Class4crypt

Videoclases de criptografía aplicada

Clase c4c0.1
Presentación

Madrid, 28 de enero de 2020

Profesor Dr. Jorge Ramió A.

Agenda

- Introducción al proyecto Class4crypt
- Documentación, software educativo de prácticas y material multimedia de apoyo a las videoclases
- Documentación recomendada
- Temario detallado y tentativo de las lecciones
- Cómo seguir estas videoclases
- Licencia y créditos

¿Qué es el proyecto Class4crypt? (1/4)

- Más de una centena de videoclases de criptografía aplicada, que se publicarán una por semana en mi canal YouTube personal
- Resumen de los 25 años de clases y conferencias que el autor ha impartido desde el año 1994 sobre esta temática en:
  - Media docena de universidades en España: grado y posgrado
  - Más de 20 universidades en países de Latinoamérica: posgrado, especialización, cursos y conferencias:
    - Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, México, Panamá, Perú, República Dominicana, Uruguay y Venezuela
- Donde se usará documentación y software de desarrollo propio

¿Qué es el proyecto Class4crypt? (2/4)

- Se tomará como una primera referencia las diapositivas del Libro Electrónico de Seguridad Informática y Criptografía, publicado en Internet en 2006, con 200.000 descargas al 31/12/19
  - URL: http://www.criptored.upm.es/guiateoria/gt_m001a.htm
- Además, el libro Curso de Criptografía Aplicada, publicado en Internet en 2018, con 10.000 descargas al 31/12/19
  - URL: http://www.criptored.upm.es/guiateoria/gt_m001s1.htm
- Y las actualizaciones y ampliaciones realizadas a la documentación de la Certificación CriptoCert Certified Crypto Analyst, en 2019
  - URL: https://www.criptocert.com/PDF/CriptoCert_Analyst_Temario.pdf

¿Qué es el proyecto Class4crypt? (3/4)

- En dichas videoclases se añadirán estos complementos prácticos formativos:
  - Prácticas con software educativo de creación propia:
    - SAMCript, Criptoclásicos v2.1, FlujoLab, safeDES, AESPhere v2.1, CriptoRES, genRSA v2.1, LegionRSA, RingRSA
  - Prácticas con otro software libre:
    - msieve153, OpenSSL, HashCalc
  - Prácticas con software online (AEE, PLD)
  - Cuadernos de prácticas de Criptografía CLCript (Mayo 2018) http://www.criptored.upm.es/software/sw_m001s.htm

¿Qué es el proyecto Class4crypt? (4/4)

- Y también estos complementos formativos multimedia:
  - La enciclopedia visual de seguridad de la información intypedia
    - http://www.criptored.upm.es/intypedia/index.php?lang=es
    - Septiembre 2010 (865.955 reproducciones al 31/12/2019)
  - El Massive Open Online Course MOOC Crypt4you
    - http://www.criptored.upm.es/crypt4you/portada.html
    - Marzo 2012 (1.494.315 accesos al 31/12/2019)
  - Las píldoras formativas en seguridad de la información Thoth
    - http://www.criptored.upm.es/thoth/index.php
    - Abril 2014 (532.528 reproducciones al 31/12/2019)

Documentación extra recomendada

- Se pretende entregar el **conocimiento mínimo en criptografía** que hoy debería tener cualquier ingeniero que se dedique a la seguridad
- Para profundizar aún más en la criptografía actual, y en la futura, se recomienda la lectura de estos tres libros, los dos primeros gratuitos
  - Criptografía y Seguridad en Computadores. Manuel Lucena, versión 5-0.1.4, noviembre 2019

    http://criptografiayseguridad.blogspot.com/p/criptografia-y-seguridad-en.html
  - A Graduate Course in Applied Cryptography. Dan Boneh & Victor Shoup, version 0.5, Jan. 2020

    https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_5.pdf
  - Serious Cryptography: A Practical Introduction to Modern Encryption. Jean-Philippe Aumasson, No Starch Press, Inc, Nov. 2017

Temática de las videoclases

- Módulo 1: Principios básicos de la seguridad
- Módulo 2: Matemáticas discretas en la criptografía
- Módulo 3: Complejidad algorítmica en la criptografía
- Módulo 4: Teoría de la información en la criptografía
- Módulo 5: Fundamentos de la criptografía
- Módulo 6: Algoritmos de criptografía clásica
- Módulo 7: Funciones hash en la criptografía
- Módulo 8: Criptografía simétrica en bloque
- Módulo 9: Criptografía simétrica en flujo
- Módulo 10: Criptografía asimétrica
- Módulo 11. Certificados digitales
- Módulo 12. Protocolos criptográficos
- Módulo 13: Temas avanzados en criptografía

