

# CRIPTOGRAFÍA PARA INGENIER@S

## Class4crypt

© Jorgeramio 2022

Aula virtual de  
criptografía  
aplicada

Diapositivas  
utilizadas en las  
clases grabadas  
de Class4crypt

<https://www.youtube.com/user/jorgeramio>

Dr. Jorge Ramió Aguirre © 2022



Attribution-NonCommercial-  
NoDerivatives 4.0 International  
(CC BY-NC-ND 4.0)

# Prólogo



El libro que tiene en sus manos es algo más que un escrito competente de la materia que ocupa. En los ulteriores folios el Dr. Jorge Ramió refleja de forma desinteresada parte de su enorme conocimiento en la disciplina de la criptografía, perfeccionado durante décadas con la docencia de miles de estudiantes a lo largo del planeta.

Usted lector tiene una gran suerte de poder beneficiarse de este material. Como lector, amigo y colega de Jorge, no tome este hecho como algo menor.

En tiempos de la inmediatez, de la banalidad y, por qué no decirlo, de la imprecisión en contra del rigor, difundir material en "texto" resultado de toda una vida pudiera parecer "traicionar" las nuevas formas de educar y preparar a las generaciones futuras.

"Roma" no paga a traidores... pero yo no soy romano. Mi admiración y mi respeto por un servidor público que dio tanto a tantos. Mis mejores deseos para esta nueva etapa Jorge.

Y usted, querido lector, no lo olvide: "Solo hay un bien: el conocimiento. Solo hay un mal: la ignorancia." - Sócrates (470 a.C. - 399 a.C.) Filósofo griego.

Dr. Alfonso Muñoz

# Nota del autor



En mis 25 años impartiendo clases de criptografía en universidades de España y de Latinoamérica, he podido comprobar una cierta dificultad en los alumnos para asimilar la gran cantidad de conceptos que encierran la criptografía y sus ramas asociadas, como son las matemáticas discretas, la complejidad de los algoritmos y la teoría de la información. Por este motivo, comencé a mediados de enero del año 2020 el proyecto de aula virtual Class4crypt en YouTube para fortalecer dicha temática entre mis estudiantes.

Sin ir más lejos, este libro de Criptografía para Ingenier@s cuenta con 350 apartados, y de cada uno de ellos pueden obtenerse uno o más conceptos. No son tan complejos, pero sí es verdad que son muchos.

Jubilado hace pocos meses, este libro viene a ser mi legado para las nuevas generaciones de amigos de la criptografía, después de haber publicado diversos documentos gratuitos en Internet, amén de algún libro con mi compañero, amigo y colega Alfonso Muñoz, donde cabe destacar el Libro Electrónico de Seguridad Informática y Criptografía de 2006 con 200.000 descargas, el Curso de Criptografía Aplicada de 2018 con 30.000 descargas, y los proyectos de nuestra red temática Criptored, como la enciclopedia de seguridad intypedia, las píldoras formativas Thoth y el MOOC Crypt4you, cada uno con un millón de visitas.

En marzo de 2022 y en Canet d'en Berenguer, mi actual residencia, te deseo una feliz y provechosa lectura.

Módulo 1. Principios básicos de la seguridad .....	37
Lección 1.1. Ciberseguridad y criptografía .....	40
1.1.1. Definiendo el concepto ciberespacio	
1.1.2. El papel de la criptografía dentro de la seguridad informática	
1.1.3. Enseñanza de la criptografía	
1.1.4. Cómo estudiar criptografía	
1.1.5. La criptografía que viene	
Lección 1.2. Percepción de la inseguridad según la década .....	60
1.2.1. La inseguridad informática en la década de los años 70	
1.2.2. La inseguridad informática en la década de los años 80	
1.2.3. La inseguridad informática en la década de los años 90	
1.2.4. La inseguridad informática en la década de los años 00	
1.2.5. La inseguridad informática en la década de los años 10	
Lección 1.3. Vulnerabilidades de la información y amenazas .....	74

- 1.3.1. La información, el activo más importante a proteger
- 1.3.2. Vulnerabilidades de la información
- 1.3.3. Amenazas a la información
- 1.3.4. Clasificación de las amenazas a la información
- 1.3.5. Controles para la protección de la información
- Lección 1.4. Seguridad informática versus seguridad de la información ..... 91
  - 1.4.1. Posible confusión entre los dos términos
  - 1.4.2. Definición de seguridad informática
  - 1.4.3. Entornos de la seguridad informática
  - 1.4.4. Definición de seguridad de la información
  - 1.4.5. Entornos de la seguridad de la información
  - 1.4.6. Roles de responsables de seguridad en la empresa
- Lección 1.5. Tríada confidencialidad, integridad y disponibilidad ..... 103
  - 1.5.1. Confidencialidad de la información

