CÓDIGOS Y CRIPTOGRAFÍA

Cifrado simétrico con mochilas y asimétrico con mochila trampa.

Mochilas simples o supercrecientes

- Dada $(a_1, a_2, ..., a_n)$ una mochila supercreciente y $m \in \mathbb{N}$. ¿Cómo encontrar x_i para que $m = \sum_{i=1}^{n} x_i a_i$?

Mochilas simples o supercrecientes

- Dada $(a_1, a_2, ..., a_n)$ una mochila supercreciente y $m \in \mathbb{N}$. ¿Cómo encontrar x_i para que $m = \sum_{i=1}^{n} x_i a_i$?

  Algoritmo:

* $j = n$

Mochilas simples o supercrecientes

- Dada $(a_1, a_2, ..., a_n)$ una mochila supercreciente y $m \in \mathbb{N}$. ¿Cómo encontrar x_i para que $m = \sum_{i=1}^{n} x_i a_i$?

  Algoritmo:

* $j = n$
* $x_j = \begin{cases} 1 & \text{si} \quad m \geq a_j \\ 0 & \text{si} \quad m < a_j \end{cases}$

Mochilas simples o supercrecientes

- Dada $(a_1, a_2, ..., a_n)$ una mochila supercreciente y $m \in \mathbb{N}$. ¿Cómo encontrar x_i para que $m = \sum_{i=1}^{n} x_i a_i$?

  Algoritmo:

* $j = n$
* $x_j = \begin{cases} 1 & \text{si} \quad m \geq a_j \\ 0 & \text{si} \quad m < a_j \end{cases}$
* $m = m - x_j a_j$

Mochilas simples o supercrecientes

- Dada $(a_1, a_2, ..., a_n)$ una mochila supercreciente y $m \in \mathbb{N}$. ¿Cómo encontrar x_i para que $m = \sum_{i=1}^{n} x_i a_i$?

  Algoritmo:

* $j = n$
* $x_j = \begin{cases} 1 & \text{si} \quad m \geq a_j \\ 0 & \text{si} \quad m < a_j \end{cases}$
* $m = m - x_j a_j$
* $j = j - 1$

Mochilas simples o supercrecientes

- Dada $(a_1, a_2, ..., a_n)$ una mochila supercreciente y $m \in \mathbb{N}$. ¿Cómo encontrar x_i para que $m = \sum_{i=1}^{n} x_i a_i$?

  Algoritmo:

* $j = n$
* $x_j = \begin{cases} 1 & \text{si} \quad m \geq a_j \\ 0 & \text{si} \quad m < a_j \end{cases}$
* $m = m - x_j a_j$
* $j = j - 1$
* ...

Mochilas simples o supercrecientes

- Dada $(a_1, a_2, ..., a_n)$ una mochila supercreciente y $m \in \mathbb{N}$. ¿Cómo encontrar x_i para que $m = \sum_{i=1}^{n} x_i a_i$?

  Algoritmo:

* $j = n$
* $x_j = \begin{cases} 1 & \text{si} \quad m \geq a_j \\ 0 & \text{si} \quad m < a_j \end{cases}$
* $m = m - x_j a_j$
* $j = j - 1$
* ...
* Si llegamos a $m = 0$ hemos acabado y encontrado la solución.

Mochilas simples o supercrecientes

- Dada $(a_1, a_2, ..., a_n)$ una mochila supercreciente y $m \in \mathbb{N}$. ¿Cómo encontrar x_i para que $m = \sum_{i=1}^{n} x_i a_i$?

  Algoritmo:

* $j = n$
* $x_j = \begin{cases} 1 & \text{si} \quad m \geq a_j \\ 0 & \text{si} \quad m < a_j \end{cases}$
* $m = m - x_j a_j$
* $j = j - 1$
* ...
* Si llegamos a $m = 0$ hemos acabado y encontrado la solución.
* En caso contrario la solución no existe.

