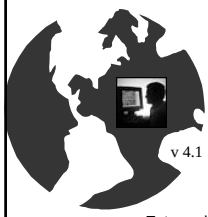
Capítulo 13
Cifrado Asimétrico con Mochilas

Seguridad Informática y Criptografía



Material Docente de
Libre Distribución

Ultima actualización del archivo: 01/03/06
Este archivo tiene: 30 diapositivas

Dr. Jorge Ramió Aguirre
Universidad Politécnica de Madrid

El problema de la mochila

El problema matemático de la mochila, referido ahora a números y no a los elementos físicos que puedan entrar en ella, se plantea como sigue:

Dada la siguiente secuencia de m números enteros positivos $S = \{S_1, S_2, S_3, ..., S_{m-2}, S_{m-1}, S_m\}$ y un valor u objetivo T, se pide encontrar un subconjunto de S $S_S = \{S_a, S_b, ..., S_j\}$ que cumpla con ese objetivo T:

$$T = \Sigma\, S_S = S_a + S_b + ... + S_j$$

Solución al problema de la mochila

Si los elementos de la mochila son números grandes, no están ordenados y no siguen una distribución supercreciente -en este tipo de distribución el elemento iésimo S_i de la mochila es mayor que la suma de todos sus antecesores-, la resolución de este problema es de tipo no polinomial.

Se trata de encontrar los vectores V_i de 0s y 1s de forma que:

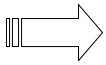
$$\Sigma S_i * V_i = T$$

Si se cumple esta relación, la mochila tiene solución. En caso contrario, no existirá solución.

Un ejemplo del problema de la mochila

Tenemos la mochila S = {20, 5, 7, 36, 13, 2} con m = 6 y el valor T = 35. Se pide encontrar una solución, si es que ésta existe, en una única vuelta. En este momento no importa que los valores de la mochila no estén ordenados.

SOLUCIÓN: Sin hacer ningún cálculo mental, podemos recorrer todos los valores (se puede descartar el elemento S_4 pues es mayor que el objetivo T) de la mochila S, bien de izquierda a derecha o al revés (da igual el sentido elegido) y restaremos el elemento iésimo si es menor que el objetivo T en esa etapa del algoritmo, como se indica:



Solución al ejemplo de la mochila

$S = \{S_1, S_2, S_3, S_4, S_5, S_6\} = \{20, 5, 7, 36, 13, 2\}$ $T = 35$

$S_1 = 20$ ¿Es menor que objetivo T = 35? Sí $\Rightarrow$ T = 35-20 = 15
$S_2 = 5$ ¿Es menor que objetivo T = 15? Sí $\Rightarrow$ T = 15-5 = 10
$S_3 = 7$ ¿Es menor que objetivo T = 10? Sí $\Rightarrow$ T = 10-7 = 3
$S_4 = 36$ ¿Es menor que objetivo T = 3? No $\Rightarrow$ T = 3
$S_5 = 13$ ¿Es menor que objetivo T = 3? No $\Rightarrow$ T = 3
$S_6 = 2$ ¿Es menor que objetivo T = 3? Sí $\Rightarrow$ T = 3-2 = 1 $\neq$ 0

Se ha recorrido toda la mochila y no se ha encontrado solución.

En cambio sí existe una solución:

$S_S = \{S_1+S_5+S_6\} = 20+13+2 = 35 \Longrightarrow$ $V_i = [1,0,0,0,1,1]$

¿Puede haber soluciones múltiples?

Si para la misma mochila S = {20, 5, 7, 36, 13, 2} buscamos ahora el valor T = 27, encontramos tres soluciones válidas:

$S_{S1} = \{S_1+S_3\} = 20+7$ $S_{S2} = \{S_1+S_2+S_6\} = 20+5+2$

$S_{S3} = \{S_2+S_3+S_5+S_6\} = 5+7+13+2$

Esto sería inadmisible en un sistema de cifra puesto que el resultado de una operación de descifrado debe ser única ya que proviene de un único mensaje. La solución será el uso de las denominadas mochilas simples en que la solución al problema de la mochila, si existe, es única.

Mochila simple o supercreciente

Una mochila es simple o supercreciente si el elemento S_k es mayor que la suma de los elementos que le anteceden:

$$S_k > \sum_{j=1}^{k-1} S_j$$

Por ejemplo, la mochila S = {2, 3, 7, 13, 28, 55, 110, 221} con m = 8 elementos es supercreciente y la solución para un objetivo T = 148 es única: $V_i = [S_2+S_3+S_5+S_7]$.