1.5.2. Integridad de la información

1.5.3. Disponibilidad de la información

1.5.4. Objetivos de la CIA y estado seguro de la información

1.5.5. Servicios de seguridad: Autenticación, Control de acceso, No repudio y Trazabilidad

**Módulo 2. Matemáticas discretas en la criptografía ..... 119**

**Lección 2.1. Aritmética modular, conjunto de restos y función de Euler ..... 122**

2.1.1. Cuerpos, grupos, anillos, campos y módulo

2.1.2. Aritmética y operaciones modulares

2.1.3. Importancia de los primos y magnitudes

2.1.4. Conjunto completo y reducido de restos

2.1.5. Función de Euler  $\phi(n)$

**Lección 2.2. El homomorfismo de los enteros en la criptografía ..... 142**

2.2.1. Recordando la aritmética modular

2.2.2. Homomorfismo de los enteros en operaciones modulares

2.2.3. Reducción por cuadrados en operaciones de exponenciación modular	
2.2.4. Importancia del homomorfismo de los enteros en la cifra moderna	
2.2.5. Calculadoras a usar para las operaciones de cifra con números grandes	
<b>Lección 2.3. Inverso aditivo, inverso xor e inverso multiplicativo</b>	<b>..... 155</b>
2.3.1. Importancia de los inversos en la criptografía	
2.3.2. Los inversos aditivos	
2.3.3. Los inversos xor	
2.3.4. Los inversos multiplicativos	
<b>Lección 2.4. Cálculo de inversos con el algoritmo extendido de Euclides</b>	<b>..... 177</b>
2.4.1. Recordando la importancia de los inversos en criptografía	
2.4.2. Divisibilidad de los números y Euclides	
2.4.3. Algoritmo de Euclides para calcular el máximo común divisor	
2.4.4. Cálculo de inversos mediante el algoritmo de Euclides y el recorrido de la tabla de restos	
2.4.5. Algoritmo extendido de Euclides para el cálculo de inversos	

Lección 2.5. Algoritmo de exponenciación modular rápida .....	195
2.5.1. Operaciones de potencia modular en criptografía moderna	
2.5.2. La solución del homomorfismo de los enteros	
2.5.3. Algoritmo de exponenciación rápida	
2.5.4. Calculadoras modulares básicas, avanzadas y online	
2.5.5. Calculadoras modulares online no recomendables	
Lección 2.6. Raíces primitivas en un primo $p$ .....	207
2.6.1. Concepto de raíz primitiva	
2.6.2. Comprobación de la existencia de raíces primitivas	
2.6.3. Búsqueda de raíces primitivas	
2.6.4. Tasa de restos que son raíces primitivas	
2.6.5. La importancia de los primos seguros	
2.6.6. Uso de las raíces primitivas en la criptografía	
Módulo 3. Complejidad algorítmica en la criptografía .....	227



Lección 3.1. Fundamentos de complejidad algorítmica .....	230
3.1.1. Introducción a la teoría de la complejidad algorítmica	
3.1.2. Problemas de tipo P y N	
3.1.3. Introducción al problema de la mochila	
3.1.4. Introducción al problema del logaritmo discreto	
3.1.5. Introducción al problema de la factorización entera	
Lección 3.2. El problema de la mochila .....	250
3.2.1. Enunciado simple del problema de la mochila	
3.2.2. Resolución de un problema de mochila	
3.2.3. Uso en criptografía: mochila tramposa de Merkle y Hellman	
3.2.4. Ejemplo de cifrado asimétrico con mochila de Merkle y Hellman	
Lección 3.3. El problema del logaritmo discreto .....	266
3.3.1. Enunciado del problema del logaritmo discreto	
3.3.2. Ejemplos y resolución de operaciones de exponenciación modular	

