3.1.10.3. Cifrados homofónicos de orden superior.

3.2. Sistemas polialfabéticos.

3.2.1. Introducción y definiciones.

3.2.2. Cifrado de Vigenere. .

3.2.3. Máquinas de Rotor y de Hagelin. La máquina Enigma y su criptoanálisis.

3.2.4. Cifrado de Vernam

Temporización 4 horas

TEMA IV

CRIPTOSISTEMAS SIMÉTRICOS O DE CLAVE SECRETA

4.1 Características de un criptosistema de clave secreta

4.2. Cifrados sustitución-permutación.

4.3. Cifrado LUCIFER (IBM).

4.4. El Data Encryption Standard (DES).

4.4.1. Descripción del sistema y filosofía de diseño.

4.4.2. Críticas al DES.

4.4.3. Criptoanálisis del DES.

4.4.4. Triple DES

4.5 Advanced Encryption Standard (AES)

4.6 Sistemas mixtos: PGP

BIBLIOGRAFIA: [DENN-83] [KOHN-81] [MEYE-82] [PATT-87] [VANT-88]

Temporización 6 horas

TEMA V

CRIPTOSISTEMAS DE CIFRADO EN FLUJO

- 5.1 Métodos de cifrado en flujo
 - 5.1.1 Cifrado en flujo síncrono
 - 5.1.2 Cifrado en flujo asíncrono
 - 5.1.3 Diferencias entre cifrado en flujo síncrono y asíncrono
 - 5.2 Cifrado de Verman
 - 5.3 Postulados de Colomb
- Temporización 2 horas

TEMA VI

CRIPTOSISTEMAS DE CLAVE PUBLICA

- 6.1 Criptosistemas de clave pública
 - 6.1.1 Introducción a los Criptosistemas de clave pública.
 - 6.1.2 Ventajas e inconvenientes sobre los de clave privada
 - 6.1.3 Criptosistema R,S.A.
 - 6.1.4 Alternativas al R.S.A.

Temporización 4 horas

TEMA VII

DISTRIBUCION DE CLAVES

- 7.1 Arquitrctura de Seguridad
 - 7.1.1 Clasificación de problemas de seguridad
 - 7.2 Modelos de validación basados en métodos distribuidos
 - 7.2.1 Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman: protocolo
 - 7.2.2 Validación de identificación usando un centro de distribución de claves (KDC)
 - 7.2.3 Validación de identificación basada en clave secreta compartida: protocolo
 - 7.3 Autenticación con Kerberos
- Temporización 2 horas

TEMA VIII

SEGURIDAD EN LA RED

- 8.1 Requerimientos de seguridad en la Red
 - 8.2 Arquitecturas seguras de tres niveles
 - 8.3 Tipos de Ataques
 - 8.4 Firewall
 - 8.4.1 Categorías de Firewall
 - 8.4.2 Nivel de Seguridad del Firewall
 - 8.4.3 Arquitecturas de Firewall
 - 8.5 DMZ (Zona desmilitarizada)
- Temporización 2 horas

TEMA IX

FUNCIONES DE AUTENTIFICACIÓN Y PROTOCOLOS CRIPTOGRÁFICOS: FIRMAS DIGITALES

- 9.1 Comunicación segura
- 9.2 funciones HAS Criptograficas

- 9.3 Firmas Digitales
 - 9.3.1 Firmas digitales y huellas digitales
 - 9.3.2 Seguridad de la firma
- 9.4 Certificado Digital
 - 9.4.1 Generación de Certificado
 - 9.4.2 Formato de un certificado
- 9.5 Autoridades de certificación (CA)
 - 9.5.1 Jerarquías de CAs
- 9.6 Protocolos criptográficos
 - 9.6.1 Transferencia transcodada
 - 9.6.2 Transferencia con conocimiento cero.

Temporización 4 horas

Requisitos Previos

Teoría de la Información. Cálculo de Probabilidades.