- En las próximas diapositivas se incluyen algunos apartados que podrían formar parte de las videoclases de Class4crypt

- Los apartados pueden cambiar o ampliarse si fuera el caso

Contenido de las videoclases

- Módulo 1: Principios básicos de la seguridad
  1.1. Ciberseguridad y criptografía
  1.2. Percepción de la inseguridad según las décadas
  1.3. Vulnerabilidades y amenazas de la información
  1.4. Seguridad informática versus seguridad de la información
  1.5. Tríada confidencialidad, integridad y disponibilidad

- Este primer módulo es sólo de introducción y de cultura general en seguridad, recomendable antes de abordar temas específicos de la criptografía

Contenido de las videoclases

- Módulo 2: Matemáticas discretas en la criptografía
  - 2.1. Operaciones modulares y conjunto de restos
  - 2.2. El homomorfismo de los enteros
  - 2.3. Inversos aditivo, xor y multiplicativo
  - 2.4. Cálculo de inversos con el algoritmo extendido de Euclides
  - 2.5. Generadores o raíces primitivas
  - 2.6. Algoritmo de exponenciación modular rápida
  - 2.7. El teorema chino de los restos
  - 2.7. Introducción a los campos de Galois

Contenido de las videoclases

- Módulo 3: Complejidad algorítmica en la criptografía
  - 3.1. El problema del logaritmo discreto y su uso en criptografía
  - 3.2. El problema de la factorización entera y su uso en criptografía

- Módulo 4: Teoría de la información en la criptografía
  - 4.1. Entropía de la información
  - 4.2. Cantidad de información y redundancia del lenguaje
  - 4.3. Esquema de cifrado aleatorio
  - 4.4. Distancia de unicidad

Contenido de las videoclases

- Módulo 5: Fundamentos de la criptografía
  - 5.1. Definiciones, principios y usos de la criptografía
  - 5.2. De la criptografía clásica a la criptografía moderna
  - 5.3. Los inicios de la criptografía
  - 5.4. Fundamentos de la criptografía clásica, difusión y confusión
  - 5.5. Máquinas y mecanismos de cifra
  - 5.6. Clasificación de los sistemas de cifra clásica
  - 5.7. Clasificación de los sistemas de cifra moderna
  - 5.8. Fundamentos de la cifra simétrica y de la cifra asimétrica

Contenido de las videoclases

- Módulo 6: Algoritmos de criptografía clásica
  - 6.1. Cifrado por permutación de filas y columnas
  - 6.2. Criptoanálisis de los sistemas de cifra por permutación
  - 6.3. Cifrado por sustitución monoalfabética: algoritmos del César y afín
  - 6.4. Criptoanálisis por sustitución monoalfabética
  - 6.5. Cifrado por sustitución polialfabética: algoritmo de Vigenère
  - 6.6. Criptoanálisis al cifrado de Vigenère por el método Kasiski
  - 6.7. Cifrado por sustitución poligrámica: algoritmo de Hill
  - 6.8. Criptoanálisis al cifrado de Hill por el método Gauss-Jordan

Contenido de las videoclases

- Módulo 7: Funciones hash en la criptografía
  - 7.1. Características y utilidad de la función hash en criptografía
  - 7.2. Propiedades de una función hash
  - 7.3. Hash MD5
  - 7.4. Hash SHA1
  - 7.5. Familia hash SHA2
  - 7.6. Algoritmo Keccak y hash SHA3
  - 7.7. Ataques a las funciones hash y comparativa de fortaleza
  - 7.8. Redes blockchain

Contenido de las videoclases

- Módulo 8: Criptografía simétrica en bloque
  - 8.1. Fundamentos de la cifra en bloque
  - 8.2. Características de algoritmos destacados de cifra simétrica en bloque
  - 8.3. Modos de cifra: ECB, CBC, CTR, GCM
  - 8.4. Formatos de relleno
  - 8.5. Algoritmo DES Data Encryption Standard
  - 8.6. Ataque divide y venderás en cifra simétrica en bloque
  - 8.7. DES Challenge
  - 8.8. Ataque meet in the middle al 2DES y formatos 3DES
  - 8.9. Algoritmo IDEA International Data Encryption Algorithm
  - 8.10. Algoritmo AES Advanced Encryption Standard

Contenido de las videoclases

- Módulo 9: Criptografía simétrica en flujo
  - 9.1. Fundamentos de la cifra en flujo
  - 9.2. Registros de desplazamientos lineales y no lineales
  - 9.3. Postulados de Golomb
  - 9.4. Cifrado y descifrado con registros de desplazamientos lineales
  - 9.5. Ataque de Berlekamp-Massey a LFSR primitivos
  - 9.6. Generadores de secuencia cifrante con LFSR de complejidad mayor
  - 9.7. Algoritmo A5/1
  - 9.8. Algoritmo RC4
  - 9.9. Algoritmo Chacha20 Poly1305
  - 9.10. Algoritmo Keccak como generador de secuencia cifrante

