Currículum Vitae

Nombre: **José de Jesús Angel Angel**
Fecha de nacimiento: 24 diciembre 1964
Teléfono: 57305538
Celular: 04455 17306307
Email: jjaa@math.com.mx

Maestría en Matemáticas de la **UAM** Iztapalapa, título y cédula profesional 4990264.
Tesis: Criptografía y Curvas Elípticas.

Licenciatura en Física y Matemáticas de la **ESFM del IPN,** título y cédula profesional 1703950.
Tesis: Una introducción a los anillos de funciones continuas.

Doctorado 100% créditos, examen predoctoral aprobado **CINVESTAV del IPN**.

Temas de interés: BlockChains, criptografía de clave pública, criptografía post-cuántica, criptografía elíptica, criptografía bilineal, seguridad Informática, criptoanálisis, historia de la criptografía en México, matemáticas aplicadas, matemáticas aplicadas en la industria, matemáticas aplicadas en la lucha contra el crimen organizado.

Curso en línea: criptografía I, impartido por Dan Boneh, Stanford University.

https://www.coursera.org/account/accomplishments/verify/3CUQNS9NJZJU

Habilidades técnicas: domino las principales técnicas de la seguridad de la información, particularmente:

1.- BlockChains.
2.- Diseño e implementación de algoritmos criptográficos simétricos y asimétricos.
3.- Planeación, diseño y administración de sistemas de seguridad de la información.
4.- Mecanismos de control de acceso.
5.- Mecanismos de seguridad en la transmisión de la información.
6.- Mecanismos en la autenticación de entidades.
7.- Mecanismos en la verificación de identidades.
8.- Mecanismos en la verificación de la integridad de la información.
9.- Mecanismos de firma digital.
10.- Aspectos generales de la seguridad de sistemas operativos, de redes, seguridad en Internet.
11.- Protocolos de seguridad, como: SSL,TLS, SSH, WAP, WEP, IPsec, VoIP.

12.- Ataques a los protocolos de seguridad.
13.- Estándares criptográficos como: IEEE P1363 Standard Specifications For Public-Key Cryptography, ISO, NIST, etc.
14.-Herramientas de seguridad comunes como AntiVirus y FireWalls.
15.- Lenguaje de programación: ANSI C, html. Python, C++, Mathematica, PHP, CSS, Delphi. Paqueteria office. SO Windows y GNU Linux.
16.- LaTeX, Scientific Word Place.

Habilidades personales:

1.- Puntualidad.
2.- Capacidad de abstracción.
3.- Solución de problemas.
4.- Innovación.
5.- Discreción.

Experiencia laboral:

De enero del 2007 a la actualidad, soy profesor por horas en la facultad de Ingeniería de la **Universidad Anáhuac Norte.** Impartiendo más de 70 cursos de las materias: Algebra Lineal, Cálculo Diferencial, Matemáticas Discretas, Métodos Numéricos, Cálculo Vectorial, Ecuaciones Diferenciales, Programación básica. He impartido cursos de Seguridad Informática y Mathematica al personal docente.

De agosto del 2016 a mayo de 2017 fui profesor de Métodos Cuantitativos en el **ITESM CEM**.

Soy colaborador de la empresa **IM Networks, S. A, de C.V**. para apoyarlos en la consultoría de desarrollar e implementar sistema de seguridad que combinen la criptografía de clave pública con la criptografía cuántica y otras técnicas, hasta 2011.

En abril de 2011 impartí curso de capacitación al centro de evaluación de la **SEDENA** sobre la implementación de una PKI con curvas elípticas. En este caso participe como asesor del grupo encargado del centro de evaluación para conocer las bases matemáticas teóricas de la criptografía basada en curvas elípticas, posteriormente se configuraron sus servidores para que sus comunicaciones puedan ser hechas con el protocolo htpps usando certificados digitales que contienen algoritmos basados en curvas elípticas como lo describen los estándares de NIST (The National Institute of Standards and Technology).

De julio del 2007 a la actualidad, administro el sitio www.math.com.mx.

De septiembre del 2006 a diciembre de 2006 fui profesor de matemáticas en la **Universidad Tecnológica de México** campus Ecatepec.

