Class4crypt

Aula virtual de criptografía aplicada

Clase c4c3.2

El problema de la mochila

Madrid, martes 27 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 (1/2)

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 (2/2)

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
34. Fundamentos de complejidad algorítmica
35. El problema de la mochila

Estadísticas del canal Class4crypt

Tu canal ha conseguido 20.544 visualizaciones en los últimos 365 días

¡COMENZAMOS!

Class4crypt c4c3.2

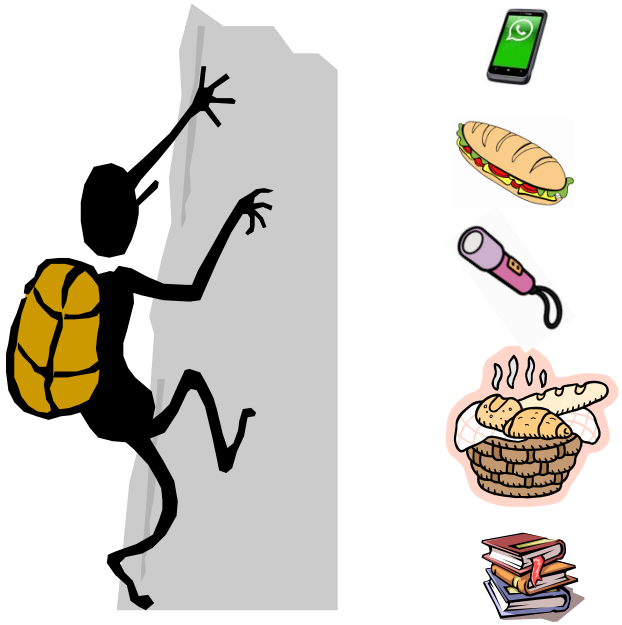
Módulo 3. Complejidad algorítmica en la criptografía

Lección 3.2. El problema de la mochila

1. Enunciado simple del problema de la mochila
2. Resolución de un problema de mochila
3. Uso en criptografía: mochila tramposa de Merkle y Hellman
4. Ejemplo de cifrado asimétrico con mochila de Merkle y Hellman