Objetivos

Criptografía. Seguridad Informática

Introducimos al alumno en el estudio de la teoría matemática de la aritmética modular así como en la teoría de la complejidad como bases necesarias para el estudio de la criptografía. Seguidamente se introduce la criptografía clásica. A continuación nos introducimos en la criptografía digital y para ello se utiliza tres grandes bloques que son: criptografía de clave privada, criptografía de clave pública y seguridad informática. Se utilizan las herramientas que le son propias, pero usando el modelo formal.

La formación que se pretende dar está orientada a que los alumnos adquieran en principio un sentido de objetivos, planteamientos y aplicaciones de la disciplina. Los objetivos básicos que se pretenden son:

Introducimos al alumno en el estudio de los fundamentos de la aritmética modular así como en la teoría de la complejidad como bases necesarias para el estudio de la criptografía.

Se introducirá al alumno en los conceptos básicos de criptografía y dotaremos a los mismos de los mecanismos y técnicas necesarias para entender, desarrollar y aplicar los algoritmos criptográficos. Dotaremos a los alumnos de los conocimientos necesarios para entender y aplicar los algoritmos criptográficos simétricos de clave secreta, así como los algoritmos criptográficos asimétricos de clave pública. También se le introducirá en los esquemas de firma digital.

Introduciremos al alumno en el conocimiento de los protocolos criptográficos así como a la gestión de claves.

El objetivo final es que los alumnos adquieran una formación en un conjunto básico de métodos y técnicas para el estudio de las técnicas criptográficas modernas y la seguridad en la Red.

Criterios de Evaluación

Evaluación

Los criterios para superar la asignatura serán los siguientes:

- 1.- La realización y entrega de los trabajos de prácticas será condición necesaria para aprobar la asignatura.
- 2.- Para aprobar por curso es necesario haber superado las pruebas que se realizarán (test) a lo largo del curso.
- 3.- Para aquellos alumnos que no aprueben por curso se realizará un examen final de la parte teórica.
- 3.- Los trabajos y prácticas realizados por el alumno tendrán un peso sobre la nota final de un 30%

y las notas de teoría un 70%.

Descripción de las Prácticas

Práctica nº 1

Descripción

ALGORITMO DE EUCLIDES Y ALGORITMO EXTENDIDO DE EUCLIDES CALCULO DE INVERSOS MODULARES.

Objetivos:

Esta práctica tiene como objetivo que el alumno implemente el algoritmo de Euclides y el algoritmo extendido de Euclides

Material de laboratorio recomendado

La práctica puede ser realizada en estaciones o PC con W-XP con conexión a red.

Nº horas estimadas en Laboratorio: 2

Nº horas total estimadas para la realización de la práctica: 2

Práctica nº 2

SIMULACIÓN DEL CRIPTOSISTEMA D.E.S.

Objetivos

Esta práctica tiene como objetivo la simulación del criptosistema DES

Material de laboratorio recomendado

La práctica puede ser realizada en estaciones o PC con W-NT-XP con conexión a red.

Nº horas estimadas en Laboratorio:5

Nº horas total estimadas para la realización de la práctica:4

Práctica nº 3

SIMULACIÓN DEL CRIPTOSISTEMA R.S.A.

Objetivos

Esta práctica tiene como objetivo la simulación del criptosistema RSA

Material de laboratorio recomendado

La práctica puede ser realizada en estaciones o PC con W-XP-NT con conexión a red.

Nº horas estimadas en Laboratorio:4

Nº horas total estimadas para la realización de la práctica:4

Práctica nº 4

CORREO SEGURO PGP

Objetivos

Tiene como objetivo la introducción al alumno en el e-mail seguro

Material de laboratorio recomendado

La práctica puede ser realizada en estaciones o PC con W-NT con conexión a red.

Nº horas estimadas en Laboratorio:4

Nº horas total estimadas para la realización de la práctica:5

Los alumnos que pueden cambiar las practicas 3 y 5 por la realización de uno de los siguientes trabajos de curso:

TRABAJOS DE CURSO

1.- Seguridad en Internet y en el comercio electrónico.