De julio de 2004 a septiembre de 2004, impartí capacitación de Algoritmos Criptográficos usados en VoIP al Departamento de Investigación y Desarrollo de la Dirección General de Transmisiones Militares de la **SEDENA.** En esta ocasión impartí la actualización básica y necesaria para poder entender el protocolo de comunicación por internet VoIP, además de protegerlo agregando las capas de IPsec encriptadas.

De enero. de 1998 a febrero. de 2004
De julio de 2002 a agosto de 2002, impartí capacitación de Algoritmos Criptográficos con certificados digitales y PKI al Departamento de Investigación y Desarrollo de la Dirección General de Transmisiones Militares de la **SEDENA.** En este proyecto trabajamos las bases matemáticas de los algoritmos tanto de clave pública (RSA, DH, DSA) como privada (AES, DES, HMAC), desarrollamos paso a paso como trabajan estos algoritmos en código ANSI C.

Director de Investigación y Desarrollo de **SeguriDATA S.A. de C.V**. En esta empresa principalmente se desarrollan soluciones de usuarios de seguridad usando certificados digitales. Apegada a los estándares internacionales, también encargado de los cursos que imparte la empresa y que ha tenido como asistentes a gente de: Banamex, SECOFI, Comisión Nacional del Agua, Bnexus, Secodam, SEDENA. Era el encargado de verificar que los algoritmos usados correspondan a los estándares actuales, de esto dependía que fueran seguros e interoperables. Se proponían soluciones de seguridad usando algoritmos criptográficos, para la autenticación de personas y documentos, para la integridad del origen de documentos y de los propios documentos. Así como la confidencialidad de la comunicación y la información. Los algoritmos usados son RSA, DSA, DH, HMAC, DES, AES, el código era elaborado en ANSI C.

De septiembre de 2002 a enero de 2003 impartí curso en Maestría, de Criptografía en el IIMAS de la UNAM.

De septiembre de 1997 a enero de 1998
Impartí cursos de Estructura de Datos en la ESIME

De septiembre de 1993 a agosto de 1997
Impartí cursos de Estadística I, II y II, Matemáticas para la Administración en CSH, Cálculo Diferencial e Integral de CBI, Bioestadística I y II de CBS, en la UAMI

De septiembre de 1993 a julio de 1995
Impartí cursos de Lógica, Estadística, Cálculo Integral y Diferencial y Matemáticas Financieras en la Facultad de Contaduría de la UNAM

De septiembre de 1992 a febrero de 1993
Impartí curso de Física en la Unidad de Biotecnología del IPN

De septiembre de 1991 a agosto de 1992
Impartí cursos de Introducción a la Variable Compleja, Bioestadística y Cálculo de Varias Variables en el Tecnológico de Ecatepec.

De septiembre de 1989 a diciembre de 1991
Impartí cursos de ayudantía en Cálculo Diferencial e Integral en la UAM

De noviembre de 19 86 a abril de 1988
Impartí cursos de programación en DBIII+, Lotus, Basic, pascal y Análisis de sistemas de información.

Participaciones

Invitado por La revista FIGURAS, **para la dictaminación de artículo de investigación sobre criptografía,** Facultad de estudios superiores de Acatlán UNAM.

Invitado por el Instituto de Ciencia y Tecnología del D.F. , **para la dictaminación de proyectos relacionados con la criptografía,** septiembre 2010, México D.F.

Member Program Committee de la conferencia "**3rd International Workshop on Computational Intelligence in Security for Information Systems**, **CISIS 2010**" November 11th-12th, 2010 - León, Spain.

Member Program Committee de la conferencia "**Sixth International Conference on Information and Security IAS 2010**", August 23-25 2010, Atlanta USA.

Participo en la revista "**International Journal of Network Security**", como revisor técnico (reviwer).

Participo en la revista "**Gerencia Tecnológica Informática**", como parte del comité editorial.

Publicaciones Importantes

Artículo: J. Angel, **”Cómo evitar el espionaje telefónico”,** el mundo del Abogado, Año 17, num 204 , abril del año 2016, pp. 52-54.

Artículo: J. Angel, **”Qué es la National Security Agency y qué hace”,** el mundo del Abogado, Año 16, num 192 , abril del año 2015, pp. 48-49.

Artículo: J. Angel, **”Las matemáticas en la lucha contra el crimen organizado”,** el mundo del Abogado, Año 15, num 158 , junio del año 2012, pp. 32-34.

