Class4crypt

Aula virtual de criptografía aplicada

Clase c4c2.6

Raíces primitivas en un primo p

Madrid, martes 13 de octubre de 2020

Profesor Dr. Jorge Ramió A.

Temario de las clases Class4crypt

- 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

Clases publicadas en Class4crypt (1)

1. Presentación de Class4crypt
2. Ciberseguridad y criptografía
3. Algoritmo RSA
4. Operaciones modulares y conjunto de restos
5. Percepción de la inseguridad según las décadas
6. Criptografía asimétrica y la analogía de los candados
7. Protocolo de intercambio de clave de Diffie y Hellman
8. Ataque man in the middle al intercambio de clave de Diffie y Hellman
9. Cifrado por sustitución polialfabética: algoritmo de Vigenère
10. Criptoanálisis al cifrado de Vigenère por el método Kasiski
11. El homomorfismo de los enteros en la criptografía
12. Inverso aditivo, inverso xor e inverso multiplicativo
13. Cálculo de inversos con el algoritmo extendido de Euclides
14. Algoritmo de exponenciación modular rápida
15. Generación de claves RSA y estándar PKCS#1
16. Cifrado y descifrado con RSA parte 1
17. Cifrado y descifrado con RSA parte 2

Clases publicadas en Class4crypt (2)

18. Introducción a la criptografía moderna
19. Comparación entre cifra simétrica y cifra asimétrica
20. Fundamentos de la cifra simétrica en flujo
21. Registros de desplazamiento realimentados lineales y no lineales
22. Aleatoriedad en registros LFSR con polinomio primitivo
23. Fundamentos de la cifra simétrica en bloque
24. Algoritmo DES: redes de Feistel y cajas S
25. Algoritmo DES: expansión de clave, cifra y rellenos
26. ECB y CBC, modos de cifra con confidencialidad
27. CFB, OFB y CTR, modos de cifra con confidencialidad
28. Ataques al DES, DES Challenge y 3DES
29. Clasificación de los sistemas de cifra clásica
30. Vulnerabilidades de la información y amenazas
31. Seguridad informática vs seguridad de información
32. Tríada confidencialidad, integridad y disponibilidad
33. Raíces primitivas en un primo p

- > 19.500 visualizaciones en el canal al 13/10/20

¡COMENZAMOS!

Class4crypt c4c2.6

Módulo 2. Matemáticas discretas en la criptografía

Lección 2.6. Raíces primitivas en un primo p

1. Concepto de raíz primitiva
2. Comprobación de la existencia de raíces primitivas
3. Búsqueda de raíces primitivas
4. Tasa de restos que son raíces primitivas
5. La importancia de los primos seguros
6. Uso de las raíces primitivas en la criptografía

Raíces primitivas o generadores en primos

- Se denomina raíz primitiva α de un primo p al resto x que cumple:

  $\alpha^{xi} \bmod p = y_i = CRR$ (con $0 \leq x_i \leq p-1$)

- Genera todos los elementos del primo excepto el 0, es decir, el Conjunto Reducido de Restos CRR (1, 2, 3, 4, … p-3, p-2, p-1)
- Por ello se le conoce también como generador
- Si α es una raíz primitiva entonces se cumple que:

  $\alpha^0 \bmod p = y_0 = 1$ $\quad\quad$ $\alpha^{p-1} \bmod p = y_{p-1} = 1$

  Y la operación $\alpha^{xi} \bmod p = y_{xi}$ (con $x_i = 1, 2, 3, \ldots p-4, p-3, p-2$) entrega valores diferentes comprendidos entre 2 y p-1

