ASIGNATURA DE MÁSTER:

CRIPTOGRAFÍA APLICADA

Curso 2017/2018

(Código:3110205-)

1.PRESENTACIÓN

Criptografía Aplicada es una asignatura de diez créditos ECTS de carácter optativo que se imparte en el segundo semestre en la titulación de posgrado de Master Universitario en Comunicación, Redes y Gestión de Contenidos, dentro de la materia de Tecnologías y seguridad en redes.

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

La asignatura de Criptografía Aplicada se encuadra en la materia de Tecnologías y seguridad en redes. Se imparte en el segundo semestre de la titulación de posgrado de Master Universitario en Comunicación, Redes y Gestión de Contenidos. Esta materia se complementa con las asignaturas:

- Seguridad en redes: Auditoría y herramientas de seguimiento, asignatura optativa del segundo semestre.
- Redes inalámbricas y móviles, que se cursa de forma optativa también en el segundo semestre.

Esta asignatura es asimismo una extensión de asignaturas relacionadas con la seguridad de la información, que encontramos en los cursos de grado en Ingeniería en Informática o Tecnologías de la información.

Entre las cualidades educativas que se pretenden alcanzar se incluye, dentro de un proceso de educación de posgrado, el ejercicio de funciones cognitivas superiores, perfeccionamiento, uso y conocimiento de herramientas y técnicas para la sociedad del conocimiento, el trabajo en equipo, el conocimiento y aplicación de algoritmos para diseñar soluciones a problemas, comprensión y gestión de la seguridad de los sistemas informáticos, la capacidad para evaluar mecanismos de certificación y tratamiento seguro de la información y el acceso a los sistemas y el conocimiento de conceptos más avanzados de computación y métodos computacionales aplicados a la ingeniería, cuya intensificación permita la participación en proyectos de ingeniería informática desde una perpectiva profesional más especializada.

3.REQUISITOS PREVIOS RECOMENDABLES

Aunque no es imprescindible es conveniente tener conocimientos avanzados de matemáticas, especialmente de aritmética modular. Es recomendable asimismo haber cursado las asignaturas obligatorias del primer semestre del master, aunque por la naturaleza de la asignatura en sí no es imprescindible. Asimismo conocimientos previos en algún lenguaje de programación orientado a objetos, como Java

4.RESULTADOS DE APRENDIZAJE

El objetivo global de la asignatura es dar una visión completa de los fundamentos de la ingeniería criptográfica. Como resultado del estudio y aprendizaje de los contenidos de

esta asignatura el alumnado será capaz de comprender las técnicas de cifrado, analizar su funcionamiento y las implicaciones más importantes de su utilización. Desarrollar proyectos de uso de las técnicas criptográficas mediante una arquitectura de seguridad criptográfica mediante algún lenguaje de programación, especialmente Java e implementar procedimientos de seguridad basadas en los algoritmos criptográficos más comunes.

Uno de los principios en los que se apoya la seguridad de redes es la protección de la información que se almacena y se transmite a través de la infraestructura en la que se apoya la red. Para realizar la protección de datos se pueden usar técnicas matemáticas propias de la criptología que difuminan la información.

Los ámbitos de utilización son muy diversos, pero toma protagonismo en especial en aquellos en los que la información es sensible: transmisión de información personal, datos bancarios, autentificación de usuarios a través de la Web, 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 para comprender el concepto de transmisión segura se hace imprescindible conocer en profundidad dichas técnicas.

Por tanto, los objetivos básicos 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 se desarrolla en base a unos conocimientos básicos del lenguaje de programación Java, ya que la realización de algunas actividades prácticas se realizará usando Java Cryptography Architecture.

Los objetivos específicos de la asignatura consisten en:

- Comprender las técnicas básicas sobre los procedimientos de difuminación de la información mediante cifrado mediante una revisión histórica de los diferentes métodos empleados hasta nuestro tiempo.
- Analizar el funcionamiento de los algoritmos de secreto compartido (clave privada) y las implicaciones más importantes de su utilización como por ejemplo la distribución segura de la clave compartida.
- Comprender y describir en profundidad algoritmos tan extendidos como DES, IDEA o RC5.
- Conocer la arquitectura de cifrado público y las bases de la teoría de números, en la cual se apoya la criptografía de clave compartida.
- Entender el funcionamiento de los algoritmos 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 algoritmos criptográficos de clave pública como RSA o El Gamal.
- Interpretar y analizar el concepto de función de resumen (Hash) para la generación de información única para la validación de la información firmada digitalmente.
- Conocer los ámbitos más extendidos de aplicación de las técnicas criptográficas en áreas de negocio como la Web (protocolos seguros: SSL o SSH), el correo electrónico (PGP o PEM) o el comercio electrónico (SET).
- Desarrollar proyectos de uso de las técnicas criptográficas mediante la arquitectura de seguridad criptográfica de Java e implementar procedimientos de seguridad basadas en los algoritmos criptográficos más comunes.

5.CONTENIDOS DE LA ASIGNATURA

Los contenidos de la asignatura de distribuyen en los siguientes contenidos temáticos o módulos.

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

La metodología de estudio utiliza la tecnología de formación a distancia en aulas virtuales, con la participación del Equipo Docente y el alumnado matriculado. En este entorno se trabajaran los contenidos teórico-prácticos cuya herramienta fundamental de comunicación será el curso virtual, utilizando la bibliografía básica y el material complementario.

El trabajo autónomo de estudio, junto con las actividades de ejercicios prácticos y cuestionarios tipo test disponibles bajo la supervisión del equipo docente.