Artículo: J. Angel, **”De Turing y la criptografía”,** Casa del tiempo UAM, Número 56, junio del año 2012.

Artículo: J. Angel, **”Criptografía de Benito Juárez”,** Relatos e Historias de México, Número 31, marzo del año 2011.

Artículo: J. Angel, **”Claves secretas de la Revolución”,** Bicentenario, el ayer y hoy de México, Volumen 3, Número 10, año 2010, pp. 20-25.

Artículo: J. Angel, G. Morales, **” Solinas primes of small weight for fixed sizes”,** Cryptology ePrint Archive: Report 2010/058.

Artículo: J. Angel, G. Morales, **”Cryptographic methods during the Mexican Revolution”,** Cryptologia, 33:1–8, 2009

Beca con arbitraje ganada de feb. 2009 a nov. 2009, otorgada po r el INEHRM, con el proyecto “**Métodos criptográficos usados en el periodo de la Revolución Mexicana**.”
http://www.inehrm.gob.mx/Portal/PtMain.php?pagina=becas

Conferencia: J. Angel, G. Morales, **"Linear and multilinear forms in Chryptography** ", ALTENCOA3-2008, Bucaramanga, julio 21-25 de 2008, Escuela de Matemáticas
Universidad Industrial de Santander – Bucaramanga, Colombia.

Artículo: J. Angel, G. Morales, "**Searching prime numbers with short binary signed representations**", Special Issue on Applied Cryptography & Data Security, Journal of “Computacion y Sistemas” ISSN 1405-5546 National Polytechnical Institute of Mexico Special Issue on January-March, 2009.

Artículo: J. Angel, G. Morales, “**Cifrado basado en la identidad con tarjetas de circuito integrado”** Luis Javier García Villalba (editor), Actas del XXIII Simposium Nacional de la Unión Científica Internacional de Radio. URSI 2008, Universidad Complutense de Madrid, Madrid, España, (en disco compacto) I.S.B.N.: 978-84-612-6291-5, septiembre de 2008.

Artículo: J. Angel, G. Morales, "**Observaciones sobre la Distribución de Primos con Representaciones Binarias Signadas Cortas**", Actas de la X RECSI (X Spanish Meeting on Cryptology and Information Security), September 2-5, 2008, Salamanca, SPAIN.

Artículo: J. Angel, G. Morales, "**Criptografía en el Porfirismo**",

CIENCIA y DESARROLLO, Conacyt, Vol 34, mayo 2008.

Artículo: J. Angel, G. Morales, "**El algoritmo de Agrawal, Kayal y Saxena para decidir primalidad**", Carta Informativa SMM (Sociedad Matemática Mexicana), No. 55, enero 2008.

Artículo: J. Angel, G. Morales, **"Breve descripción de la criptografía en la Revolución Mexicana"** Revista Digital Universitaria, Vol 9 No. 3. http://www.revista.unam.mx/vol.9/num3/art18/int18.htm, http://www.revista.unam.mx/vol.9/num3/art18/art18.pdf, Marzo 2008.

Artículo: J. Angel, G. Morales,"**Criptografía en la Revolución Mexicana**", disponible en línea en www.virusprot.com, diciembre 2007.

Libro : J. Angel, G. Morales,"**Historia de la Criptografía en México**", en preparación CINVESTAV 2008.

Artículo: J. Angel, G. Morales, "**La hipótesis de Riemann y Primalidad**", Carta Informativa SMM(Sociedad Matemática Mexicana), No. 53, julio 2007.

Código: **Elliptic Curve Diffie-Hellman key agreement scheme,** Wolfram Library Archive: http://library.wolfram.com/infocenter/MathSource/6575/

Código: **DSA Scheme using elliptic curves over a prime field,** Wolfram Library Archive: http://library.wolfram.com/infocenter/MathSource/6727/

J. Angel, G. Morales, "**Counting Prime Numbers with Short Binary Signed Representation**", accepted in the "Symposium on Algebraic Geometry and its Applications", Tahiti, May 2007.

Participe en el "**Summer School on Computational Number Theory and Applications to Cryptography**" June 19-July 7, 2006, Laramie, University of Wyoming**.**

Conferencia: "**Computation of secure Pairing for Identity Based Encryption**", XXXVIII congreso de la SMM, J.J. Angel, G. Morales , octubre 2005.

Libro: **"AES para principiantes"**: Angel J.J., enero 2005.