Para resolver cualquier valor T válido para esta mochila, ésta se recorre de derecha a izquierda (desde el valor mayor al menor) una sola vez con el algoritmo ya visto.

Compruebe que para T = 289, 196 y 353 los vectores son V_1 = 00010101; V_2 = 01001110; V_3 = 10110011.

Operación de cifra con mochila simple

Se representa la información en binario y se pasan los bits por la mochila. Los bits 1s incluyen en la suma el elemento al que apuntan y los bits 0s no.

Con la mochila S = {2, 4, 10, 19, 40} de m = 5 elementos cifraremos el mensaje M = ADIOS.

SOLUCIÓN: Usando código ASCII/ANSI: A = 01000001; D = 01000100; I = 01001001; O = 01001111; S = 01010011

M = 01000 00101 00010 00100 10010 10011 11010 10011

C = (4), (10+40), (19), (10), (2+19), (2+19+40), (2+4+19), (2+19+40)

C = 4, 50, 19, 10, 21, 61, 25, 61

Descifrado con mochila simple

C = 4, 50, 19, 10, 21, 61, 25, 61 | S = {2, 4, 10, 19, 40}

La operación de descifrado es elemental: pasamos por la mochila los valores de C, encontramos el vector V_i y por último agrupamos el resultado en grupos de 8 bits. En este caso $4 \Rightarrow V_i = 01000$, $50 \Rightarrow V_i = 00101$, etc.

PROBLEMA: Es muy fácil cifrar y descifrar pero también criptoanalizar el sistema de cifra porque se usa una mochila simple.

Una posible solución es usar mochilas de Merkle y Hellman.

Mochila de Merkle y Hellman MH

- En 1978 Ralph Merkle y Martin Hellman proponen un sistema de cifra de clave pública denominado Mochila con Trampa.
- El algoritmo se basa en crear una mochila difícil a partir de una mochila simple de forma que el cifrado se haga con la mochila difícil y el descifrado con la mochila simple o fácil. Se puede pasar fácilmente de la mochila simple a la difícil o viceversa usando una trampa.

La trampa será nuestra clave secreta.
La mochila difícil será nuestra clave pública.

http://www-fs.informatik.uni-tuebingen.de/~reinhard/krypto/English/4.5.3.e.html

Diseño mochila de Merkle y Hellman (1)

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.

$$\mu > \sum_{i=1}^{m} S_i'$$

más fácil: $\mu \geq 2 * S_m'$

3. Se elige un entero ω primo relativo con μ.

$$mcd(\omega, \mu) = 1$$

Se asegura el inverso

Se recomienda que ω no tenga factores con los elementos de S'

4. Se multiplica S' por ω mod μ. $S_i = \omega * S_i' \bmod \mu$

Obteniendo una mochila difícil $S = \{S_1, S_2, ..., S_m\}$

Diseño mochila de Merkle y Hellman (2)

5. Se calcula el inverso de ω en el cuerpo μ. $\omega^{-1} = inv(\omega, \mu)$

Clave privada: μ, ω^{-1}

Clave pública: mochila S

Esto se interpreta como encontrar los vectores que cumplan con un valor de T.

CIFRADO:	DESCIFRADO:
$C = S * M$	$M = \omega^{-1} * C \bmod \mu$
como $S = \omega * S' \bmod \mu$	Entonces obtenemos:
$C = \omega * S' * M \bmod \mu$	$S' * M$

Cifrado mochila de Merkle y Hellman (1)

Se pide cifrar el mensaje codificado en ASCII M = Sol usando la mochila simple y supercreciente S' = {3, 5, 12, 21}.

1. Elección de μ: $\mu \geq 2*S'_4 \geq 2*21$ $\mu = 49$
2. Elección de ω: mcd (ω, μ) = 1 $\omega = 32 \Rightarrow \omega^{-1} = 23$
3. Mochila S: $S = \omega * S' \bmod \mu$

$S_1 = 32 * 3 \bmod 49 = 96 \bmod 49 = 47$

$S_2 = 32 * 5 \bmod 49 = 160 \bmod 49 = 13$

$S_3 = 32 * 12 \bmod 49 = 384 \bmod 49 = 41$

$S_4 = 32 * 21 \bmod 49 = 672 \bmod 49 = 35$

Clave pública: S = {47,13,41,35} Clave privada: $\mu = 49$, $\omega^{-1} = 23$

Cifrado mochila de Merkle y Hellman (2)

Clave pública: S = {47,13,41,35} Clave privada: $\mu = 49$, $\omega^{-1} = 23$

Como m = 4, cifraremos bloques de 4 bits, convirtiendo el mensaje a su equivalente en binario del código ASCII.