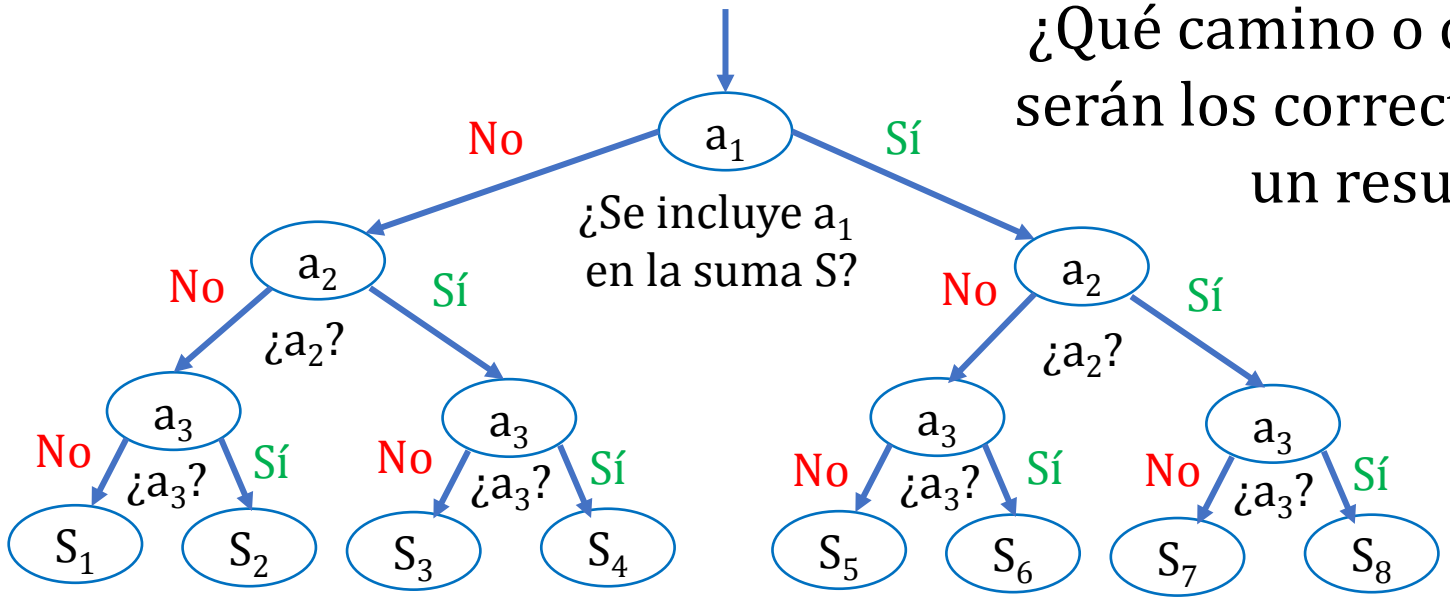
El problema de la mochila

- Dada una mochila de dimensiones de alto, ancho y fondo conocidas, y un conjunto de elementos de distintos tamaños menores que ella y de cualquier dimensión, ... ¿es posible llenar la mochila al 100% con distintos elementos de ese conjunto?
- Dichos elementos, además de un volumen, pueden tener un peso específico o valor
- Resolución: vuelta atrás (*backtracking*), ramificación y poda (*branch and bound*)



Mochila con solución por fuerza bruta

Sea A = {a_1, a_2, a_3} y el objetivo S (un valor resultado de una suma con los elementos de A)



¿Qué camino o caminos serán los correctos para un resultado S?

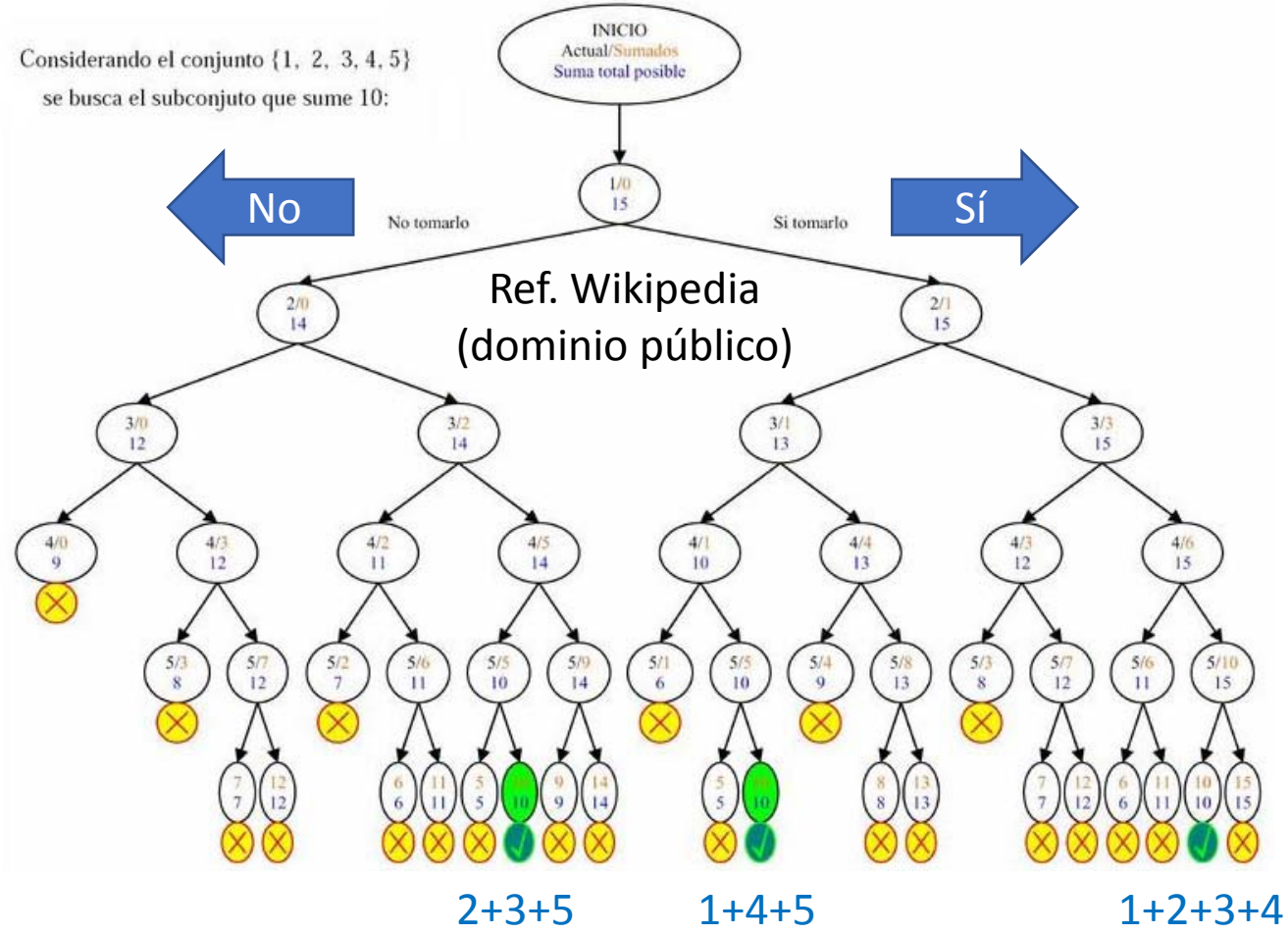
Habrá $2^3 = 8$ estados (si A tiene n números, habrá 2^n, carácter exponencial)