Artículo: **"Breve Reseña Sobre la Hipótesis de Riemann, Primalidad, y el algoritmo AKS"**: Angel J.J., Morales G., junio 2005

Artículo: **"On the Computation of the Tate Pairing for Elliptic Curves over Fields of Large Characteristic"**: Angel J.J., Morales G., Sep. 2005, Tercer congreso Iberoamericano de Seguridad Informática (CIBSI-05) Valparaíso Chile, noviembre 2005.

Artículo: **"Counting Prime Numbers with Short Binary Signed Representation"**, Cryptology ePrint Archive: Report 2006/121, Angel J.J., Morales G., Mar. 2006

Esta publicado un programa tutorial de AES (Advanced Encryption Standard) en la pagina de Vincent R. www.esat.kuleuven.ac.be/~rijmen/rijndael.

Escribí el libro: "Criptografía para principiantes", disponible en línea.

Publique un artículo de divulgación en la revista G.A.U.S.S. de la facultad de ciencias de la computación de la Universidad de Puebla, marzo de 1996
Nombre: "**Aspecto Elementales de la Criptografía**"

Menciones en revistas y periódicos de circulación nacional:

Mención: "**Revista Proceso 1514** " del 6 de noviembre de 2005. Mención de un artículo sobre la computación cuántica, página 54. Periodista Leonardo Boix.

Entrevista: "**Periódico Reforma**" del 1 de junio de 2000. Entrevista sobre las claves del Fobaproa. Periodista Jonathan Hernández.

Mención: "**Gaceta UNAM**" del 2 de febrero de 1998. Sobre una conferencia de **Dinero Electrónico**, página 11. Periodista Guadalupe Lugo y Laura Romero.

Apariciones en programas a nivel internacional:

Aparición: "Continente Nazi", documental transmitido por **History Channel**, el día 2 de agosto 2014 .

Entrevistas en radio:

Programa Agenda Pública. 660 de AM, XEDTL, La Radio de los Ciudadanos, IMER.
En el programa México y el mundo conducido por Lic. Elsa Aguilar Casas.
El día 21 de Mayo de 2009.
Tema: criptografía en la revolución mexicana.

Programa Radio UACM. 660 de AM.
Programa No 1
Tema: Algoritmos
Conduce: Ismael Ledesma

Agradecimientos:

Se me menciona como revisor técnico del libro Cálculo 1 de una variable de R. Larson, B.H. Edwards, novena edición, McGrawHill 2010.

Se me menciona en la lista de agradecimientos del libro: **Mathematics of Public Key Cryptography** de **Steven Galbraith.**

Cursos tomados cortos sobre enseñanza:

Taller de habilidades docentes, microenseñanza, junio 2007, Universidad Anáhuac.
Seminario de metodologías didácticas, septiembre 2007, Universidad Anáhuac.
Aprendizaje significativo, julio 2009, Universidad Anáhuac.
Métodos de enseñanza, junio 2010. Universidad Anáhuac.
Introducción a la didáctica por competencias y su evaluación, julio 2010. Universidad Anáhuac.

Cursos y talleres Impartidos:

Impartí curso de **Introducción a Mathematica**, abril 2015, impartido en la Universidad Anáhuac al personal académico.

Impartí taller de **Password Cracking**, noviembre 2014, impartido en IX congreso internacional de informática, organizado por Centro Nacional de Capacitación Universitaria en Manzanillo Colima.

Impartí curso de **Introducción a la seguridad Informática**, junio 2014, impartido en la Universidad Anáhuac al personal académico.

Impartí curso de criptografía básica en el XL congreso de la
Sociedad Matemática Mexicana, Monterrey octubre 2007.
Nombre: **Criptografía Básica**.

Impartí curso tutorial en Apizaco Tlaxcala, con el nombre "**Criptografía Básica**" (2004).

Impartí seminario "**Seminario de Seguridad por VirusProt** " en Madrid, España, febrero de 2003.

Impartí curso "Congreso de la SMM " en Durango octubre 2002.
Nombre: **Matemáticas en la seguridad de la información**.

Impartí curso en el "CONESCAPAN XX", en San José Costa Rica en agosto 2001.
Nombre: **Seguridad en la Transmisión de datos a través de Internet**.