Ejemplo: restos raíces y no raíces en p = 7

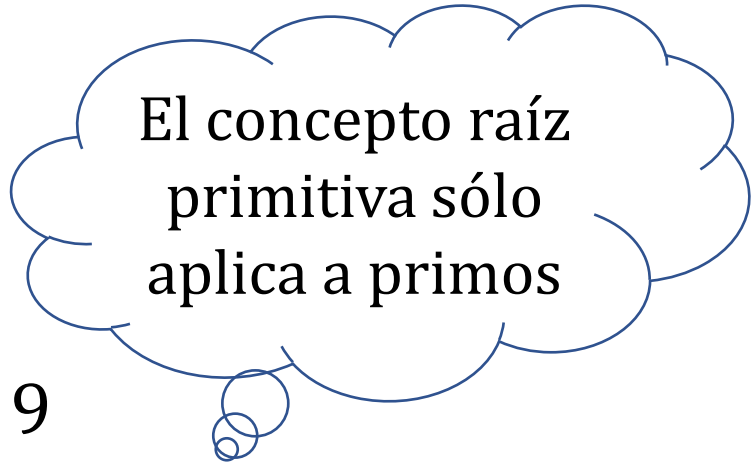
- α = 2 no es una raíz primitiva del primo p = 7
  - $2^0 \bmod 7 = 1$ ←
  - $2^1 \bmod 7 = 2$
  - $2^2 \bmod 7 = 4$
  - $2^3 \bmod 7 = 1$ ←
  - $2^4 \bmod 7 = 2$
  - $2^5 \bmod 7 = 4$
  - $2^6 \bmod 7 = 1$ ←
- α = 3 sí es una raíz primitiva del primo p = 7
  - $3^0 \bmod 7 = 1$ ←
  - $3^1 \bmod 7 = 3$
  - $3^2 \bmod 7 = 2$
  - $3^3 \bmod 7 = 6$
  - $3^4 \bmod 7 = 4$
  - $3^5 \bmod 7 = 5$
  - $3^6 \bmod 7 = 1$ ←

¿Y si el módulo no fuese primo? (1/2)

- Supongamos n = 3*5 = 15
- Los restos serían {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14}
- Para α = 2, 3, 4, … 13, 14, hacemos $\alpha^{xi} \bmod n = y_i$ (con $0 \leq x_i \leq n-1$)
  - $2^{xi} \bmod 15$ = 1, 2, 4, 8, 1, 2, 4, … 2, 4
  - $3^{xi} \bmod 15$ = 1, 3, 9, 12, 6, 3, 9, 12, … 3, 9
  - $4^{xi} \bmod 15$ = 1, 4, 1, 4, 1, … 4, 1
  - $5^{xi} \bmod 15$ = 1, 5, 10, 5, 10, 5, … 5, 10
  - $6^{xi} \bmod 15$ = 1, 6, 6, 6, 6, … 6, 6
  - $7^{xi} \bmod 15$ = 1, 7, 4, 13, 1, 7, 4, … 7, 4

¿Y si el módulo no fuese primo? (2/2)

- $8^{xi} \bmod 15 = 1, 8, 4, 2, 1, 8, 4, \ldots 8, 4$
- $9^{xi} \bmod 15 = 1, 9, 6, 9, 6, 9, \ldots 9, 6$
- $10^{xi} \bmod 15 = 1, 10, 10, 10, 10, \ldots 10, 10$
- $11^{xi} \bmod 15 = 1, 11, 1, 11, 1, \ldots 11, 1$
- $12^{xi} \bmod 15 = 1, 12, 9, 3, 6, 12, 9, 3, \ldots 12, 9$
- $13^{xi} \bmod 15 = 1, 13, 4, 7, 1, 13, 4, \ldots 13, 4$
- $14^{xi} \bmod 15 = 1, 14, 1, 14, 1, \ldots 14, 1$



- Nunca se han obtenido o generado todos los restos de n = 15
- Han aparecido unos “anillos”. Esto lo estudiaremos en RSA