1.1 Requisitos de seguridad en la web. 1.2 Conceptos sobre comercio electrónico.

1.2.1 Arquitecturas del E-Com

- 1.2.2 Dinero electrónico.
- 1.2.3 Sistemas de crédito y débito.
- 1.2.4 Tarjetas de crédito. 1.2.5 Micropagos.
- 1.3 Protocolos del E-Com
- 1.3.1 SSL 1.3.1.1 Qué es SSL.
- 1.3.1.2 Registro en SSL.
- 1.3.1.3 Protocolos en SSL
- 1.3.1.4 Handshake del SSL
- 1.1.3.4 FSTC
- 1.4 SET
- 1.4.1 Características de SET
- 1.4.2 Agentes.
- 1.4.3 Módulos de programación.
- 1.4.4 Firma dual.
- 1.4.5 Transacciones.
- 1.5 Ventajas del SET sobre el SSL

- 2 Infraestructuras de clave pública (PKI)
- 2.1 Características de una PKI.
- 2.2 Uso de PGP para una PKI.
- 2.3 X.509
- 2.4 Seguridad de DNS
- 2.5 Sistemas PKI basados en credenciales.

- 3 Seguridad en comunicaciones móviles
- 3.1 Sistemas de comunicaciones móviles.
- 3.2 Sistemas GSM.
- 3.3 Sistemas de red alámbrica de AT&T
- 3.4 Sistema UTMS
- 3.5 Seguridad en el m-commerce

- 4.- Protocolos criptográficos.
- 4.1 Procedimientos para la distribución de secretos.
- 4.1.1 Método umbral de Shamir.
- 4.1.2 Método de las sombras congruentes.
- 4.2 Problemas de distribución de secretos.
- 4.2.1 Transferencia transcordada.
- 4.2.2 Pruebas de conocimiento cero.

- 5.- Intrusos, virus y gusanos
- 5.1 Intrusos.
- 5.2 Técnicas de intrusión.
- 5.3 Protecciones de password.
- 5.4 Detección de intrusos.
- 5.5 Virus y temas relacionados.
- 5.5.1 Programas maliciosos.
- 5.5.1.1 Puertas traseras.
- 5.5.1.2 Bombas lógicas.
- 5.5.1.3 Caballos de Troya.
- 5.5.1.4 Virus.
- 5.5.1.5 Gusanos.
- 5.5.1.6 Bacterias.
- 5.5.2 La naturaleza de los virus.

- 5.5.2.1 Estructura de un virus.
- 5.5.2.2 Tipos de virus.
- 5.5.3 Cómo funcionan los antivirus.

6 Cortafuegos.

- 6.1 Principios de diseño de un cortafuegos.
 - 6.1.1 Características de un cortafuegos.
 - 6.1.2 Tipos de cortafuegos.
 - 6.1.3 Distintas configuraciones.
- 6.2 Sistemas de confianza
 - 6.2.1 El concepto de sistemas de confianza.
 - 6.2.2 Protección frente a troyanos.
- 6.3 DMZ Demilitarized Zone

7 Seguridad de documentos.

- 7.1 Firma digital de documentos.
- 7.2 Certificados digitales.
- 7.3 Pruebas de autenticidad.
- 7.4 Autoridades de Certificación
- 7.5 Autenticidad, Confidencialidad, Integridad y No Repudio.
- 7.6 Sello Temporal
- 7.7 Medidas de seguridad.