Impartí Curso tutorial "**Algoritmos Criptográficos**" en la Escuela "CIMPA" en el CIMAEF de la Habana Cuba en noviembre de 2000.

Conferencias Impartidas

Impartí conferencia en XVI ANSYS Convergence México 2019, San Miguel de Allende Guanajuato, octubre 2019.
Nombre: **Las Matemáticas de la Dinámica de Fluidos Computacional**.

Impartí conferencia en Sixth International Conference on Mathematics and its Applications (6CIMA) septiembre 2019.
Nombre: **Las curvas elípticas de BitCoin**.

Impartí conferencia en Sixth International Conference on Mathematics and its Applications (6CIMA) septiembre 2019.
Nombre: **Algunas aplicaciones de BlockChains**.

Impartí conferencia en Sixth International Conference on Mathematics and its Applications (6CIMA) septiembre 2019.
Nombre: **La probabilidad en BitCoin**.

Impartí conferencia en Sixth International Conference on Mathematics and its Applications (6CIMA) septiembre 2019.
Nombre: **Aplicaciones de la lógica difusa**.

Impartí conferencia en el XIII Coloquio Nacional de Códigos, Criptografía y Áreas Relacionadas en Ciudad de México, abril 2019.
Nombre: **Blockchains y sus aplicaciones**.

Impartí conferencia en el XVI congreso de la Sociedad Matemática Mexicana, (Villahermosa) octubre 2018.
Nombre: **Criptografía en serio**.

Impartí conferencia invitada en el XVI congreso de la Sociedad Matemática Mexicana, (Villahermosa) octubre 2018.
Nombre: **Matemáticas usadas en la industria**.

Impartí conferencia en el XVI congreso de la Sociedad Matemática Mexicana, (Villahermosa) octubre 2018.
Nombre: **Dinámica de Fluidos Computacional** (complementaria a Matemáticas usadas en la industria).

Impartí conferencia Semana de la Ingeniería en la Universidad Anáhuac 2017.
Nombre: **Matemáticas usadas en la Industria.**

Impartí conferencia invitada en las XI jornadas de Modelación matemática en la Universidad Autónoma de la Ciudad de México, noviembre 2017.
Nombre: **A 40 años de la criptografía de clave pública**

Impartí conferencia en el XV congreso de la Sociedad Matemática Mexicana, octrubre 2017.
Nombre: **El uso de la dificultad de encontrar isogenias de curvas elípticas en criptografía post-cuántica.**

Impartí conferencia en el XV congreso de la Sociedad Matemática Mexicana, octrubre 2017.
Nombre: **Bitcoin, sus métodos y algoritmos.**

Impartí conferencia en el XV congreso de la Sociedad Matemática Mexicana, octrubre 2017.
Nombre: **Historia de la criptografía en México.**

Impartí conferencia en el XV congreso de la Sociedad Matemática Mexicana, octrubre 2017.
Nombre: **Matemáticas Industriales.**

Impartí conferencia en el XII Coloquio Nacional de Códigos, Criptografía y Áreas Relacionadas en Ciudad de México, junio 2017.
Nombre: **Criptografía Post-cuántica**

Impartí conferencia en el XIII Congreso Internacional de Informática, Robótica, Macatrónica, y Tecnologías organizado por CNCU (Centro Nacional de Capacitación Universitaria) en Mazatlán, octubre 2016. Nombre: **Aplicaciones de la criptografía (**Invitada**)**.

Impartí conferencia en el Congreso Internacional de Matemáticas y sus Aplicaciones, en la Benemérita Universidad Autónoma de Puebla, septiembre 2015. Nombre: **Las matemáticas en la lucha contra el crimen**.

Impartí conferencia en el Congreso Internacional de Matemáticas y sus Aplicaciones, en la Benemérita Universidad Autónoma de Puebla, septiembre 2015. Nombre: **Las matemáticas de Google**.

Impartí conferencia en el Congreso Internacional de Matemáticas y sus Aplicaciones, en la Benemérita Universidad Autónoma de Puebla, septiembre 2015. Nombre: **Las matemáticas a través de la historia en la criptografía**.

Impartí conferencia de **Historia de la Criptografía en México**, noviembre 2014, en IX congreso internacional de informática, organizado por Centro Nacional de Capacitación Universitaria en Manzanillo Colima, 1 noviembre 2014 (invitada)..

