CRIPTOGRAFÍA

Horas: 67.5
Horas/sem: 4.5
Créditos: 9

DESCRIPCIÓN DE LA ASIGNATURA:

En la actualidad es cada vez más común que instituciones bancarias, comerciales, gubernamentales, educativas, etc. se comuniquen y realicen transacciones a través de la internet o medios de transmisión inseguros. La información que viaja por éstos medios es en muchas ocasiones de carácter confidencial, y por lo tanto necesita ser protegida contra el acceso de personas o entidades no autorizadas. Para ello, se tienen un conjunto de herramientas y mecanismos que conforman la *seguridad computacional* o seguridad *informática*. La *criptografía* es de los más importantes mecanismos para este propósito.

La palabra criptografía viene del griego *kryptos* (ocultar) y *graphos* (escritura), es decir, significa ocultar la escritura. En un principio era considerada como un arte, sin embargo al evolucionar y basar sus conceptos en diversas ramas de las matemáticas como la teoría de números, el álgebra, la probabilidad y la estadística, entre otras, y posteriormente en las ciencias de la computación, se ha constituido como una ciencia. Actualmente, ésta ciencia juega un papel de suma importancia en la protección de la información garantizando su privacidad, integridad, autenticidad y no repudio, refiriéndose esto último a que una entidad no puede negar la autoría de sus mensajes.

Desde el nacimiento de la criptografía de llave pública, números sistemas criptográficos basados en este esquema han sido propuestos. Cada uno de dichos sistemas basa su seguridad en un problema matemático. Ninguno de éstos ha sido probado a ser invencible (difícil de resolver es a veces suficiente). Sin embargo, ellos se creen totalmente seguros porque años de estudio intenso liderados por las matemáticas y la computación han fallado en hallar algoritmos eficientes para resolverlos, así que en la práctica, ellos se mantienen intocables por la tecnología computacional actual.

Las curvas elípticas son construcciones matemáticas que han sido estudiadas desde el siglo 17. Concretamente, en 1985, Neal Koblitz y Victor Miller de manera independiente propusieron criptosistemas de llave pública usando un grupo de puntos sobre una curva elíptica y así fue como la criptografía sobre curvas elípticas (ECC) nació. Desde entonces, un área de investigación es encontrar técnicas para su implementación. La ECC permite reducciones en las llaves y en los tamaños de los certificados lo cual representa reducciones de costos bastante significativos. Esto significa que los criptosistemas de llave pública pueden ofrecer un alto rendimiento y bajo costo.

OBJETIVO:

Estudiar los principales métodos, algoritmos, técnicas y herramientas necesarias para la implementación de aplicaciones criptográficas y de seguridad de datos. Resolver eficientemente el problema de cómo establecer una comunicación segura entre dos o más entidades de manera tal que se garantice un alto grado de confidencialidad, integridad y

autenticidad en los datos y documentos intercambiados. Implementar algoritmos y esquemas criptográficos para resolver problemas prácticos en el envío de datos y comunicación de manera segura.

CONTENIDO:

1. Visión general de la Criptografía y sus aplicaciones.
   1.1. Antecedentes Históricos.
   1.2. Comunicaciones seguras.
   1.3. Aplicaciones Criptográficas.

2. Fundamentos teóricos de la Criptografía.
   2.1. Divisibilidad y máximo común divisor.
   2.2. Aritmética modular.
   2.3. El Teorema Chino del Resto.
   2.4. Exponenciación Modular.
   2.5. La fórmula de Euler.
   2.6. Invirtiendo matrices mód *n*
   2.7. Fracciones continuas.
   2.8. Protocolo de tres pasos.

3. Cifrados Clásicos.
   3.1. Cifrado por desplazamiento.
   3.2. Cifrados Afines.
   3.3. El Cifrado Vigenère.
   3.4. Permutaciones.
   3.5. El cifrado de sustitución.
   3.6. Cifrados de bloques.
   3.7. Libreta de un solo uso.
   3.8. Registros de desplazamiento con retroalimentación lineal.
   3.9. Máquinas de rotores. La Máquina ENIGMA.