3.3.3. Ejemplos y resolución de operaciones de logaritmo discreto	
3.3.4. Usos en la criptografía: intercambio de clave de Diffie y Hellman, cifra y firma de Elgamal, algoritmo de firma digital DSA	
<b>Lección 3.4. El problema de la factorización entera</b>	<b>281</b>
3.4.1. Enunciado del problema de la factorización entera PFE	
3.4.2. Operaciones de multiplicación y su inversa la factorización entera	
3.4.3. Solución del problema de la factorización entera con msieve153	
3.4.4. Solución del problema de la factorización entera con web Alpertron	
3.4.5. Algoritmos del PFE y complejidad asociada	
3.4.6. Uso en criptografía moderna de clave pública: algoritmo RSA	
<b>Módulo 4. Teoría de la información en la criptografía</b>	<b>297</b>
<b>Lección 4.1. Cantidad de información e incertidumbre</b>	<b>300</b>
4.1.1. Definiciones de información y teoría de la información	
4.1.2. La figura de Claude Shannon	

- 4.1.3. Cantidad de información asociada a un mensaje
  - 4.1.3.a. Análisis en función de su extensión (visión subjetiva)
  - 4.1.3.b. Análisis en función de su utilidad (visión subjetiva)
  - 4.1.3.c. Análisis en función de su probabilidad (visión objetiva)
- 4.1.4. Definiciones de incertidumbre y de cantidad de información
- Lección 4.2. Entropía de la información y codificador óptimo ..... 319
  - 4.2.1. Definición de entropía
  - 4.2.2. Propiedades de la entropía
  - 4.2.3. Codificador óptimo
  - 4.2.4. Codificación mediante el método de Huffman
  - 4.2.5. Ejemplos de entropía de mensajes
- Lección 4.3. Ratio y redundancia del lenguaje ..... 334
  - 4.3.1. Recordando el concepto de entropía  $H(X)$
  - 4.3.2. La ratio absoluta del lenguaje  $R$

4.3.3. La ratio real del lenguaje r	
4.3.4. Redundancia del lenguaje D	
4.3.5. Debilidades de la cifra clásica por la redundancia del lenguaje	
4.3.6. Relación entre la redundancia del lenguaje y la compresión alcanzada en los programas zip	
<b>Lección 4.4. Secreto perfecto y distancia de unicidad</b>	<b>..... 353</b>
4.4.1. Secreto de un sistema criptográfico	
4.4.2. Cifrado con secreto perfecto	
4.4.3. Cifrado sin secreto perfecto	
4.4.4. Modelo de cifrador aleatorio	
4.4.5. Distancia de unicidad	
<b>Lección 4.5. Métodos de difusión y confusión en la criptografía</b>	<b>..... 369</b>
4.5.1. Importancia de la difusión y la confusión en la criptografía	
4.5.2. Método de difusión	
4.5.3. Obtención de difusión mediante operaciones de permutación	

4.5.4. Método de confusión	
4.5.5. Obtención de confusión mediante operaciones de sustitución	
4.5.6. Cifradores de producto	
<b>Módulo 5. Fundamentos de la criptografía</b>	<b>383</b>
<b>Lección 5.1. Definiendo criptografía y criptoanálisis</b>	<b>386</b>
5.1.1. La criptografía y el criptoanálisis como parte de la criptología	
5.1.2. Definiciones de criptografía según su ámbito de estudio	
5.1.3. Diferencias entre cifrar y codificar	
5.1.4. Definición de criptoanálisis	
5.1.5. Entornos de cifra más o menos propensos al criptoanálisis	
<b>Lección 5.2. Esquema y elementos de un criptosistema</b>	<b>402</b>
5.2.1. La necesidad de cifrar la información	
5.2.2. Esquema de un sistema de cifra	
5.2.3. Texto en claro y criptograma	

5.2.4. Algoritmo de cifrado y de descifrado	
5.2.5. Clave de cifrado y de descifrado	
5.5.6. Canal o medio de transmisión	
5.2.7. Alfabeto de cifra	
Lección 5.3. Principios de Kerckhoffs y fortaleza de la cifra	413
5.3.1. La figura de Auguste Kerckhoffs	
5.3.2. Los principios, postulados o lemas de Kerckhoffs	
5.3.3. Ataques por fuerza bruta y criptoanálisis	
5.3.4. Tipos de ataque a los algoritmos de cifra	
5.3.5. Fortaleza de un algoritmo de cifra	
Lección 5.4. Introducción a la esteganografía	427
5.4.1. Definición de esteganografía y estegoanálisis	
5.4.2. El problema de los prisioneros	
5.4.3. Casos históricos del uso de la esteganografía	