Impartí conferencia de **Cracking Passwords**, noviembre 2014, en IX congreso internacional de informática, organizado por Centro Nacional de Capacitación Universitaria en Manzanillo Colima, 31 de octubre 2014 (invitada).

Impartí conferencia en el XLVII Congreso Nacional de la Sociedad Matemática Mexicana, octubre 2014.
Nombre: **El algoritmo Dual_EC_DRBG**.

Impartí conferencia en el XLVII Congreso Nacional de la Sociedad Matemática Mexicana, octubre 2014.
Nombre: **Ataques criptográficos algebraicos**.

Impartí conferencia en el XLVII Congreso Nacional de la Sociedad Matemática Mexicana, octubre 2014.
Nombre: **Side Channel Attacks**.

Impartí conferencia en el XLV Congreso Nacional de la Sociedad Matemática Mexicana, noviembre 2012.
Nombre: **100 aplicaciones de las matemáticas**.

Impartí conferencia en el XLV Congreso Nacional de la Sociedad Matemática Mexicana, noviembre 2012.
Nombre: **Turing en la criptografía**.

Impartí conferencia en el XLIV Congreso Nacional de la Sociedad Matemática Mexicana, octubre 2011.

Nombre: **Las matemáticas usadas en la lucha contra el crimen organizado**.

Impartí conferencia en la Universidad Iberoamericana, octubre 2010.
Nombre: **Criptografía: como se aplica la matemática en la seguridad informática**.

Impartí conferencia en la Dirección de Estudios Históricos del INAH, julio 2009.
Nombre: **Criptografía usada en la época de la Revolución Mexicana**.

Impartí conferencia en el congreso de la SMM en Valle de Bravo, octubre 2008.
Nombre: **A 32 años del problema de Diffie-Hellman**.

Impartí conferencia en la semana de tecnología 2008 en el Instituto Tecnológico Superior de Irapuato, septiembre 2008.,
Nombre: **Certificados Digitales**.

Impartí conferencia en el congreso Dos Siglos de Revoluciones de México, septiembre 2008., Universidad Michoacana de San Nicolás de Hidalgo.
Nombre: **Criptografía usada en la Revolución Mexicana**.

Impartí conferencia en la Universidad del Estado de México (Ixtapa) mayo 2008.
Nombre: **Introducción a la seguridad de la información**.

Impartí conferencia y taller de criptografía en el Instituto Tecnológico Superior de Valladolid en Yucatán. mayo 2008.
Nombre: **Criptografía Moderna**.

Impartí conferencia y taller de criptografía en la Universidad Mayab en Yucatán. febrero 2008.
Nombre: **Criptografía en la Seguridad de la Información**.

Impartí conferencia en el Instituto Tecnológico Superior de Zacapoaxtla, mayo 2007.
Nombre: **Algoritmos, esquemas y protocolos criptográficos**.

Impartí conferencia en el I.S.C. Chiapas 2005.
Nombre: "**Criptografía**" (2005).

Impartí curso México D.F. en el congreso de la SMM.
Nombre **"Criptografía Básica"**. (2005)

Impartí conferencia en la semana de la seguridad del IPN, con la conferencia, "**Criptografía Basada en la Identidad**" en septiembre 2004.

Impartí conferencia "Congreso de la SMM " en Pachuca octubre 2003.
Nombre: **Firma Digital**.

Impartí conferencia en "Congreso Nacional de Tecnología" efectuado en Huancayo, Perú en marzo de 2003
Nombre: "**Comercio electrónico seguro**".

Impartí conferencia "CONCAPAN XXII " en Panamá noviembre de 2002.
Nombre: **Transacciones seguras por Internet**.

Impartí conferencia "V coloquio nacional de criptografía" en México DF julio 2002
Nombre: **Curvas elípticas y criptografía**.

Impartí conferencia "**Seguridad en la Transmisión de datos a través de internet**" en el SE2001, en Bogota Colombia septiembre 2001.

Impartí Curso en el "Congreso Nacional de Tecnología" efectuado en Lima Perú en septiembre de 1999
Nombre: "**Seguridad en Internet y aplicaciones de la criptografía**".

Impartí conferencia en “Congreso Nacional de Tecnología” efectuado en Lima Perú en septiembre de 1999
Nombre: “**Seguridad en Internet**”.

Impartí conferencia en Congreso General de Cómputo 99 en la UNAM noviembre de 1999
Nombre: “**Firma Digital**”.