Cifrado: M = Sol = 0101 0011 0110 1111 0110 1100

C = (13+35), (41+35), (13+41), (47+13+41+35), (13+41), (47+13)

C = 48, 76, 54, 136, 54, 60

Observe que se repite el valor 54 puesto que m = 4 sería una muy mala elección.

Descifrado mochila de Merkle y Hellman

Clave pública: S = {47,13,41,35} | Clave privada: $\mu = 49$, $\omega^{-1} = 23$

Cifrado: M = Sol = 0101 0011 0110 1111 0110 1100

C = 48, 76, 54, 136, 54, 60

Como S' = {3,5,12,21}

Descifrado:

23∗48 mod 49 = 1.104 mod 49 = 26	23∗136 mod 49 = 3.128 mod 49 = 41
23∗76 mod 49 = 1.748 mod 49 = 33	23∗54 mod 49 = 1.242 mod 49 = 17
23∗54 mod 49 = 1.242 mod 49 = 17	23∗60 mod 49 = 1.380 mod 49 = 8

M = 0101 0011 0110 1111 0110 1100 = Sol

Valores de diseño de mochilas M-H (1)

Merkle y Hellman proponen los siguientes parámetros:

a) Tamaño de la mochila $m \geq 100$

b) Módulo μ uniforme en el siguiente intervalo:

Intervalo μ: $[2^{2m+1}+1, 2^{2m+2}-1] \Rightarrow 2m+2$ bits

Si m = 100: todos los elementos de S son de 202 bits.

c) Valores de S_i' elegidos uniformemente en el intervalo:

Intervalo S_i': $[(2^{i-1}-1)*2^m+1, 2^{i-1}*2^m]$

Si m = 100: $1 \leq S_1' \leq 2^{100} \leq S_2' \leq 2^{101} \leq S_3' \leq 2^{102}$ ...

d) Elegir un valor x en el intervalo $[2, \mu-2]$. El factor ω se calcula como: $\omega = mcd(\mu, x)$

Mochila con parámetros proporcionales (1)

a) Mochila con m = 6

Todos estos elementos serán de (2m+2) = 14 bits

b) Intervalo μ: $[2^{2m+1}+1, 2^{2m+2}-1] = [2^{2*6+1}+1, 2^{2*6+2}-1]$

$[2^{13}+1, 2^{14}+1] = [8.193, 16.385]$ Sea $\mu = 13.515$

c) Elección de los valores S'_i:

i=1 : $[(2^{1-1}-1)*2^6+1, (2^{1-1})*2^6]$ $1 \le S_1' \le 64$

i=2 : $[(2^{2-1}-1)*2^6+1, (2^{2-1})*2^6]$ $65 \le S_2' \le 128$

i=3 : $[(2^{3-1}-1)*2^6+1, (2^{3-1})*2^6]$ $193 \le S_3' \le 256$

i=4 : $[(2^{4-1}-1)*2^6+1, (2^{4-1})*2^6]$ $449 \le S_4' \le 512$

i=5 : $[(2^{5-1}-1)*2^6+1, (2^{5-1})*2^6]$ $961 \le S_5' \le 1.024$

i=6 : $[(2^{6-1}-1)*2^6+1, (2^{6-1})*2^6]$ $1.985 \le S_6' \le 2.048$

UNA ELECCIÓN

$S_1' = 39$

$S_2' = 72$

$S_3' = 216$

$S_4' = 463$

$S_5' = 1.001$

$S_6' = 1.996$

Mochila con parámetros proporcionales (2)

d) Cálculo del factor ω. Buscamos un valor x en el intervalo $[2, \mu-2] = [2, 13.513]$, por ejemplo x = 9.805.

Como el máximo común divisor entre $\mu = 13.515$ y x = 9.805 es 265, luego $\omega = 9.805/265 = 37$.