$S_1 = \varnothing$ $S_2 = a_3$ $S_3 = a_2$ $S_4 = a_2 + a_3$

$S_5 = a_1$ $S_6 = a_1 + a_3$ $S_7 = a_1 + a_2$ $S_8 = a_1 + a_2 + a_3$

$S_1 = 000$, $S_2 = 001$, $S_3 = 010$, $S_4 = 011$, $S_5 = 100$, $S_6 = 101$, $S_7 = 110$, $S_8 = 111$

Mochila con solución *branch and bound*



- Para el objetivo suma 10, hay tres soluciones: 2+3+5, 1+4+5 y 1+2+3+4
- En vez de $2^5 = 32$, hay 24 ramas
- Aquí resulta muy obvio sumar y se puede hacer mentalmente
- Si son muchos los números, o bien estos tienen decimales, el problema sería más difícil
- Lo mismo si se usan muchos números enteros y muy grandes, como ocurre en los algoritmos criptográficos

Operaciones en la solución de la mochila

- Dada la siguiente secuencia S = {S_1, S_2, S_3, ..., S_{m-2}, S_{m-1}, S_m} de m números enteros positivos y un valor T, se pide encontrar un subconjunto S_S = {S_a, S_b, ..., S_j}, que cumpla con ese objetivo T
  - $T = \Sigma S_S = S_a + S_b + ... + S_j$
- Si los elementos de la mochila son números grandes, no están ordenados y no siguen una distribución supercreciente (en que S_i es mayor que la suma de los anteriores S_j) el problema es tipo NP
- Se trata de encontrar los vectores binarios V_i de forma que se cumpla la relación $\Sigma (S_i * V_i) = T$

Interés de las mochilas en la criptografía

- Aplicación en la criptografía asimétrica con dos claves, una de ellas pública y la otra privada, inversas entre sí dentro de un módulo
- Se puede usar el problema de la mochila, para permitir realizar una operación de cifra rápida y fácil y, por el contrario, su ataque resulte muy difícil, al ser un problema del tipo NP completo
- Si los elementos de esa mochila son números enteros, la solución al problema -en el caso de que exista solución- será única y fácil
- Esto se da cuando los números $S = \{s_1, s_2, s_3, s_4, \ldots s_{n-1}, s_n\}$ forman una cadena supercreciente, es decir que el número siguiente de la lista es mayor que la suma de los todos s_j anteriores

Cifrado con mochila de Merkle y Hellman

- En 1978 (pocos meses después que RSA) Ralph Merkle y Martin Hellman proponen un sistema de cifra de clave pública denominado mochila tramposa
- Cada usuario crea una mochila difícil (desordenada, clave pública) a partir de una mochila simple (supercreciente, clave privada)
- En el cifrado se usa la mochila difícil (pública) del receptor y en el descifrado se usa la mochila simple (privada) de ese receptor
- Para la cifra se usan los bits 1 del texto en claro para contar con el número que se encuentra en esa posición de la mochila difícil o pública del destino, y los bits ceros para no tenerlo en cuenta
- Se puede pasar fácilmente de la mochila simple a la difícil o viceversa usando una trampa, que solo posee el dueño de la clave