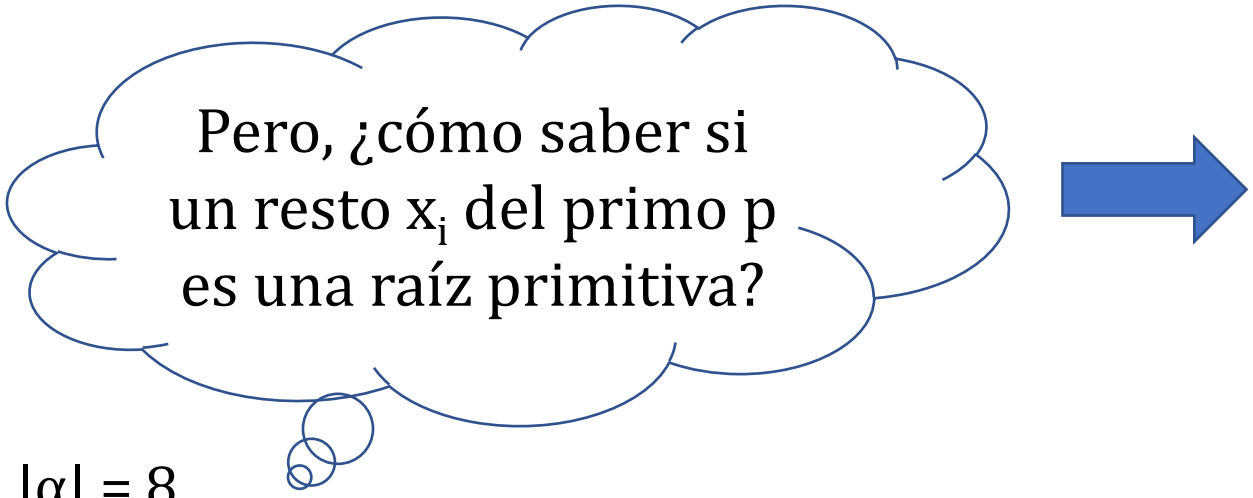
Números candidatos a tener o a ser raíces

- El primo p = 2 no tendrá raíces primitivas porque sus restos son 0 y 1 y ambos valores no generan nada puesto que $0^0 \bmod 2 = 0$ y $0^1 \bmod 2 = 0$ (no se obtiene el resto 1) y $1^0 \bmod 2 = 1$ y $1^1 \bmod 2 = 1$ (no se obtiene el resto 0)
- Como $\alpha^{xi} \bmod p = y_i = CRR$ (con $0 \leq x_i \leq p-1$) y α son restos de p:
  - El resto 0 nunca será una raíz α de p porque $0^{xi} \bmod p = 0 \ \forall \ x_i$
  - El resto 1 nunca será una raíz α de p porque $1^{xi} \bmod p = 1 \ \forall \ x_i$
  - Además, el resto p-1 tampoco será nunca una raíz α de p
  - Los demás restos de p, desde 2 hasta p-2, sí pueden ser raíces y la cantidad de raíces y valores dependerá del primo en cuestión

Raíces primitivas de los primeros primos

Raíces calculadas con el programa SAMCript (|α| es la cantidad de raíces)

- 3 = (2) |α| = 1
- 5 = (2, 3) |α| = 2
- 7 = (3, 5) |α| = 2
- 11 = (2, 6, 7, 8) |α| = 4
- 13 = (2, 6, 7, 11) |α| = 4
- 17 = (3, 5, 6, 7, 10, 11, 12, 14) |α| = 8
- 19 = (2, 3, 10, 13, 14, 15) |α| = 6
- 23 = (5, 7, 10, 11, 14, 15, 17, 19, 20, 21) |α| = 10
- 29 = (2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27) |α| = 12



SAMCript

Buscando raíces primitivas en p

- Existen muchos números dentro del CRR que son raíces del primo p, pero su búsqueda no es algo fácil. Necesitamos tener un procedimiento que nos permita encontrar esos números, diferente a aplicar la fuerza bruta
- Si conociendo la factorización de p-1 obtenemos (q_1, q_2, ... q_n) donde q_i son los factores primos de p-1, diremos que un número g será una raíz α de p si
  - $\forall\ q_i \qquad g^{(p-1)/qi} \bmod p \neq 1$
  - Ejemplo 1: para p = 13, como p-1 = 12 = 2^2 x 3, entonces los valores de q_i serán $q_1 = 2$, $q_2 = 3$
  - Ejemplo 2: para el primo p = 181, como p-1 = 180 = 2^2 x 3^2 x 5, entonces los valores de q_i serán $q_1 = 2$, $q_2 = 3$, $q_3 = 5$
- Si alguno de esos resultados es igual a 1, ese valor de g no será una raíz

Raíces primitivas en el primo p = 13 (1/3)

Si se cumple $g^{(p-1)/qi} \bmod p \neq 1 \ \forall \ q_i$ entonces g será una raíz de p
Sea p = 13, entonces p-1 = 12 = $2^2 * 3$ y $q_1 = 2$ y $q_2 = 3$