Vamos a elegir:

$\omega = 37$ de forma que $\omega^{-1} = 4.018$ inv (37, 13.515) = 4.018

Luego, la mochila simple y la clave privada serán:

Mochila simple: $S' = \{39, 72, 216, 463, 1.001, 1.996\}$

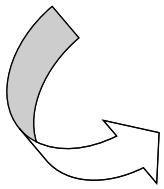
Clave Privada: $\mu = 13.515$ $\omega^{-1} = 4.018$

Mochila con parámetros proporcionales (3)

Mochila simple:

S' = {39, 72, 216, 463, 1.001, 1.996} Módulo: $\mu = 13.515$

Factor multiplicador: $\omega = 37$; $\omega^{-1} = 4.018 \Rightarrow$ Clave privada



$S_1 = 39*37 \bmod 13.515 = 1.443$
$S_2 = 72*37 \bmod 13.515 = 2.664$
$S_3 = 216*37 \bmod 13.515 = 7.992$
$S_4 = 463*37 \bmod 13.515 = 3.616$
$S_5 = 1.001*37 \bmod 13.515 = 10.007$
$S_6 = 1.996*37 \bmod 13.515 = 6.277$

Mochila difícil:

S = {1.443, 2.664, 7.992, 3.616, 10.007, 6.277} $\Rightarrow$ Clave pública

Fortaleza de las mochilas M-H

En el año 1982 Adi Shamir y Richard Zippel encuentran debilidades a las mochilas de Merkle-Hellman:

- Si se conoce el módulo μ (o bien éste puede deducirse) ...
- Y si los dos primeros elementos (S_1 y S_2) de la mochila difícil se corresponden con los dos primeros elementos (S_1' y S_2') de la mochila simple y son primos con μ ...
- Entonces podemos generar la mochila simple a partir de la difícil ya que encontraremos la clave secreta ω^{-1} ... 💣
- Esta debilidad no hace recomendable el uso de mochilas de M-H para el cifrado de la información ... ☹

http://www.behdad.org/download/Presentations/knapsack/knapsack.ppt

Criptoanálisis de Shamir y Zippel

Este ataque exige fuertes restricciones. Para una mochila con 100 elementos, los autores suponen:

a) Que los dos primeros elementos de S' de 100 y 101 bits son mucho más pequeños que el módulo μ de 202 bits.

b) Que podemos identificar los elementos S_1 y S_2 en la mochila difícil y hacerlos corresponder con S_1' y S_2'.

c) Que conocemos el módulo μ o podemos deducirlo.

- Con estos datos se trata de encontrar los valores de S_1' y S_2' además del factor de multiplicación ω.
- Con estos valores generamos la mochila fácil S.

Pasos del ataque de Shamir y Zippel (1)

1. Se calcula $q = (S_1/S_2) \bmod \mu$

   Como $S_i = S_i' * \omega \bmod \mu$ entonces:

   $q = (S_1'/S_2') \bmod \mu = [S_1' * \text{inv}(S_2', \mu)] \bmod \mu$

   Esto implica una condición fuerte: $\text{mcd}(S_2', \mu) = 1$

2. Se calculan todos los múltiplos modulares del valor q con multiplicadores en el rango $[1, 2^{m+1}] = [1, 2^{101}]$

   $CM = \{1*q \bmod \mu, 2*q \bmod \mu, ..., 2^{m+1}*q \bmod \mu\}$

3. El candidato para S_1' será el valor más pequeño de CM puesto que ese elemento podría ser el más pequeño de la mochila fácil S'.

Pasos del ataque de Shamir y Zippel (2)

4. Encontrado el candidato para S_1'se calcula:
   $\omega = (S_1/S_1') \bmod \mu = [S_1 * \text{inv}(S_1', \mu)] \bmod \mu$
   Esto implica otra condición fuerte: $\text{mcd}(S_1', \mu) = 1$
5. Conocido ω encontramos $\omega^{-1} = \text{inv}(\omega, \mu)$ y así calculamos todos los elementos de la mochila $S_i' = S_i * \omega^{-1} \bmod \mu$ que debería ser de tipo supercreciente o fácil.
6. Si no se genera una mochila supercreciente, se elige el siguiente valor más pequeño del conjunto CM y así hasta recorrer todos sus valores. Si con este conjunto CM no se obtiene una mochila simple, se repite el punto 2 tomando ahora valores en el rango 2^{m+i} con i = 2, 3, etc. Por lo general el ataque prospera con el primer conjunto CM.