Código ASCII (extendido)

A	65	0100 0001
B	66	0100 0010
C	67	0100 0011
D	68	0100 0100
E	69	0100 0101
F	70	0100 0110
G	71	0100 0111
H	72	0100 1000
I	73	0100 1001
J	74	0100 1010
K	75	0100 1011
L	76	0100 1100
M	77	0100 1101

N	78	0100 1110
O	79	0100 1111
P	80	0101 0000
Q	81	0101 0001
R	82	0101 0010
S	83	0101 0011
T	84	0101 0100
U	85	0101 0101
V	86	0101 0110
W	87	0101 0111
X	88	0101 1000
Y	89	0101 1001
Z	90	0101 1010

Cifrado simétrico con mochilas

Cifrado

- Clave: Mochila de longitud n.

Cifrado simétrico con mochilas

Cifrado

- Clave: Mochila de longitud n.
- Texto llano: En código ASCII en binario, utilizando 8 bits por caracter.

Cifrado simétrico con mochilas

Cifrado

- Clave: Mochila de longitud n.
- Texto llano: En código ASCII en binario, utilizando 8 bits por caracter.
- Juntamos todos los bloques de 8 bits y volvemos a dividir en bloques de longitud n.

Cifrado simétrico con mochilas

Cifrado

- Clave: Mochila de longitud n.
- Texto llano: En código ASCII en binario, utilizando 8 bits por caracter.
- Juntamos todos los bloques de 8 bits y volvemos a dividir en bloques de longitud n. Si es necesario añadimos 1s.

Cifrado simétrico con mochilas

Cifrado

- Clave: Mochila de longitud n.
- Texto llano: En código ASCII en binario, utilizando 8 bits por caracter.
- Juntamos todos los bloques de 8 bits y volvemos a dividir en bloques de longitud n. Si es necesario añadimos 1s.
- Cada bloque implica una selección de elementos de la mochila, y por tanto un objetivo (valor) que se satisface con dichos elementos.

Cifrado simétrico con mochilas

Cifrado

- Clave: Mochila de longitud n.
- Texto llano: En código ASCII en binario, utilizando 8 bits por caracter.
- Juntamos todos los bloques de 8 bits y volvemos a dividir en bloques de longitud n. Si es necesario añadimos 1s.
- Cada bloque implica una selección de elementos de la mochila, y por tanto un objetivo (valor) que se satisface con dichos elementos.
- Texto cifrado: Los distintos objetivos que se alcanzan con los bloques anteriores.

Cifrado simétrico con mochilas

Cifrado

- Clave: Mochila de longitud n.
- Texto llano: En código ASCII en binario, utilizando 8 bits por caracter.
- Juntamos todos los bloques de 8 bits y volvemos a dividir en bloques de longitud n. Si es necesario añadimos 1s.
- Cada bloque implica una selección de elementos de la mochila, y por tanto un objetivo (valor) que se satisface con dichos elementos.
- Texto cifrado: Los distintos objetivos que se alcanzan con los bloques anteriores.

⋆ Para realizar el proceso anterior la mochila no tiene porqué ser supercreciente.

Cifrado simétrico con mochilas

Descifrado

- Clave: Mochila supercreciente de longitud n.

Cifrado simétrico con mochilas

Descifrado

- Clave: Mochila supercreciente de longitud n.
- Texto cifrado: Una sucesión de objetivos alcanzables de la mochila anterior.

Cifrado simétrico con mochilas

Descifrado

- Clave: Mochila supercreciente de longitud n.
- Texto cifrado: Una sucesión de objetivos alcanzables de la mochila anterior.
- Resolvemos la mochila para cada uno de los objetivos, obteniendo sucesiones de dígitos binarios de longitud n.

Cifrado simétrico con mochilas

Descifrado

- Clave: Mochila supercreciente de longitud n.
- Texto cifrado: Una sucesión de objetivos alcanzables de la mochila anterior.
- Resolvemos la mochila para cada uno de los objetivos, obteniendo sucesiones de dígitos binarios de longitud n.
- Reestructuramos en bloques de longitud 8, eliminando caracteres extra si es que sobran.

Cifrado simétrico con mochilas

Descifrado

- Clave: Mochila supercreciente de longitud n.
- Texto cifrado: Una sucesión de objetivos alcanzables de la mochila anterior.
- Resolvemos la mochila para cada uno de los objetivos, obteniendo sucesiones de dígitos binarios de longitud n.
- Reestructuramos en bloques de longitud 8, eliminando caracteres extra si es que sobran.
- Texto llano: Lo obtenemos mediante el código ASCII.

