ASIGNATURA DE MÁSTER:

CRIPTOGRAFÍA APLICADA

Curso 2013/2014

(Código:3110205-)

1.PRESENTACIÓN

El objetivo de esta asignatura es presentar los principios básicos de la criptografía moderna y su aplicación a la seguridad de la información y de las comunicaciones telemáticas actuales.

2.CONTEXTUALIZACIÓN

3.REQUISITOS PREVIOS RECOMENDABLES

Aunque No es imprescindible es conveniente tener conocimientos avanzados de matemáticas

4.RESULTADOS DE APRENDIZAJE

Uno de los principios en los que se apoya la seguridad de redes es la protección de la informaciónque se almacena y se transmite a través de la infraestructura en la que se apoya la red. Pararealizar la protección de datos se pueden usar técnicas matemáticas (agrupadas bajo unadisciplina denominada Criptología) que difuminan la información para que sólo se puedareconocer y obtener por parte del actor receptor de dicha información. La criptología se empleaen muchos ámbitos pero en especial en aquellos en los que la información es sensible:transmisión de información personal, datos bancarios, autentificación de usuarios a través de laWeb, etc... El desarrollo de los protocolos de comunicación correspondientes (SSL, SET, PGP,PEM, etc¿) se ha hecho en base a las diferentes técnicas criptográficas por lo que paracomprender el concepto de transmisión segura se hace imprescindible conocer en profundidaddichas técnicas. Por tanto, los objetivos de la asignatura son:· Conocer y comprender las diferentes técnicas criptográficas· Resolver y aplicar la amplia gama de algoritmos criptográficos (DES, IDEA, RSA, RC5,Diffie-Hellman, etc.) sobre problemas de tratamiento de datos concretos.. Sensibilizarse ante la protección de la información,Esta asignatura requiere de unos conocimientos básicos del lenguaje de programación Java yaque la realización de las actividades prácticas se realizará usando Java CryptographyArchitecture.Objetivos específicosPara lograr el objetivo principal de la asignatura el alumno debe ser capaz de:· Comprender las técnicas básicas sobre los procedimientos de difuminación de lainformación mediante cifrado mediante una revisión histórica de los diferentes métodosempleados hasta nuestro tiempo.· Analizar el funcionamiento de los algoritmos de secreto compartido (clave privada) y lasimplicaciones más importantes de su utilización como por ejemplo la distribución segura de laclave compartida. Es muy importante que el alumno se capaz de describir en profundidadalgoritmos tan extendidos como DES, IDEA o RC5.· Conocer la arquitectura de cifrado público y las bases de la teoría de números, en la cuálse apoya la criptografía de clave compartida. Además deberá entender el funcionamiento de losalgoritmos más importantes (RSA) y las bases de los algoritmos de curvas elípticas.· Entender el concepto de firma digital y como se implementan en base a algoritmoscriptográficos de clave pública como RSA o El Gamal. Además debe interpretar y analizar elconcepto de función de resumen (Hash) para la generación de información única para lavalidación de la información firmada digitalmente.· Conocer los ámbitos más extendidos de aplicación de las técnicas criptográficas en áreasde negocio como la Web (protocolos seguros: SSL o SSH), el correo electrónico (PGP o PEM) o elcomercio electrónico (SET).· Desarrollar proyectos de uso de las técnicas criptográficas mediante la arquitectura deseguridad criptográfica de Java e implementar procedimientos de seguridad basadas en losalgoritmos criptográficos más comunes.

5.CONTENIDOS DE LA ASIGNATURA

1.- Introducción a la criptología. 1.1.- Procedimientos clásicos de cifrado. 1.2.- Introducción al Criptoanálisis. 2.1-. Teoría de la Información. 2.2.- Distribución de las letras de una lengua escrita. 3.1.- Criptografía de Clave Privada. 3.2.- Arquitectura del cifrado en bloque. 3.3.- Cifrados de Feistel. 3.4..- DES. 3.5.- Modos de implementación de los cifrados en bloque. 3.6.- Cifrado múltiple. 3.7.- IDEA. 3.8.- RC5. 3.9.- AES y Rijndael. 3.10 - Ataques especializados a los cifrados en bloque. 4.1.- Criptografía de Clave Pública. 4.2.- Definiciones. 4.3.- Cambio de clave de Diffie-Hellman. 4.4.- Criptosistemas de clave pública. 4.5.- Criptosistema RSA. 4.6.- Ataque el criptosistema RSA. 4.7.- Criptoanálisis del tipo Wiener-Boneh. 4.8.- Criptosistema de ElGamal. 4.9.-. Ataque al criptosistema de ElGamal. 4.10.-- Criptosistemas de curvas elípticas. 4.11.- Criptosistema de la mochila tramposa. 5.1- Protocolos criptográficos y firmas digitales. 5.2.- Firma digital. 5.3.- Firma digital del criptosistema RSA. 5.4.- Firma digital del criptosistema de ElGamal. 5.5.- Funciones hash. 5.6.- Firma digital estándar del NIST. 6.1.- Aplicaciones de la criptografía de clave pública. 6.2.- Autenticación de un mensaje. 6.3.- Identificación del usuario. 6.4.- Seguridad en la Web. 6.5.- Correo electrónico seguro. 6.6.- Aplicaciones bancarias y comercio electrónico. APENDICE A: Soporte criptológico de JAVA: JCA12.1. A.1 Introducción. A.2 Evolución de la seguridad en Java. A.3 Autentificación y autorización.. A.4 Encriptación y Desencriptación.

