17-18

MÁSTER UNIVERSITARIO EN COMUNICACIÓN, REDES Y GESTIÓN DE CONTENIDOS

GUÍA DE ESTUDIO PÚBLICA

CRIPTOGRAFÍA APLICADA

CÓDIGO 3110205-

UNED

Ámbito: GUI - La autenticidad, validez e integridad de este documento puede ser verificada mediante el "Código Seguro de Verificación (CSV)" en la dirección https://sede.uned.es/valida/
C389B10ACFD9421D2B01E34E1906811C

17-18

CRIPTOGRAFÍA APLICADA

CÓDIGO 3110205-

ÍNDICE

PRESENTACIÓN Y CONTEXTUALIZACIÓN

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

EQUIPO DOCENTE

HORARIO DE ATENCIÓN AL ESTUDIANTE

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

RESULTADOS DE APRENDIZAJE

CONTENIDOS

METODOLOGÍA

SISTEMA DE EVALUACIÓN

BIBLIOGRAFÍA BÁSICA

BIBLIOGRAFÍA COMPLEMENTARIA

RECURSOS DE APOYO Y WEBGRAFÍA

Ámbito: GUI - La autenticidad, validez e integridad de este documento puede ser verificada mediante el "Código Seguro de Verificación (CSV)" en la dirección https://sede.uned.es/valida/

C389B10ACFD9421D2B01E34E1906811C

Nombre de la asignatura	CRIPTOGRAFÍA APLICADA
Código	3110205-
Curso académico	2017/2018
Títulos en que se imparte	MÁSTER UNIVERSITARIO EN COMUNICACIÓN, REDES Y GESTIÓN DE CONTENIDOS
Tipo	CONTENIDOS
Nº ETCS	10
Horas	250.0
Periodo	SEMESTRE 2
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

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.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

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

EQUIPO DOCENTE

Nombre y Apellidos	ROBERTO HERNANDEZ BERLINCHES
Correo Electrónico	roberto@scc.uned.es
Teléfono	91398-7196
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

COLABORADORES DOCENTES EXTERNOS

Nombre y Apellidos	JESUS SALVADOR CANO CARRILLO
Correo Electrónico	jcano@scc.uned.es

Ámbito: GUI - La autenticidad, validez e integridad de este documento puede ser verificada mediante el "Código Seguro de Verificación (CSV)" en la dirección https://sede.uned.es/valida/
C389B10ACFD9421D2B01E34E1906811C

HORARIO DE ATENCIÓN AL ESTUDIANTE

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.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

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

Ámbito: GUI - La autenticidad, validez e integridad de este documento puede ser verificada mediante el "Código Seguro de Verificación (CSV)" en la dirección https://sede.uned.es/valida/
C389B10ACFD9421D2B01E34E1906811C

•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.

CONTENIDOS

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.

Ámbito: GUI - La autenticidad, validez e integridad de este documento puede ser verificada mediante el "Código Seguro de Verificación (CSV)" en la dirección https://sede.uned.es/valida/
C389B10ACFD9421D2B01E34E1906811C

SISTEMA DE EVALUACIÓN

BIBLIOGRAFÍA BÁSICA

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.

BIBLIOGRAFÍA COMPLEMENTARIA

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.

Ámbito: GUI - La autenticidad, validez e integridad de este documento puede ser verificada mediante el "Código Seguro de Verificación (CSV)" en la dirección https://sede.uned.es/valida/
C389B10ACFD9421D2B01E34E1906811C

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).

RECURSOS DE APOYO Y WEBGRAFÍA

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.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no hayan sido sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.

Ámbito: GUI - La autenticidad, validez e integridad de este documento puede ser verificada mediante el "Código Seguro de Verificación (CSV)" en la dirección https://sede.uned.es/valida/
C389B10ACFD9421D2B01E34E1906811C