5.4.4. Usos actuales de la esteganografía	
5.4.5. Introducción a la esteganografía usando imágenes	
5.4.6. La esteganografía mediante el uso de acrósticos	
5.4.7. Ocultación de texto dentro de una imagen desde símbolo del sistema	
<b>Lección 5.5. Mecanismos y máquinas de cifra</b>	<b>443</b>
5.5.1. Viaje histórico por los mecanismos, las máquinas y los personajes de la criptografía clásica	
5.5.2. Cifradores de los siglos V, II y I antes de Cristo	
5.5.3. Algunos cifradores a partir del siglo XV: Alberti, Vigenère, Jefferson, Playfair, Wheatstone, Bazeries y Hill	
5.5.4. El telegrama de Zimmermann (WWI) y la máquina Enigma (WWII)	
5.5.5. Personajes destacados: Allan Poe, Alan Turing y Claude Shannon	
<b>Lección 5.6. Clasificación de los sistemas de cifra clásica</b>	<b>465</b>
5.6.1. ¿Qué se entiende por cifra clásica?	
5.6.2. Frontera entre la criptografía clásica y la criptografía moderna	

5.6.3. Clasificación histórica de los sistemas de cifra	
5.6.4. Algunos sistemas de cifra clásica representativos	
5.6.5. Clasificación de los criptosistemas de cifra clásica	
5.6.6. Debilidades de los criptosistemas de cifra clásica	
<b>Lección 5.7. Introducción a la criptografía moderna</b>	<b>476</b>
5.7.1. Objetivos, definiciones y diferencias entre la criptografía clásica y la moderna	
5.7.2. Hitos que marcan el cambio de la criptografía clásica a la criptografía moderna	
5.7.3. Clasificación de la cifra moderna según el tipo de claves utilizadas	
5.7.4. Clasificación de la cifra moderna según el tratamiento de la información	
5.7.5. Introducción a los métodos y algoritmos de cifra modernos	
5.7.6. Introducción a la cifra en flujo y a la cifra en bloque	
5.7.7. Introducción a la cifra simétrica y a la cifra asimétrica	
<b>Lección 5.8. Comparativa entre cifra simétrica y cifra asimétrica</b>	<b>495</b>
5.8.1. Recordando las diferencias entre la cifra simétrica y la cifra asimétrica	



5.8.2. Comparativa entre sistemas de cifra simétrica versus sistemas de cifra asimétrica

5.8.2.1. Ante la seguridad del sistema

5.8.2.2. Ante la gestión de las claves

5.8.2.3. Ante el espacio de las claves

5.8.2.4. Ante la vida de las claves

5.8.2.5. Ante el intercambio de clave

5.8.2.6. Ante la firma digital

5.8.2.7. Ante la velocidad de cifra

5.8.3. Entornos de cifra híbrida

Módulo 6. Algoritmos de criptografía clásica ..... 517

Lección 6.1a. Cifrado por permutación o transposición parte 1 ..... 520

6.1a.1. Técnica de permutación para lograr la difusión

6.1a.2. Cifrado por escítala

6.1a.3. Cifrado por filas y columnas

Lección 6.1b. Cifrado por permutación o transposición parte 2	536
6.1b.1. Cifrado tipo rail fence	
6.1b.2. Cifrado por rejilla de Cardano	
6.1b.3. Cifradores por permutación de bloques de texto	
Lección 6.2. Criptoanálisis a la cifra por permutación	550
6.2.1. Estadísticas del lenguaje: digramas o bigramas	
6.2.2. Criptoanálisis por anagramación en cifras de filas y columnas	
6.2.3. Dificultad del criptoanálisis por la complejidad del modo de cifra	
Lección 6.3. Cifrado por sustitución	564
6.3.1. Técnicas de sustitución para lograr la confusión	
6.3.2. Sustitución monoalfabética	
6.3.3. Cifrado por sustitución monoalfabética con desplazamiento o César	
6.3.4. Cifrado por sustitución monoalfabética con decimación	
6.3.5. Cifrado por sustitución monoalfabética afín	