Generadores en Z_{13}

2

$2^{(13-1)/2} \bmod 13 = 2^6 \bmod 13 = 12$
$2^{(13-1)/3} \bmod 13 = 2^4 \bmod 13 = 3$ El resto 2 es una raíz primitiva 

$3^{(13-1)/2} \bmod 13 = 3^6 \bmod 13 = 1$
$3^{(13-1)/3} \bmod 13 = 3^4 \bmod 13 = 3$ El resto 3 no es una raíz primitiva

$4^{(13-1)/2} \bmod 13 = 4^6 \bmod 13 = 1$
$4^{(13-1)/3} \bmod 13 = 4^4 \bmod 13 = 9$ El resto 4 no es una raíz primitiva

Raíces primitivas en el primo p = 13 (2/3)

Generadores en Z_{13}

2 6 7

$5^{(13-1)/2} \bmod 13 = 5^6 \bmod 13 = 12$

$5^{(13-1)/3} \bmod 13 = 5^4 \bmod 13 = 1$ El resto 5 no es una raíz primitiva

$6^{(13-1)/2} \bmod 13 = 6^6 \bmod 13 = 12$

$6^{(13-1)/3} \bmod 13 = 6^4 \bmod 13 = 9$ El resto 6 es una raíz primitiva

$7^{(13-1)/2} \bmod 13 = 7^6 \bmod 13 = 12$

$7^{(13-1)/3} \bmod 13 = 7^4 \bmod 13 = 9$ El resto 7 es una raíz primitiva

$8^{(13-1)/2} \bmod 13 = 8^6 \bmod 13 = 12$

$8^{(13-1)/3} \bmod 13 = 8^4 \bmod 13 = 1$ El resto 8 no es una raíz primitiva

Raíces primitivas en el primo p = 13 (3/3)

Generadores en Z_{13}

2 6 7 11

$9^{(13-1)/2} \bmod 13 = 9^6 \bmod 13 = 1$

$9^{(13-1)/3} \bmod 13 = 9^4 \bmod 13 = 9$ El resto 9 no es una raíz primitiva

$10^{(13-1)/2} \bmod 13 = 10^6 \bmod 13 = 1$

$10^{(13-1)/3} \bmod 13 = 10^4 \bmod 13 = 3$ El resto 10 no es una raíz primitiva

$11^{(13-1)/2} \bmod 13 = 11^6 \bmod 13 = 12$

$11^{(13-1)/3} \bmod 13 = 11^4 \bmod 13 = 3$ El resto 11 es una raíz primitiva

$$\alpha_{13} = (2, 6, 7, 11)$$

¿Cuántas raíces primitivas tiene un primo?

- La tasa τ de raíces primitivas en el primo p será aproximadamente
  - $\tau = \phi(p-1)/(p-1)$
  - Donde $\phi(p-1)$ es el Indicador de Euler de (p-1), es decir la cantidad de restos de (p-1) que no tienen factores en común con (p-1), además del 1
- Por ejemplo, si p = 41, entonces p-1 = 40 y $\phi(40) = 16$ $(40 = 2^3*5)$
  - 16 restos: 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39
  - $\tau = \phi(40)/40 = 16/40 = 0{,}40$ (un 40%)
- Pregunta: ¿obtendremos siempre un porcentaje similar?

La tasa τ de raíces depende del primo

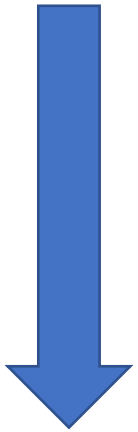
- Si p = 3, p-1 = 2 $\tau = \phi(2)/2 = 1/2 = 0{,}50$ 50%
- Si p = 5, p-1 = 4 $\tau = \phi(4)/4 = 2/4 = 0{,}50$ 50%
- Si p = 7, p-1 = 6 $\tau = \phi(6)/6 = 2/6 = 0{,}33$ 33%
- Si p = 11, p-1 = 10 $\tau = \phi(10)/10 = 4/10 = 0{,}40$ 40%
- Si p = 13, p-1 = 12 $\tau = \phi(12)/12 = 4/12 = 0{,}33$ 33%
- Si p = 17, p-1 = 16 $\tau = \phi(16)/16 = 8/16 = 0{,}50$ 50%
- Si p = 19, p-1 = 18 $\tau = \phi(18)/18 = 6/18 = 0{,}33$ 33%
- Si p = 23, p-1 = 22 $\tau = \phi(22)/22 = 10/22 = 0{,}45$ 45%
- Si p = 29, p-1 = 28 $\tau = \phi(28)/28 = 12/28 = 0{,}43$ 43%
- Si p = 31, p-1 = 30 $\tau = \phi(30)/30 = 8/30 = 0{,}27$ 27%