4. Cifrados Simétricos Modernos.
   4.1. Redes Feistel.
   4.2. Data Encryption Standard (DES).
   4.3. Seguridad por contraseña.
   4.4. El algoritmo IDEA.
   4.5. Rijndael: The Advance Encryption Standard (AES).
   4.6. Representación algebraica del AES.
   4.7. Criptoanálisis de Algoritmos Simétricos.

5. Logaritmos Discretos y Diffie-Hellman.
   5.1. El problema del logaritmo discreto.
   5.2. El intercambio de llaves Diffie-Hellman.
   5.3. El criptosistema de llave pública de ElGamal.
   5.4. Un pequeño resumen de teoría de grupos.
   5.5. Qué tan difícil es el problema del logaritmo discreto?
   5.6. Un algoritmo de colisión para el problema de logaritmo discreto.

6. Factorización entera y el algoritmo RSA.
   6.1. El criptosistema de llave pública RSA.
   6.2. Implementación y seguridad.
   6.3. Pruebas de primalidad. La prueba de Miller-Rabin.
   6.4. El algoritmo de factorización *p−1* de Pollard.
   6.5. Residuos cuadráticos y reciprocidad cuadrática.
   6.6. Cifrado probabilístico. El criptosistema de Goldwasser-Micali.

7. Curvas Elípticas y Criptografía.
   7.1. Curvas elípticas.
   7.2. Curvas elípticas sobre campos finitos.
   7.3. El problema del logaritmo discreto elíptico.
   7.4. Criptografía sobre curvas elípticas.
   7.5. El algoritmo de Lenstra.
   7.6. Curvas elípticas sobre $\mathbb{F}_2$ y $\mathbb{F}_{2^k}$.
   7.7. Emparejamientos bilineales sobre curvas elípticas.
   7.8. El emparejamiento de Weil sobre campos de orden potencias de primos.
   7.9. Aplicaciones del emparejamiento de Weil.

ESTRATEGIAS DE ENSEÑANZA:
Conferencia, interrogatorio, lluvia de ideas, resolución de ejercicios, demostraciones.

CRITERIOS DE EVALUACIÓN:
3 Exámenes parciales: 60 %
Tareas: 20 %
Proyecto Final: 20 %

BIBLIOGRAFÍA:
1. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. 2014. *An Introduction to Mathematical Cryptography* (2nd ed.). Springer Publishing Company, Incorporated.
2. Wade Trappe and Lawrence C. Washington. 2005. *Introduction to Cryptography with Coding Theory (2nd Edition)*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA.
3. Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone. 2010. *Guide to Elliptic Curve Cryptography* (1st ed.). Springer Publishing Company, Incorporated.
4. Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. 1996. *Handbook of Applied Cryptography* (1st ed.). CRC Press, Inc., Boca Raton, FL, USA.
5. *Elementary Number Theory and its applications*, Fourth Edition, K. Rosen, AT&T Bell Laboratories, 2000.
6. Jorge Ramió Aguirre, *Seguridad Informática y Criptografía*, Tercera edición 3.1 2003, disponible en: http://www.criptored.upm.es.

7. Koblitz, N. (2001). *Cryptography. Mathematics Unlimited - 2001 and Beyond*, Págs. 749-769. doi: 10.1007/978-3-642-56478-9_9
8. Koblitz, N. (Ed.). (1996). Advances in Cryptology CRYPTO '96. Lecture Notes in Computer Science. doi: 10.1007/3-540-68697-5
9. Koblitz, N. (1987). A Course in Number Theory and Cryptography. Graduate Texts in Mathematics. doi:10.1007/978-1-4684-0310-7
10. Oded Goldreich. 2006-2009. *Foundations of Cryptography: Volume 1 and 2*. Cambridge University Press, New York, NY, USA.

PERFIL PROFESIOGRÁFICO:

Licenciado en matemáticas, preferentemente con posgrado, y experiencia docente, de investigación o trabajo en el área.

Elaboración: Dr. Víctor Manuel Bautista Ancona.
Fecha de elaboración: Agosto, 2012.
Actualización: Agosto, 2017.