6.3.6. Introducción a la sustitución polialfabética	
<b>Lección 6.4. Criptoanálisis a la sustitución monoalfabética</b>	<b>583</b>
6.4.1. Al-Kindi y las estadísticas del lenguaje	
6.4.2. Criptoanálisis a la cifra por desplazamiento puro	
6.4.3. Criptoanálisis a la cifra por decimación pura	
6.4.4. Criptoanálisis a la cifra afín	
6.4.5. Mejorando la seguridad de la cifra con sustitución polialfabética	
<b>Lección 6.5. Sustitución polialfabética y algoritmo de Vigenère</b>	<b>600</b>
6.5.1. La cifra por sustitución polialfabética soluciona la vulnerabilidad de la monoalfabética	
6.5.2. La figura de Blaise de Vigenère	
6.5.3. El cifrado y la tabla de Vigenère	
6.5.4. Característica de la cifra de Vigenère	
6.5.5. Ejercicios prácticos de cifrado y descifrado de Vigenère	
<b>Lección 6.6. Criptoanálisis a la cifra de Vigenère por el método Kasiski</b>	<b>614</b>

- 6.6.1. Recordando la cifra por sustitución polialfabética periódica de Vigenère
- 6.6.2. La redundancia del lenguaje
- 6.6.3. La figura de Friedrich Kasiski y otros criptólogos de la época
- 6.6.4. Desarrollo del método de Kasiski para el criptoanálisis de Vigenère
- 6.6.5. Ejercicio práctico de criptoanálisis a Vigenère por el método de Kasiski
- Lección 6.7. Cifrado digramico de Playfair ..... 637**
- 6.7.1. Monogramas y digramas
- 6.7.2. Formando bloques de letras
- 6.7.3. Charles Wheatstone y Lyon Playfair
- 6.7.4. Cifrado digramico por cuadrado de Playfair
- 6.7.5. Descifrado digramico por cuadrado de Playfair
- 6.7.6. Criptoanálisis a la cifra de Playfair
- Lección 6.8. Cifrado poligrámico con matrices de Hill ..... 649**
- 6.8.1. Cifrado poligrámico de Hill

6.8.2. Fortalezas y debilidades de la cifra de Hill	
6.8.3. Uso de bloques en la cifra moderna	
<b>Lección 6.9. Criptoanálisis a la cifra de Hill por Gauss-Jordan</b>	<b>665</b>
6.9.1. Buscando los vectores unitarios	
6.9.2. Las figuras de Gauss y Jordan	
6.9.3. Criptoanálisis de Gauss-Jordan	
6.9.4. Ejemplo práctico mod 27 y mod 191	
6.9.5. Usos de matrices en la criptografía moderna	
<b>Módulo 7. Funciones hash</b>	<b>687</b>
<b>Lección 7.1. Funciones hash en la criptografía</b>	<b>690</b>
7.1.1. Qué son y qué no son las funciones hash	
7.1.2. Ejemplos de funciones hash, cálculo y utilidad en la criptografía	
7.1.3. Principio del palomar: seguridad y unicidad de las funciones hash	

7.1.4. Propiedades de las funciones hash: facilidad de cálculo, propiedad de unidireccionalidad, propiedad de compresión, propiedad de difusión, propiedad de no predictibilidad, resistencia a primera preimagen, resistencia simple a colisiones y resistencia fuerte a colisiones

7.1.5. Ataque al hash por la paradoja del cumpleaños

Lección 7.2. Función hash MD5: estructura y operaciones ..... 710

7.2.1. Construcción de hashes

7.2.2. La estructura de Merkle-Damgård

7.2.3. Cronología de los algoritmos de hash

7.2.4. Características de la función hash MD5

7.2.5. Funcionamiento del hash MD5

7.2.6. MD5 por dentro con el software CriptoRes

Lección 7.3. Función hash SHA-1 ..... 731

7.3.1. Información compartida con la clase c4c7.2 sobre MD5: estructura Merkle-Damgård , relleno ISO/IEC 7816-4, bits de indicación del tamaño

7.3.2. Funciones hash SHA y el proyecto Capstone con DSA

7.3.3. Por qué se habla de SHA-0	
7.3.4. Características de la función hash SHA-1	
7.3.5. Funcionamiento del hash SHA-1	
7.3.6. SHA-1 por dentro con el software CriptoRes	
<b>Lección 7.4. Colisiones en funciones hash MD5 y SHA-1</b>	<b>751</b>
7.4.1. El efecto de difusión o avalancha, que no siempre se cumple	
7.4.2. Repasando las debilidades de las funciones hash	
7.4.3. Colisiones en MD5	
7.4.3.1. Certificados digitales X.509	
7.4.3.2. Archivos ejecutables	
7.4.3.3. Archivos de documentos PDF e imágenes JPG	
7.4.4. Colisiones en SHA-1	
<b>Lección 7.5. SHA-2, SHA-3 y resumen de funciones hash</b>	<b>770</b>
7.5.1. Resúmenes SHA-224, SHA-256, SHA-384 y SHA-512	