8.- Criptografía Visual

- 8.1 Algoritmos de Criptografía Visual
- 8.2 Esquemas de Umbral

9.- Criptografía Cuántica

- 9.1 Información Cuántica
 - 9.1.1 Informática Cuántica
 - 9.1.2 Experimento de Informática Cuántica en Los Alamos
- 9.2 Criptografía Cuántica
 - 9.2.1 Principios Básicos de la Criptografía Cuántica
- 9.3 Protocolo BB84
- 9.4 Aplicaciones de la Criptografía Cuántica

10 Seguridad en redes inalámbricas (II)

- 10.1 Sistemas GSM.
- 10.2 Arquitectura de una red GSM
- 10.3 Seguridad en GSM
 - 10.3.1 Algoritmos de encriptado
- 10.4 Sistemas de red alámbrica de AT&T
- 10.5 Sistema UTM
- 10.5.1 Situación Actual de la 3ª Generación
- 10.5.2 Arquitectura General de UTM
- 10.5.3 Seguridad en UTM

Bibliografía

[1 Básico] Public key cryptography /

Arto Salomaa.

Springer-Verlag,, Berlin ; New York : (1990)

3540528318

[2 Básico] The codebreakers :the story of secret writing /

David Kahn.

Scribner,, New York : (1996) - (ed. rev. and updated.)

0684831309

[3 Básico] Seguridad informática y criptografía: libro impreso de la edición electrónica del mismo título sobre seguridad informática y protección de la información mediante el uso de técnicas criptográficas : documento de estudio en diapositivas animadas /

Jorge Ramió Aguirre.

Universidad Politécnica de Madrid. Escuela Universitaria de Informática,, Madrid : (2003) - (3ª ed.)

84-86451-69-8

[4 Básico] Seguridad y protección de la información /

José Luis Morant Ramón,

Arturo Ribagorda Garnacho, Justo Sancho Rodríguez.

Centro de estudios Ramón Areces,, Madrid : (1994)

848004098X

[5 Básico] Criptografía digital: fundamentos y aplicaciones /

José Pastor Franco, Miguel Angel Sarasa López.

Prensas Universitarias de Zaragoza,, Zaragoza : (1998)

8477334919

[6 Básico] Comunicación digital: teoría matemática de la información, codificación algebraica, criptología /

Josep Rifà i Coma, LLorenç Huguet i Rotger.

Masson,, Barcelona : (1991)

8431105763

[7 Básico] Fundamentos de seguridad en redes: Aplicaciones y estándares /

William Stallings.

Pearson,, Madrid : (2003) - (2ª ed.)

8420540021

[8 Recomendado] Handbook of applied cryptography /

Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.

CRC,, Boca Ratón [etc.] : (1996)

0-8493-8523-7

[9 Recomendado] Cryptography and data security /

Dorothy Elizabeth Robling Denning.

Addison-Wesley,, Reading, Mass : (1982)

0201101505

[10 Recomendado] Security and protection in information systems [

edited by Andre Grissonnanche.

North-Holland,, Amsterdam : (1989)

0-444-87345-7

[11 Recomendado] Cryptography: an introduction to computer security /

Jennifer Seberry, Josef Pieprzyk.

Prentice Hall,, New York : (1989)

0131949861

[12 Recomendado] Foundations of coding: theory and applications of error-correcting codes, with an introduction to cryptography and information theory /

Jirí

Adámek.

Wiley,, Chichester ; New York : (1991)

0471621870

[13 Recomendado] Security in computing.

Pfleeger, Charles P.

Prentice Hall,, Englewood Cliffs (New Jersey) : (1997) - (2nd ed.)

0131857940

[14 Recomendado] Cryptography and network security: principles and practice /

William Stallings.

Prentice Hall,, Upper Saddle River, New Jersey : (1999) - (2nd ed.)

0-13-869017-0

[15 Recomendado] Network security essentials: applications and standards /

William Stallings.

Prentice Hall,, Upper Saddle River, New Jersey : (2003) - (2nd ed.)

0-13-035128-8

Equipo Docente

MARTÍN MANUEL GONZÁLEZ RODRÍGUEZ

(COORDINADOR)

Categoría: TITULAR DE UNIVERSIDAD

Departamento: INFORMÁTICA Y SISTEMAS

Teléfono: 928458726 **Correo Electrónico:** manuel.gonzalez@ulpgc.es