Impartí conferencia en el tercer coloquio de Codigos y Criptografía UAMI, julio de 1999
Nombre: “**Ataques a los sistemas RSA y CCE**”.

Impartí conferencia en “Vinculación en sistemas Distribuidos” efectuado en México DF en mayo de 1999
Nombre: “**Factorización en paralelo**”.

Impartí dos conferencias en Congreso General de Cómputo 98 en la UNAM noviembre de 1998
Nombre: “**Criptosistemas Elípticos e Hiperelípticos**”.
Nombre: “**Criptografía Moderna**”.

Impartí conferencia en la VII semana de las Matemáticas en la UAMI del 5 al 9 de octubre
Nombre: “**Criptografía de llave Pública**”.

Impartí conferencia en el Simposio Seguridad en Cómputo Disc 97, diciembre 1997 en la UNAM
Nombre: “**Dinero Electrónico**”.

Impartí conferencia en el Segundo Simposio de Códigos y Criptografía en la UNAM en 1998
Nombre: “**RSA vs CCE**”.

Impartí dos conferencias en el XXX Congreso Nacional de la Sociedad Matemática, en Aguascalientes Ags. del 28 septiembre al 4 de octubre.
Nombre: “**La Criba de Campos Numéricos y Criptografía**”
Nombre: “**Como Funciona el Dinero Electrónico**”.

Impartí conferencia en el primer Coloquio Nacional de Códigos y Criptografía, en la UAMI el 9 de mayo de 1997
Nombre: “**Aspectos Generales Sobre la Seguridad en la Transmisión de la Información usando Curvas Elípticas**”.

Impartí conferencia en la Escuela Militar de Transmisiones, el 8 de junio de 1996
Nombre: “**Criptografía Aplicada**”.

Impartí conferencia en el XXIX Congreso de la Sociedad Matemática Mexicana, en San Luis Potosí, octubre de 1996
Nombre: “**Algunos Grupos y el Problema del Logaritmo Discreto**”.

Impartí dos conferencias en el 2° encuentro Internacional Sobre la Enseñanza y Aplicaciones de la Matemáticas, organizado por el ITESM campus Guadalajara, del 10 al 12 de abril de 1997
Nombre: “**Matemáticas en las comunicaciones**”
Nombre: “**La obtención de algunos límites de forma rápida**”.

Impartí conferencia en el CINVESTAV en el Seminario de Investigación en Temas Avanzados de Combinatoria y sus Aplicaciones el 29 de junio de 1995
Nombre: “**Curvas Elípticas y Criptografía**”.

Impartí conferencia en el XXVIII Congreso Nacional de la Sociedad Matemática, en Colima Colima, Realizado del 1 al 7 de octubre de 1995
Nombre: “**Matemáticas y Criptografía**”.

Actividades Académicas de Apoyo

Fui Director de Tesis del Capitán Heriberto Hernández Juárez, de la Escuela Militar de Ingenieros Militares,
Nombre: "**Diseño de Un Dispositivo que Proporcione Seguridad Criptográfica a la Red Telefónica Militar**", 2001

Fui Director de Tesis del Capitán Raúl Cristobal Hernández, de la Escuela Militar de Transmisiones para obtener el titulo de Ingeniero en Transmisiones Militares,
Nombre: "**Análisis y desarrollo de un algoritmo para cifrado de llave privada tipo RC-5**"
(con mención honorífica), 1998

Fui Director de Tesis del Capitán Filiberto Mendoza García, de la Escuela Militar de transmisiones para obtener el titulo de Ingeniero en Transmisiones Militares,
Nombre: "**Una solución al problema de intercambio de claves privadas y firma digital, utilizando el sistema de cifrado de clave pública del tipo RSA**", 1998

Otras Actividades Importantes

Obtuve la medalla al Mérito Universitario de la UAMI, noviembre 1998

Asistencia al Workshop ECC'98 (Eliptic Curve Cryptosystems) en Waterloo University, sep1998

Asistencia a the Mathematics of Public-Key Cryptography en The Fields Institute of Toronto Jun. 1999

Forme parte del comité que organizó el ciclo CRIPTOGRAFÍA 99, conjuntamente con la Dirección General de Registro Mercantil y Correduría de SECOFI y el Depto. De Matemáticas de la UAMI.