7.5.2. Construcción esponja	
7.5.3. Primitiva criptográfica Keccak	
7.5.4. El algoritmo SHA-3	
7.5.5. Resumen comparativo MD5, SHA-1, SHA-2 y SHA-3	
<b>Módulo 8. Criptografía simétrica en bloque</b>	<b>789</b>
<b>Lección 8.1. Fundamentos de la cifra simétrica en bloque</b>	<b>792</b>
8.1.1. Formando bloques para cifrar	
8.1.2. Esquema de la cifra simétrica en bloque	
8.1.3. Características de la cifra simétrica en bloque	
8.1.4. Recorrido histórico por los algoritmos de cifra en bloque más populares	
8.1.5. Algoritmos de cifra en bloque que deberíamos conocer y estudiar	
<b>Lección 8.2. Algoritmo DES: redes de Feistel y cajas S</b>	<b>811</b>
8.2.1. Estudio cronológico del Data Encryption Standard DES	
8.2.2. Limitaciones de la NSA a los tamaños del bloque y de la clave	



8.2.3. La clave real del DES y el código hexadecimal	
8.2.4. Redes de Feistel: creación de bloques izquierdo y derecho del texto en claro	
8.2.5. Operaciones de permutación en el texto en claro y en resultados	
8.2.6. Operaciones de sustitución con cajas S	
<b>Lección 8.3. Algoritmo DES: expansión de clave, cifra y rellenos</b>	<b>..... 834</b>
8.3.1. Los bits de paridad en la clave del DES	
8.3.2. Generación de las 16 subclaves de ronda $k_1$ a $k_{16}$ en cifrado y descifrado	
8.3.3. Operaciones de cifrado y descifrado	
8.3.4. Relleno zero padding	
8.3.5. Claves débiles y semidébiles	
<b>Lección 8.4a. ECB y CBC, modos de cifra con confidencialidad</b>	<b>..... 848</b>
8.4a.1 Necesidad de los modos de cifra en bloque	
8.4a.2. Modos de cifra aprobados por el NIST	
8.4a.3. Modo de cifra ECB Electronic codebook	

- 8.4a.4 Modo de cifra CBC Cipher block chaining
- Lección 8.4b. CFB, OFB y CTR, modos de cifra con confidencialidad ..... 867
- 8.4b.1 Modos de cifra aprobados por el NIST
- 8.4b.2. Modo de cifra CFB Cipher feedback
- 8.4b.3. Modo de cifra OFB Output feedback
- 8.4b.4. Modo de cifra CTR Counter
- 8.4b.5 Comparativa entre modos de cifra con confidencialidad
- Lección 8.5. Ataques al DES, DES Challenge y 3DES ..... 882
- 8.5.1. Debilidades del DES
- 8.5.2. Ataques en red a la cifra simétrica en bloque usando divide y vencerás
- 8.5.3. El desafío DES Challenge
- 8.5.4. Necesidad del cifrado múltiple
- 8.5.5. Fortaleza real del doble DES por ataque meet in the middle
- 8.5.6. Características y usos del 3DES

8.5.7. Formato de cifra EDE Encrypt Decrypt Encrypt

Lección 8.6a. Algoritmo AES parte 1: visión general y fortaleza ..... 907

8.6a.1. El concurso del NIST para el Advanced Encryption Standard

8.6a.2. Características del algoritmo

8.6a.3. Esquemas de cifrado y de descifrado

8.6a.4. Relleno PKCS#7

8.6a.5. Operaciones de cifrado y de descifrado

8.6a.6. Consideraciones sobre la fortaleza del algoritmo

Lección 8.6b. Algoritmo AES parte 2: Campos de Galois y expansión de clave ..... 927

8.6b.1. Resumen y esquema del AES

8.6b.2. Representación de bytes en GF

8.6b.3. Operaciones de suma y multiplicación en campos de Galois

8.6b.4. Inversos en GF ( $2^8$ )

8.6b.5. Funciones RotWord y Rcon

8.6b.6. Algoritmo de expansión de clave

Lección 8.6c. AES parte 3: SubBytes, ShiftRows, MixColumns, AddRoundKey ..... 945