6.EQUIPO DOCENTE

- ROBERTO HERNANDEZ BERLINCHES

7.METODOLOGÍA

8.BIBLIOGRAFÍA BÁSICA

Comentarios y anexos:

En esta asignatura se han elegido dos textos básicos recomendados:Técnicas Criptográficas de Protección de Datos. 3ª Edición actualizada.FÚSTER, A. y Otros, Editorial RA-MA, 2004Tutorial sobre JCA, Pedro Del Gallego VidaDisponible de forma gratuita en:http://www.javahispano.org/download.download.action?type=tutorials&id=8El segundo texto se distribuye de forma gratuita por lo que no redunda en ningún tipo deperjuicio económico extra para el alumno. El primer libro se adapta al contenido de los temasteóricos mientras que la publicación electrónica se emplea para el estudio de los contenidosdetallados en el apéndice A. Acompañando a los textos teóricos se adjunta la guía didáctica de laasignatura tal y como se define la metodología de enseñanza a distancia de la UNED. En dichaguía didáctica se detalla la distribución del temario sobre los dos textos bases y las actividadesprácticas de la asignatura. Adicionalmente, mediante la utilización de los medios telemáticosnecesarios (web, e-mail, etc.) se le proporcionará al alumno realimentación sobre informaciónrelevante de la asignatura que, dada la naturaleza de la misma, complementará la formación delalumno.

9.BIBLIOGRAFÍA COMPLEMENTARIA

Comentarios y anexos:

El alumno puede consultar la siguiente BIBLIOGRAFIA con el fin de aclarar o extender losconocimientos que debe adquirir a lo largo del curso, y más en concreto en lo concerniente a lasherramientas de software libre disponibles para la realización de las actividades prácticas:· Pastor, J.; Sarasa, M. A.: CRIPTOGRAFIA DIGITAL. Fundamentos y aplicaciones, EditorialPrensas Universitarias de Zaragoza (1998)· Brassard G.: Modern Criptology, LNCS, n.325, Springer-Verlag (1988).· Jason Weiss, Java Cryptography Extensions: Practical Guide for Programmers, MorganKaufmann, 2004.· Hardy, G.H. and Wright, E.M.: An Introduction to the Theory of Numbers, Oxford SciencePublications, Clarendon Press, Oxford (1989).· A. Menezes, P. van Oorschot and S.Vanstone.: Handbook of Applied Cryptography, CRCPress. (2001). Disponible en: http://www.cacr.math.uwaterloo.ca/hac/· An Introduction to Computer Security: The NIST Handbook}. Special Publication 800-12.NIST(1995). {http://csrc.nist.gov/}\texttt{publications/nistpubs/800-12/handbook.pdf}· Robling Denning D.E.: Cryptography and Data Security. Addison-Wesley PublishingCompany (1988).· Schneier, B.: Applied Criptography, John Wiley and Sons, Inc. 1996.· Simmons, G.S.: Contemporary Criptology. The Science of Information Integrity, IEEEPress

(1991).· Anderson, R.: Security Engineering: A Guide to Building Dependable Distributed System,Wiley (2001).· Pfleeger, C.P.: Security in Computing. , Prentice Hall (1997).

10.RECURSOS DE APOYO AL ESTUDIO

11.TUTORIZACIÓN Y SEGUIMIENTO

Los jueves lectivos de 16 a 20 h en el despacho 2.21 de la E.T.S. de IngenieríaInformática de la UNED (c(Juan del Rosal 16) o en el teléfono 913987614.En cualquier momento mediante mensaje al fax 913988909 o al correo electrónicojminguet@issi.uned.es o por carta a la dirección arriba indicada.

12.EVALUACIÓN DE LOS APRENDIZAJES

En el proceso de evaluación se tendrá en cuenta la resolución de las pruebas de evaluación adistancia, la participación en los foros, así como un examen presencial global de la asignatura.

13.COLABORADORES DOCENTES

- JESUS SALVADOR CANO CARRILLO