Diseño mochila de Merkle y Hellman

1. Se selecciona una mochila supercreciente de m elementos $S' = \{S_1', S_2', ..., S_m'\}$
2. Se elige un entero μ (módulo de trabajo) mayor que la suma de los elementos de la mochila $\mu > \sum_{i=1}^{m} S_i'$ $\mu \geq 2*S_m'$
3. Se elige un entero ω primo relativo con μ $\omega^{-1} = inv(\omega, \mu)$
4. Se multiplica $\omega*S'$ mod μ, obteniendo una mochila difícil $S = \{S_1, S_2, ..., S_m\}$ $S_i = \omega*S_i' \bmod \mu$
5. La clave pública será $S = \{S_1, S_2, ..., S_m\}$ y la clave privada será (ω^{-1}, μ)
6. Cifrado: $C = M*S$ (M en bits) --- Descifrado: $M = \omega^{-1}*C \bmod \mu$

Ejemplo de cifrado con mochila de MH

- $S' = \{S'_1, S'_2, S'_3, S'_4, S'_5, S'_6, S'_7, S'_8\} = \{40, 75, 201, 488, 1.013, 2.001, 3.919, 8.106\}$
- Elegimos $\mu \geq 2*S_m' \geq 2*8.106 = 16.212$, sea $\mu = 16.250$
- Si elegimos $\omega = 171$ [mcd $(\omega, \mu) = 1$], $\omega^{-1} = \text{inv}(\omega, \mu) = \text{inv}(171, 16.250) = 3.231$
- Calculamos nuestra clave pública: $S_i = \omega * S_i' \bmod \mu$

  $S_1 = 171*40 \bmod 16.250 = 6.840$ $S_2 = 171*75 \bmod 16.250 = 12.825$

  $S_3 = 171*201 \bmod 16.250 = 1.871$ $S_4 = 171*488 \bmod 16.250 = 2.198$

  $S_5 = 171*1.013 \bmod 16.250 = 10.723$ $S_6 = 171*2.001 \bmod 16.250 = 921$

  $S_7 = 171*3.919 \bmod 16.250 = 3.899$ $S_8 = 171*8.106 \bmod 16.250 = 4.876$

- Clave pública $S = \{S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8\}$
  - $S = \{6.840, 12.825, 1.871, 2.198, 10.723, 921, 3.899, 4.876\}$
- Cifrar el texto Hola = 01001000 01101111 01101100 01100001

SAMCript

Cifrando con mochila pública de MH

- Nuestra clave pública
  - S = {6.840, 12.825, 1.871, 2.198, 10.723, 921, 3.899, 4.876}
- Nuestra clave privada
  - μ = 16.250, ω^{-1} = 3.231, S' = S*ω^{-1} mod μ = {40, 75, 201, 488, 1.013, 2.001, 3.919, 8.106}
- Alguien nos enviará cifrado Hola = 01001000 01101111 01101100 01100001
  - 01001000 Pasando por clave pública: 12.825 + 10.723 = 23.548
  - 01101111 Pasando por clave pública: 12.825 + 1.871 + 10.723 + 921 + 3.899 + 4.876 = 35.115
  - 01101100 Pasando por clave pública: 12.825 + 1.871 + 10.723 + 921 = 26.340
  - 01100001 Pasando por clave pública: 12.825 + 1.871 + 4.876 = 19.572
- C = 23.548, 35.115, 26.340, 19.572 (cuatro números)
  - Como los números de este ejemplo son muy pequeños y la mochila tiene muy pocos elementos, además de un tamaño 8 (byte), no sería tan difícil recuperar el mensaje usando la clave pública

Descifrando con mochila privada de MH (1)

- Nuestra clave privada
  - μ = 16.250
  - ω^{-1} = 3.231
  - $S' = S*\omega^{-1} \bmod \mu = \{S'_1, S'_2, S'_3, S'_4, S'_5, S'_6, S'_7, S'_8\}$
  - S' = {40, 75, 201, 488, 1.013, 2.001, 3.919, 8.106}
- Criptograma
  - C = 23.548, 35.115, 26.340, 19.572
- Calculamos $M_i = C_i*\omega^{-1} \bmod \mu$ y se recorre una sola vez la mochila simple de derecha a la izquierda. Si el elemento S'_i está en la suma, siempre lo estará
- Se descuenta ese número de M_i y se continúa con el proceso hasta llegar al valor 0
- La solución de M_i será única