8.6c.1. Esquema del AES y recuerdo de operaciones en GF ( $2^8$ )

8.6c.2. Función SubBytes

8.6c.3. Función ShiftRows

8.6c.4. Función MixColumns

8.6c.5. Función AddRoundKey

Módulo 9. Criptografía simétrica en flujo ..... 971

Lección 9.1. Fundamentos de la cifra simétrica en flujo ..... 974

9.1.1. El código Baudot

9.1.2. El cifrado de Vernam con código Baudot

9.1.3. Vernam, la libreta de un solo uso OTP y el secreto perfecto

9.1.4. Introducción y estructura de un cifrado en flujo

9.1.5. Características que debe presentar una buena secuencia cifrante binaria

9.1.5.1. Tamaño de la secuencia	
9.1.5.2. Imprevisibilidad de la secuencia	
9.1.5.3. Aleatoriedad de la secuencia	
Lección 9.2. Registros de desplazamiento realimentados LFSR y NLFSR	991
9.2.1. Generadores de secuencias cifrantes	
9.2.2. Registro de desplazamiento realimentado	
9.2.3. Registros de desplazamiento realimentados no lineales NLFSR	
9.2.4. Registros de desplazamiento realimentados lineales LFSR	
9.2.4.1. Registros con polinomio asociado factorizable	
9.2.4.2. Registros con polinomio asociado irreducible	
9.2.4.3. Registros con polinomio asociado primitivo	
Lección 9.3. Aleatoriedad en registros LFSR con polinomio primitivo	1.014
9.3.1. Postulado de Golomb R1	
9.3.2. Rachas de bits	

9.3.3. Postulado de Golomb R2	
9.3.4. Autocorrelación fuera de fase	
9.3.5. Postulado de Golomb R3	
9.3.6. Prácticas con el software FlujoLab	
<b>Lección 9.4. Complejidad en LFSR, A5, RC4 y ChaCha20</b>	<b>1.032</b>
9.4.1. Complejidad algorítmica de los registros de desplazamiento FSR	
9.4.2. Ataque de Berlekamp-Massey a una m-secuencia	
9.4.3. Uso de dos o más registros para generar secuencias cifrantes	
9.4.4. Algoritmo A5	
9.4.5. Algoritmo RC4	
9.4.6. Algoritmo ChaCha20	
<b>Módulo 10. Criptografía asimétrica</b>	<b>1.057</b>
<b>Lección 10.1. Criptografía asimétrica y la analogía de los candados</b>	<b>1.061</b>
10.1.1. Buscando enviar un secreto en un medio de transmisión inseguro	

10.1.2. Primer escenario con un único candado del receptor	
10.1.3. Segundo escenario con dos candados, de emisor y de receptor	
10.1.4. En criptografía el orden es importante	
10.1.5. Soluciones al problema de enviar un secreto en un medio de transmisión inseguro	
<b>Lección 10.2. Intercambio de clave de Diffie y Hellman</b>	<b>..... 1.080</b>
10.2.1. Recordando el Problema del Logaritmo Discreto y generadores en un cuerpo	
10.2.2. Protocolo de intercambio de clave de Diffie y Hellman	
10.2.3. Protocolo de intercambio de clave de Diffie y Hellman no simultáneo	
10.2.4. Seguridad del protocolo de intercambio de clave de Diffie y Hellman	
<b>Lección 10.3. Ataque man in the middle al intercambio de clave de DH</b>	<b>..... 1.100</b>
10.3.1. Recordando el protocolo de intercambio de clave de Diffie y Hellman	
10.3.2. Ataque man in the middle con una tercera parte usando una sola clave secreta	
10.3.3. Ataque man in the middle con una tercera parte usando dos claves secretas	
10.3.4. Ejercicio práctico	

- Lección 10.4. Algoritmo RSA ..... 1.116
  - 10.4.1. La historia del algoritmo RSA: el MIT y el GCHQ
  - 10.4.2. Pasos para la generación de una clave RSA
  - 10.4.3. Introducción al cifrado y descifrado con RSA
  - 10.4.4. Fortaleza del algoritmo RSA
  - 10.4.5. Importancia de los valores elegidos para los primos  $p$  y  $q$  y para la clave pública  $e$
- Lección 10.5. Generación de claves RSA y estándar PKCS#1 ..... 1.138
  - 10.5.1. Recordando el algoritmo RSA
  - 10.5.2. Generación de una clave RSA manualmente sin ayuda de software
  - 10.5.3. Generación de claves RSA con el software genRSA v2.1
  - 10.5.4. Estándar en RSA con indicador de Euler y función de Carmichael
  - 10.5.5. Generación de claves RSA con OpenSSL
- Lección 10.6a. Cifrado y descifrado con RSA (parte 1) ..... 1.152
  - 10.6a.1. Recordando el algoritmo RSA