Ejemplo de ataque de Shamir y Zippel (1)

La clave pública de un sistema de mochila Merkle-Hellman es:
$S = \{S_1, S_2, S_3, S_4, S_5\} = \{3.241, 572, 2.163, 1.256, 3.531\}$
Si de alguna forma hemos conseguido conocer que el módulo $\mu = 4.089$, se pide encontrar la mochila fácil $S' = \{S_1', S_2', S_3', S_4', S_5'\}$.

Solución:

- $q = S_1/S_2 \bmod \mu = S_1 * \text{inv}(S_2, \mu) \bmod \mu$. Calculamos ahora $\text{inv}(S_2, \mu)$ es decir inv (572, 4,089) = 309, luego $q = 3.241 * 309 \bmod 4.089 = 599$.
- Múltiplos CM = $\{1*q \bmod \mu, 2*q \bmod \mu, 3*q \bmod \mu, ..., 64*q \bmod \mu\}$ puesto que la mochila tiene m = 5 elementos y el intervalo será $[1, 2^{5+1}]$.
- Luego CM = [599, 1.198, 1.797, 2.396, 2.995, 3.594, 104, 703, 1.302, 1.901, 2.500, 3.099, 3.698, 208, 807, 1.406, 2.005, 2.604, 3.203, 3.802, 312, 911, 1.510, 2.109, 2.708, 3.307, 3.906, 416, 1.015, 1.614, 2.213, 2.812, 3.411, 4.010, 520, 1.119, 1.718, 2.317, 2.916, 3.515, 25, 624, 1.223, 1.822, 2.421, 3.020, 3.619, 129, 728, 1.327, 1.926, 2.525, 3.124, 3.723, 233, 832, 1.431, 2.030, 2.629, 3.228, 3.827, 337, 936, 1.535].

Ejemplo de ataque de Shamir y Zippel (2)

- Suponemos que el número más pequeño de CM es candidato a $S_1' = 25$.
- El factor de multiplicación sería $\omega = (S_1/S_1') = S_1 * inv(S_1', \mu) \bmod \mu$.
- Como $inv(S_1', \mu) = inv(25, 4{,}089) = 2.617$, el factor de multiplicación $\omega = 3.241 * 2.617 \bmod 4.089 = 1.111$.
- Por lo tanto su valor inverso será $\omega^{-1} = inv(\omega, \mu) = inv(1.111, 4.089)$. Luego $\omega^{-1} = 622$.
- Multiplicamos ahora los valores S de la mochila difícil por ω^{-1} a ver si obtenemos una mochila supercreciente S' ($S_i' = S_i * \omega^{-1} \bmod \mu$):
  - $S_1' = 25$ (valor elegido como candidato del conjunto CM)
  - $S_2' = S_2 * \omega^{-1} \bmod \mu = 572 * 622 \bmod 4.089 = 41$ 👍
  - $S_3' = S_3 * \omega^{-1} \bmod \mu = 2.163 * 622 \bmod 4.089 = 105$ 👍
  - $S_4' = S_4 * \omega^{-1} \bmod \mu = 1.256 * 622 \bmod 4.089 = 233$ 👍
  - $S_5' = S_5 * \omega^{-1} \bmod \mu = 3.531 * 622 \bmod 4.089 = 489$ 👍
- Como la mochila S' = {25, 41, 105, 233, 489} es supercreciente, el ataque ha prosperado y hemos encontrado la clave privada. ☹

Uso de los criptosistemas de mochilas

Existen varios algoritmos propuestos como sistemas de cifra usando el problema de la mochila: el de Graham-Shamir, Chor-Rivest, etc., pero su estudio aquí no tiene sentido.

No obstante todos han sucumbido a los criptoanálisis y en la actualidad en el único entorno que se usan es en la protección de diversos programas de aplicación, en forma de hardware que se conecta en la salida paralela del computador para descifrar el código ejecutable de esa aplicación dejando, sin embargo, activa la salida a impresora. De esta manera sólo en aquel sistema con la mochila instalada se puede ejecutar el programa. No se usa en comunicaciones.

http://www.derf.net/knapsack/

Fin del capítulo

Cuestiones y ejercicios (1 de 2)