Descifrando con mochila privada de MH (2)

- μ = 16.250, ω^{-1} = 3.231, S' {40, 75, 201, 488, 1.013, 2.001, 3.919, 8.106}
- Criptograma: C = 23.548, 35.115, 26.340, 19.572
  - $M_1 = C_1 * \omega^{-1} \bmod \mu$ = 23.548*3.231 mod 16.250 = 1.088
    - M_1 = 1.013 + 75 = 01001000 = H
  - $M_2 = C_2 * \omega^{-1} \bmod \mu$ = 35.115*3.231 mod 16.250 = 15.315
    - M_2 = 8.106 + 3.919 + 2.001 + 1.013 + 201 + 75 = 01101111 = o
  - $M_3 = C_3 * \omega^{-1} \bmod \mu$ = 26.340*3.231 mod 16.250 = 3.290
    - M_3 = 2.001 + 1.013 + 201 + 75 = 01101100 = l
  - $M_4 = C_4 * \omega^{-1} \bmod \mu$ = 19.572*3.231 mod 16.250 = 8.382
    - M_4 = 8.106 + 201 + 75 = 01100001 = a
- M = Hola (se ha recuperado el texto en claro, con confidencialidad)

Otras mochilas en la criptografía

- El cifrado con mochila de Merkle y Hellman fue roto por Adi Shamir y Richard Zippel en 1982
  - Mayor información sobre este ataque en la bibliografía: Libro Electrónico de Seguridad Informática y Criptografía
- Además del algoritmo de cifrado con mochila de Merkle y Hellman, hubo otros sistemas propuestos, entre ellos Graham-Shamir, Morii-Kasahara , Chor-Rivest y Goodman-McAuley
  - Mayor información en documento Universidad de California que se incluye en la bibliografía

Conclusiones de la Lección 3.2

- El problema de la mochila es un ejemplo de problema matemático con tiempo de ejecución NP, es decir polinomial no determinista
- Para su resolución, pueden usarse técnicas de vuelta atrás (backtracking) y ramificación y poda (branch and bound), que significa recorrer varios caminos diferentes, donde solo alguno o algunos de ellos entregan la solución
- La mochila de Merkle y Hellman de 1978, es un sistema de cifra asimétrica propuesto unos meses después de RSA
- Permite cifrar un mensaje conociendo la clave pública del destinatario (una mochila difícil) permitiendo confidencialidad en el envío
- El destino descifra el criptograma con su mochila simple supercreciente, que es inversa de la difícil y que sólo conoce su dueño gracias a una trampa

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 (1/2)

- Knapsack problema / Vuelta atrás, Wikipedia
  - https://en.wikipedia.org/wiki/Knapsack_problem
  - https://es.wikipedia.org/wiki/Vuelta_atr%C3%A1s
- Teoría de Algoritmos, Curso de Análisis y Diseño de Algoritmos (Backtracking, vuelta atrás), Fernando Berzal Galiano, Univ. de Granada
  - http://elvex.ugr.es/decsai/algorithms/
- Capítulo 13 Cifrado asimétrico con mochilas, Libro Electrónico de Seguridad Informática y Criptografía versión 4.1, Jorge Ramió, marzo de 2006
  - http://www.criptored.upm.es/guiateoria/gt_m001a.htm

Lectura recomendada (2/2)

Fin de la clase 3.2

- RapidTables
  - https://www.rapidtables.com/convert/number/ascii-to-binary.html
- SAMCript: Software de Aritmética Modular para Criptografía, María Nieto Díaz, dirección Jorge Ramió, 2018
  - http://www.criptored.upm.es/software/sw_m001t.htm
- Merkle-Hellman Knapsack Encryption
  - https://asecuritysite.com/encryption/knapcode
- Knapsack Cryptosystems: The Past and the Future, Dept. of Information and Computer Science, University of California, Ming Kin Lai, 2001
  - http://ljk.imag.fr/membres/Jean-Guillaume.Dumas/Enseignements/ProjetsCrypto/sac-a-dos-LLL/knapsack.html

Más lecciones en el canal Class4crypt

Fuera webcam y dentro música

SUSCRIBIRSE

1.590 suscriptores
27 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