10.6a.2. Aquí ciframos números	
10.6a.3. ¿Por qué podemos usar como exponente la clave inversa para descifrar?	
10.6a.4. Operaciones simples de cifra y firma de números usando RSA	
<b>Lección 10.6b. Cifrado y descifrado con RSA (parte 2)</b>	<b>1.166</b>
10.6b.1. Recordando la analogía de los candados: el orden en el cifrado y descifrado es muy importante	
10.6b.2. Opciones de cifra y firma simultáneas con RSA	
10.6b.3. Cifrando texto o bloques de texto con RSA	
<b>Lección 10.7. Números no cifrables en RSA</b>	<b>1.184</b>
10.7.1. Números no cifrables	
10.7.2. Cantidad de números no cifrables	
10.7.3. Buscando los números no cifrables	
10.7.4. Supuesta debilidad de RSA debido a los números no cifrables	
<b>Lección 10.8. Claves parejas y números piratas en RSA</b>	<b>1.201</b>
10.8.1. Qué son y cómo se calculan las claves privadas parejas	

10.8.2. Supuesta vulnerabilidad en RSA por las claves privadas parejas	
10.8.3. Qué son y cómo se calculan las claves públicas parejas	
10.8.4. Supuesta vulnerabilidad en RSA por las claves públicas parejas	
10.8.5. Descifrando RSA con números piratas	
10.8.6. Supuesta vulnerabilidad en RSA por los números piratas	
<b>Lección 10.9a. Ataques teóricos y prácticos a RSA parte 1</b>	<b>..... 1.222</b>
10.9a.1. Ataques significativos a RSA	
10.9a.2. Ataque por factorización entera del módulo n	
10.9a.3. Ataque por cifrado cíclico	
<b>Lección 10.9b. Ataques teóricos y prácticos a RSA parte 2</b>	<b>..... 1.235</b>
10.9b.1. Resumen de la parte 1	
10.9b.1a. Ataque por factorización entera del módulo n	
10.9b.1b. Ataque por cifrado cíclico	
10.9b.2. Ataque por la paradoja del cumpleaños	

10.9b.3. Ataque acústico por canal lateral	
10.9b.4. Lectura recomendada y conclusiones de la lección 10.9	
<b>Lección 10.10. Algoritmo de cifra de Elgamal</b>	<b>1.254</b>
10.10.1. Breve repaso del PLD e intercambio de clave de Diffie y Hellman	
10.10.2. La figura de Taher Elgamal	
10.10.3. Generación de claves en el algoritmo de Elgamal	
10.10.4. Cifrado de Elgamal	
10.10.5. Descifrado de Elgamal	
10.10.6. Operaciones de cifra sobre números y textos	
<b>Lección 10.11. Algoritmos de firma digital RSA y de Elgamal</b>	<b>1.269</b>
10.11.1. Firma electrónica y firma digital	
10.11.2. Autenticación asimétrica vía hash	
10.11.3. Firma digital RSA	
10.11.4. Ejemplo de firmado RSA y comprobación de la firma	

10.11.5. Firma digital de Elgamal	
10.11.6. Ejemplo de firmado de Elgamal y comprobación de la firma	
Lección 10.12. Firma digital DSA y ataques a firmas de Elgamal y DSA	..... 1.283
10.12.1. Firma digital DSA y DSS	
10.12.2. Ejemplo de firma DSA	
10.12.3. Ejercicio práctico de firma DSA con ExpoCrip	
10.12.4. Ejemplo de ataque con éxito a una firma de Elgamal	
10.12.5. Ejemplo de ataque fallido a una firma de Elgamal	
10.12.6. Seguridad y ataques a la firma DSA y ECDSA	
Lección 10.13. Criptografía con curvas elípticas ECC	..... 1.299
10.13.1. Justificación del tema para el estudio personal	
10.13.2. Bibliografía	
Contraportada	..... 1.302