1. Recorra de izquierda a derecha y de derecha a izquierda la mochila S = {13, 6, 1, 3, 4, 9, 10} para T = 24. ¿Tiene solución rápida?
2. Para la mochila de la pregunta anterior, ¿hay una o más soluciones?
3. ¿Interesa usar en criptografía el problema de la mochila con una solución no única? ¿Por qué sí o no?
4. ¿Qué significa que una mochila sea supercreciente? ¿Es la mochila S = {3, 4, 9, 18, 32, 73} supercreciente? ¿Por qué?
5. A partir de la mochila S' = {3, 5, 10, 21, 43} obtenga la mochila M-H difícil S. Para ω y μ use los valores mínimos posibles.
6. Si la mochila fácil es S' = {1, 2, 4, 8, 16, 32, 64, 128} con $\mu = 257$ y $\omega = 21$, cifre con una mochila de M-H el mensaje en ASCII de 10 caracteres M = Hola amigo (recuerde que el espacio se cifra).
7. Descifre el criptograma obtenido en la pregunta anterior.

Cuestiones y ejercicios (2 de 2)

8. ¿Qué valores mínimos de diseño propusieron Merkle y Hellman para su sistema de cifrado con mochila? ¿Por qué?
9. Diseñe una mochila de MH con parámetros proporcionales si m = 5.
10. No es un buen criterio elegir m = 4, m = 8 o m = 16. ¿Por qué?
11. ¿En qué consiste el ataque de Shamir y Zippel a la mochila de M-H?
12. En el ejemplo de los apuntes, ¿cuántas operaciones ha tenido que hacer nuestro algoritmo para romper la clave privada?
13. ¿Es posible que una mochila difícil provenga de más de una mochila fácil? ¿Por qué?
14. ¿Qué sucederá en el caso anterior para mochilas equivalentes con los valores del factor de multiplicación w?
15. ¿Usaría un sistema de mochila para cifrar información en un entorno como Internet? ¿Y en una intranet para respuestas a un examen?

Use el portapapeles Prácticas del tema 13 (1/2)

Software mochilas: http://www.criptored.upm.es/software/sw_m001b.htm

1. Cifre el mensaje M = ABCabc, usando una mochila de cuatro elementos de creación manual y valores S' = {3, 5, 11, 23}, M = 47 y W = 23. Observe la repetición de valores y justifique lo que sucede.
2. Vuelva a cifrar ese mensaje pero con una mochila de cinco elementos de creación manual y valores S' = {3, 5, 11, 23, 44}, M = 89 y W = 21. ¿Qué sucede ahora con el criptograma? Descifre el criptograma.
3. Ataque la mochila difícil, primero por criptoanálisis rápido y luego por criptoanálisis exhaustivo. En ambos casos vea y analice los detalles.
4. Para el mensaje M = Una prueba, cree una mochila manual S' = {28, 62, 126, 254, 510}, con M = 4051 y W = 4004. Ataque ahora la mochila por criptoanálisis rápido y luego exhaustivo y finalmente analice los detalles.
5. Cree varias mochilas automáticas con parámetros proporcionales a MH de tamaños 6, 7 y 8. Active la opción garantizar criptoanálisis y atáquelas.

Use el portapapeles Prácticas del tema 13 (2/2)

6. Repita el ejercicio anterior y opción garantizar criptoanálisis desactivada.
7. Para el mensaje M = Otra prueba, cree la mochila manual S' = {122, 250, 506, 1018, 2042, 4090, 8186}, con μ = 59369 y ω = 59361. Realice un ataque rápido y luego exhaustivo. Observe lo que sucede y explique lo observado. Repita el ataque para la mochila fácil S' = {1016, 1964, 4088, 8108, 16376, 32684, 65528, 130988, 262136, 524204}, con μ = 4186947 y ω = 1393196. Comente lo observado.
8. Repita el ejemplo anterior pero S' = {59, 123, 251, 507, 1019, 2043, 4091, 8187, 16379}, μ = 1044529 y ω = 1044193. Ataque ahora la mochila con S' = {115, 371, 883, 1907, 3955, 8051, 16243, 32627, 65395, 130931}, siendo μ = 4193897 y ω = 2562721. ¿Qué ha sucedido en estos casos?
9. Cree una mochila automática de MH de tamaño 10 y la opción garantizar criptoanálisis activada. Proceda a atacarla y si pasados 45 segundos no logra romperla, detenga el ataque y observe los detalles.
10. Cree una mochila MH de tamaño 100 y observe las mochilas completas