El porcentaje τ de restos que serán raíces primitivas se encontrará entre el 25% y el % 50%

¿Con qué tipo de primos obtenemos una tasa τ mayor?

Raíces primitivas en primos seguros

- Primo seguro p = 2q + 1, siendo q un primo (interesante en criptografía asimétrica)
- 5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467, 479, …
- Si p = 47, p-1 = 46 $\tau = \phi(46)/46 = 22/46 = 0{,}4783$ 47,83%
- Si p = 59, p-1 = 58 $\tau = \phi(58)/58 = 28/58 = 0{,}4828$ 48,28%
- Si p = 83, p-1 = 82 $\tau = \phi(82)/82 = 40/82 = 0{,}4878$ 48,78%
- Si p = 107, p-1 = 106 $\tau = \phi(106)/106 = 52/106 = 0{,}4906$ 49,06%
- Si p = 167, p-1 = 166 $\tau = \phi(166)/166 = 82/166 = 0{,}4940$ 49,40%
- Si p = 179, p-1 = 178 $\tau = \phi(178)/178 = 88/178 = 0{,}4944$ 49,44%
- Si p = 227, p-1 = 226 $\tau = \phi(226)/226 = 112/226 = 0{,}4956$ 49,56%
- p = 1.048.343, p-1 = 1.048.342 $\tau = \phi(p-1)/p-1 = 524.170/1.048.342$ 49.9999046%



Primos seguros entregan una mayor tasa τ

- A medida que el primo seguro es mayor, la tasa τ se va acercando al valor del 50%
- Comprobación. Sabemos que $\tau = \phi(p-1)/(p-1)$
- Si $p = 2q + 1$, entonces $p-1 = 2q$
- Por lo tanto $\tau = \phi(p-1)/(p-1) = \phi(2q)/2q$
- Pero $\phi(2q) = \phi(2)*\phi(q) = 1*\phi(q) = q-1$
- Luego $\tau = q-1/2q$
- Si q es muy grande, entonces $q-1 \approx q$ y por tanto $\tau \approx ½$ (50%)

Distribución de raíces en primos seguros

- Ejemplo: distribución de las 52 raíces primitivas de p = 107
  - {2, 5, 6, 7, 8, 15, 17, 18, 20, 21, 22, 24, 26, 28, 31, 32, 38, 43, 45, 46, 50, 51, 54, 55, 58, 59, 60, 63, 65, 66, 67, 68, 70, 71, 72, 73, 74, 77, 78, 80, 82, 84, 88, 91, 93, 94, 95, 96, 97, 98, 103, 104}
  - Se asemeja a una distribución uniforme, hay largas cadenas de números seguidos y consecutivos {5, 6, 7, 8}, {20, 21, 22}, {58, 59, 60}, {65, 66, 67, 68}, {70, 71, 72, 73, 74}, {93, 94, 95, 96, 97, 98} y es bastante frecuente observar una separación entre números raíces igual a 2 o 3
- Por tanto, si en la ecuación $g^{(p-1)/qi} \bmod p \neq 1$ para saber si g es una raíz primitiva de p, elegimos un valor g que no resulta ser una raíz primitiva, la posibilidad de que g+1 o g+2 sí lo sea, será muy alta