8.BIBLIOGRAFÍA BÁSICA

Comentarios y anexos:

En esta asignatura se ha elegido el texto básico recomendado: Técnicas Criptográficas de Protección de Datos. 3ª Edición actualizada. FÚSTER, A. y Otros, Editorial RA-MA, 2004

Asimismo se proporcionarán unos guiones de apoyo elaborados por el equipo docente que se distribuye de forma gratuita por lo que no redunda en ningún tipo de perjuicio económico extra para el alumno, así como material disponible en Internet también de carácter abierto.

El primer libro se adapta al contenido de los temas teóricos mientras que los guiones proporcionados y recomendados en el entorno corresponden más a la parte práctica de la asignatura.

Adicionalmente, mediante la utilización de los medios telemáticos necesarios (web, e-mail, etc.) se le proporcionará al alumno realimentación sobre información relevante de la asignatura que, dada la naturaleza de la misma, complementará la formación del alumnado.

9.BIBLIOGRAFÍA COMPLEMENTARIA

Comentarios y anexos:

La bibliografía complementaria siguiente cubre en su conjunto gran parte de los contenidos de la asignatura, algunos de los cuales se referencian porque están disponibles online (ver licencias de uso en su caso, el Handbook es de uso personal por cortesía de la Editorial CRC). El alumnado puede consultarla con el fin de aclarar o extender los conocimientos que debe adquirir a lo largo del curso, y más en concreto en lo concerniente a las herramientas de software libre disponibles para la realización de las actividades prácticas.

Robert M. Gray. “Entropy and Information Theory”. First Edition (1991), Corrected (2013). [Disponible online] http://www-ee.stanford.edu/~gray/it.pdf [Accedido 2013].

Nigel Smart. “Cryptography: An Introduction”. 3rd Edition. 2008. [Disponible online] http://www.cs.bris.ac.uk/~nigel/Crypto_Book. [Accedido 2013]

A. Menezes, P. van Oorschot, S. Vanstone. “Handbook of cryptography”. 1997. [Disponible online] http://www.cacr.math.uwaterloo.ca/hac. [Accedido 2013]

Bruce Schneier. “Applied Cryptography”, 2ª Edición. 1996. [Disponible online] http://www.schneier.com/book-applied-toc.html [Accedido 2013]

Libro impreso: Fuster y otros; “Técnicas criptográficas de protección de datos”, 3ª Edición, de (2004).

Libro impreso: Castro Gil, Manuel Alonso; Mur Pérez, Francisco ; Peire Arroba, Juan ; Díaz Orueta, Gabriel. “Seguridad en las comunicaciones y en la información”. 1ª Ed. Editorial UNED.

Pastor, J.; Sarasa, M. A.: CRIPTOGRAFIA DIGITAL. Fundamentos y aplicaciones, Editorial Prensas 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 Science Publications, Clarendon Press, Oxford (1989).

Robling Denning D.E.: Cryptography and Data Security. Addison-Wesley PublishingCompany (1988

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

Como materiales adicionales para el estudio de la asignatura se ofrece en el curso virtual:

- Esta guía y el plan didáctico de estudio de la asignatura.
- Distintos libros electrónicos gratuitos, algunos interactivos.
- Material desarrollado exprofeso para el curso por el equipo docente
- Apartado de noticias y enlaces interesantes, relacionados con el desarrollo de la asignatura.
- Pruebas prácticas y cuestionarios teóricos de evaluación a distancia.
- Enunciados y soluciones de ejercicios teórico-prácticos que el alumno puede usar como ejercicios de autoevaluación.
- Foros de comunicación con los compañeros y el equipo docente.

11.TUTORIZACIÓN Y SEGUIMIENTO

La enseñanza a distancia utilizada para el seguimiento de esta asignatura, que garantiza la ayuda al alumnado disponer de los siguientes recursos:

- Entorno Virtual. A través de la plataforma de la UNED el equipo docente de la asignatura pondrá a disposición de los alumnos diverso material de apoyo al estudio, así como el enunciado del trabajo practico-teórico a distancia.
- Foros de discusión donde los alumnos podrán plantear sus dudas para que sean respondidas por el profesorado de tutoría o por el propio equipo docente. Este recurso es el SOPORTE FUNDAMENTAL de la asignatura, y supone la principal herramienta de comunicación entre equipo docente, personal tutor y alumnado, así como éstos entre sí.
- Tutorías con el equipo docente: los lunes de 15:00 a 19:00 h para el periodo durante el que se desarrolla la asignatura, en el teléfono 913988909 o presencialmente. También en cualquier momento del curso por correo electrónico a jscano@scc.uned.es o en el entorno virtual.

12.EVALUACIÓN DE LOS APRENDIZAJES

En esta asignatura se utilizan las modalidades de evaluación continua, pruebas de evaluación a distancia y evaluación final, según se expone a continuación.

- Evaluación continúa: En esta asignatura se plantea a los alumnos un proceso de autoevaluación, basado en la realización de cuestionarios de test. En el módulo de contenidos dentro del entorno virtual (ALF) de la UNED el alumnado podrán autoevaluar sus conocimientos.
- Pruebas prácticas de evaluación a distancia: En el entorno virtual de la UNED se encontrará pruebas prácticas que serán evaluadas por profesorado. Consistirán en pequeños trabajos prácticos principalmente y algún pequeño desarrollo en Java que permitirán comprobar la correcta asimilación de contenidos y la adquisición real de los conocimientos.
- Evaluación final de la asignatura que se llevará a cabo mediante un examen teórico-práctico, que es necesario aprobar para la superación de la asignatura.

13.COLABORADORES DOCENTES

- JESUS SALVADOR CANO CARRILLO