Contenido de las videoclases

- Módulo 10: Criptografía asimétrica (primera parte)
  - 10.1. Criptografía asimétrica y la analogía con los candados
  - 10.2. Protocolo de intercambio de clave de Diffie y Hellman
  - 10.3. Ataque man in the middle al protocolo de Diffie y Hellman
  - 10.4. Algoritmo RSA
  - 10.5. Estándares y generación de claves en RSA
  - 10.6. Cifrado y descifrado en RSA
  - 10.7. Particularidades de las claves en RSA
  - 10.8. Particularidades de la cifra en RSA
  - 10.9. Uso del Teorema Chino de los Restos en el descifrado RSA
  - 10.10. Relleno OAEP Optimal Asymmetric Encryption Padding en RSA

Contenido de las videoclases

- Módulo 10: Criptografía asimétrica (segunda parte)
  - 10.11. Ataque a RSA mediante cifrado cíclico
  - 10.12. Ataque a RSA mediante la paradoja del cumpleaños
  - 10.13. Ataque a RSA por canal lateral
  - 10.14. Algoritmo de Elgamal para el intercambio de clave
  - 10.15. Algoritmo de Elgamal para la firma digital
  - 10.16. Algoritmo de firma digital DSA Digital Signature Algorithm
  - 10.17. Uso de curvas elípticas en criptografía
  - 10.18. ECC Elliptic Curve Cryptography

Contenido de las videoclases

- Módulo 11: Certificados digitales
  - 11.1. Principios de infraestructura de clave pública PKI
  - 11.2. Esquema de un certificado digital X.509

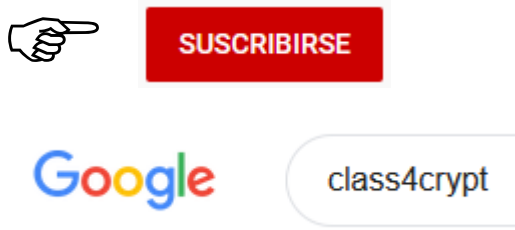
- Módulo 12: Protocolos criptográficos
  - 12.1. Introducción a los protocolos criptográficos
  - 12.2. Transferencia trascordada
  - 12.3. Distribución de secretos
  - 12.4. Protocolo de firma ciega
  - 12.5. Protocolo del póquer mental
  - 12.6. Pruebas de conocimiento cero

Contenido de las videoclases

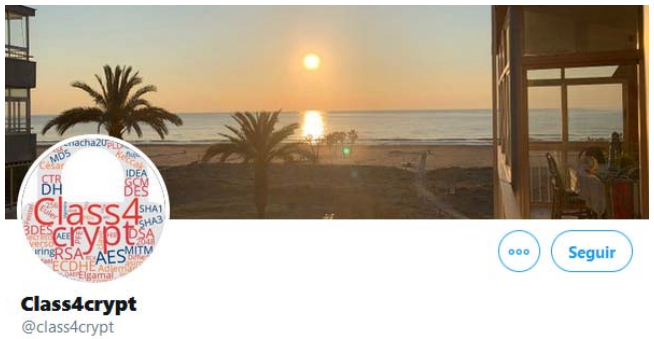
- Módulo 13: Temas avanzados en criptografía
  - 13.1. Computación segura multiparte
  - 13.2. Cifrado homomórfico
  - 13.3. Cifrado ligero
  - 13.4. Computación cuántica y criptografía

¿Dónde ver y cómo seguir las videoclases?

- Las videoclases se subirán al canal YouTube del profesor Ramió
  - https://www.youtube.com/user/jorgeramio



- Más información y seguimiento en canal Twitter de Class4crypt
  - https://twitter.com/class4crypt



¿Cómo puedo usar esta documentación?

- Estas videoclases y la documentación utilizada en ellas, se encuentran bajo licencia *Creative Commons* tipo CC BY-NC-ND 4.0
- Reconocimiento - No Comercial - Sin Obra Derivada
- Permite que otros puedan descargar esta obra y compartirla con otras personas, siempre que se reconozca su autoría, pero no se puede cambiar de ninguna manera su contenido ni se puede utilizar comercialmente

¡Muchas gracias!

- Síguenos en Class4crypt, tu aula virtual de criptografía aplicada
- https://www.youtube.com/user/jorgeramio
- https://twitter.com/class4crypt

- Música:
- Enter_Blonde, Max Surla, Media Right Productions, YouTube Audio Library - Free Music https://www.youtube.com/audiolibrary/music?nv=1