Uso de raíces primitivas en la criptografía

- La utilidad de este concepto en criptografía lo veremos cuando se estudien los sistemas de clave pública y, en particular, el protocolo de intercambio de claves de Diffie Hellman
- También se recurrirá a esto cuando estudiemos la firma digital según Elgamal y el estándar de firma digital DSA Digital Signature Algorithm
- Pregunta. ¿Será fácil encontrar las primeras raíces primitivas de un primo p muy grande, por ejemplo de 2.048 bits? No, porque habrá que factorizar el valor p-1, que será un trabajo muy costoso
- ¿Solución? Usar como raíz primitiva un número pequeño (por ejemplo 2 o 5), aunque no lo sea, sin comprobarlo, tal y como lo hace OpenSSL ¿inseguro? 
- Como los números son tan grandes, en la práctica el sistema no será inseguro

Importancia de las raíces primitivas

- En criptografía de clave pública, por ejemplo intercambio de clave de Diffie y Hellman, el usuario calcula su clave pública **y** usando la siguiente ecuación: **y** = α^{x} mod p, siendo p un primo, α una raíz primitiva de p y **x** su clave privada

- Sea x = 18, p = 31, α = 3 (raíz)
- y = 3^{18} mod 31 = 4
- Como 3 es una raíz primitiva de 31, el único valor privado que entrega un valor público 4 será el número 18, porque y = 3^{xi} mod 31 entrega todos sus resultados diferentes

- Sea x = 18, p = 31, α = 2 (no raíz)
- y = 2^{18} mod 31 = 8
- Como 2 no es una raíz primitiva de 31, habrá más de un número x_i que la ecuación y = 2^{xi} mod 31 entregue como resultado el valor público 8
- Por ejemplo x_i = 3, 8, 13, 18, 23 y 28

Conclusiones de la Lección 2.6

- Los restos α son raíces primitivas en un primo p si cumplen con la condición de que $\alpha^{xi} \bmod p = y_i$ entrega números distintos para $0 \leq xi \leq p-1$
- En este caso de raíz primitiva, para un valor y_i existirá un único número x_i que cumpla con la ecuación anterior (muy interesante en criptografía asimétrica)
- Si no se usa una raíz primitiva α sino otro resto g, entonces habrá al menos dos valores de x_i que $g^{xi} \bmod p = y_i$ entregue el mismo valor y_i
- Si x es una clave privada que genera una clave pública $y = \alpha^x \bmod p$, entonces encontrar qué exponente x le corresponde al número y, significa resolver el problema del logaritmo discreto PLD, de muy difícil solución si p es grande
- La tasa de raíces primitivas τ se encuentra entre el 25% y el 50%
- Si p es un primo seguro, la tasa de raíces primitivas τ acerca al 50%

Un proyecto sin ánimo de lucro

- Class4crypt es un proyecto sin ánimo de lucro
- Si te ha gustado el vídeo, has aprendido algo nuevo o bien has podido reforzar algún conocimiento que ya tenías
- Entonces, por favor, pon un "**Me gusta**" al vídeo
- Si deseas expresar alguna opinión sobre el contenido de esta clase o tienes alguna duda, hazlo por favor en YouTube. Todos los comentarios serán muy bien recibidos y las dudas que plantees serán contestadas a la mayor brevedad posible

¡Muchas gracias!

Lectura recomendada

Fin de la clase 2.6

- Euler's Totient Calculator
  - http://www.javascripter.net/math/calculators/eulertotientfunction.htm
- Primitive root modulo n / List of prime numbers, Wikipedia
  - https://en.wikipedia.org/wiki/List_of_prime_numbers
  - https://en.wikipedia.org/wiki/Primitive_root_modulo_n
- List of safe primes
  - https://prime-numbers.info/list/safe-primes-page-4
- SAMCript: Software de Aritmética Modular para Criptografía, María Nieto Díaz, dirección Jorge Ramió, 2018
  - http://www.criptored.upm.es/software/sw_m001t.htm

Más lecciones en el canal Class4crypt

Fuera webcam y dentro música

SUSCRIBIRSE

1.540 suscriptores
13 octubre 2020

- https://www.youtube.com/user/JorgeRamio

Licencia y créditos

- Estas videoclases y la documentación utilizada en ellas están publicadas bajo licencia *Creative Commons* tipo CC BY-NC-ND 4.0
  - Reconocimiento - No Comercial - Sin Obra Derivada

- Esto 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

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

Próximamente una nueva videoclase de criptografía aplicada en Class4crypt

Criptosaludos