Cifrado simétrico con mochilas

Descifrado

- Clave: Mochila supercreciente de longitud n.
- Texto cifrado: Una sucesión de objetivos alcanzables de la mochila anterior.
- Resolvemos la mochila para cada uno de los objetivos, obteniendo sucesiones de dígitos binarios de longitud n.
- Reestructuramos en bloques de longitud 8, eliminando caracteres extra si es que sobran.
- Texto llano: Lo obtenemos mediante el código ASCII.

* Si la mochila no fuera supercreciente no podríamos asegurar unicidad, y por tanto el descifrado podría no ser posible.

Cifrado simétrico con mochilas

Descifrado

- Clave: Mochila supercreciente de longitud n.
- Texto cifrado: Una sucesión de objetivos alcanzables de la mochila anterior.
- Resolvemos la mochila para cada uno de los objetivos, obteniendo sucesiones de dígitos binarios de longitud n.
- Reestructuramos en bloques de longitud 8, eliminando caracteres extra si es que sobran.
- Texto llano: Lo obtenemos mediante el código ASCII.

* Si la mochila no fuera supercreciente no podríamos asegurar unicidad, y por tanto el descifrado podría no ser posible.
* Las mochilas supercrecientes son fáciles de revertir: no son funciones matemáticas de doble sentido.

Ejemplo: cifrado

Clave: $(1, 4, 6, 13, 25)$

Texto llano: HOLA

Ejemplo: cifrado

Clave: $(1, 4, 6, 13, 25)$

Texto llano: HOLA

* Convertimos el texto llano a 8 bits mediante ASCII:

Ejemplo: cifrado

Clave: $(1, 4, 6, 13, 25)$

Texto llano: HOLA

* Convertimos el texto llano a 8 bits mediante ASCII:

$H \to 0100\,1000,\ O \to 0100\,1111,\ L \to 0100\,1100,\ A \to 0100\,0001$

Ejemplo: cifrado

Clave: $(1, 4, 6, 13, 25)$

Texto llano: HOLA

* Convertimos el texto llano a 8 bits mediante ASCII:

  $H \to 0100\,1000,\ O \to 0100\,1111,\ L \to 0100\,1100,\ A \to 0100\,0001$

* Reagrupamos en bloques de 5 dígitos, añadiendo 1s si es necesario:

Ejemplo: cifrado

Clave: $(1, 4, 6, 13, 25)$

Texto llano: HOLA

* Convertimos el texto llano a 8 bits mediante ASCII:

$H \to 0100\,1000,\ O \to 0100\,1111,\ L \to 0100\,1100,\ A \to 0100\,0001$

* Reagrupamos en bloques de 5 dígitos, añadiendo 1s si es necesario:

01001 00001 00111 10100 11000 10000 01111

Ejemplo: cifrado

Clave: $(1, 4, 6, 13, 25)$

Texto llano: HOLA

* Convertimos el texto llano a 8 bits mediante ASCII:

$H \to 0100\,1000,\ O \to 0100\,1111,\ L \to 0100\,1100,\ A \to 0100\,0001$

* Reagrupamos en bloques de 5 dígitos, añadiendo 1s si es necesario:

01001 00001 00111 10100 11000 10000 01111

* Sustituimos en la mochila

Ejemplo: cifrado

Clave: $(1, 4, 6, 13, 25)$

Texto llano: HOLA

* Convertimos el texto llano a 8 bits mediante ASCII:

$H \to 0100\,1000,\ O \to 0100\,1111,\ L \to 0100\,1100,\ A \to 0100\,0001$

* Reagrupamos en bloques de 5 dígitos, añadiendo 1s si es necesario:

01001 00001 00111 10100 11000 10000 01111

* Sustituimos en la mochila

$01001 \to 4 + 25 = 29$
$00001 \to 25$
$00111 \to 6 + 13 + 25 = 44$
$10100 \to 1 + 6 = 7$

$11000 \to 1 + 4 = 5$
$10000 \to 1$
$01111 \to 4 + 6 + 13 + 25 = 48$

Ejemplo: cifrado

Clave: $(1, 4, 6, 13, 25)$

Texto llano: HOLA

* Convertimos el texto llano a 8 bits mediante ASCII:

$H \to 0100\,1000,\ O \to 0100\,1111,\ L \to 0100\,1100,\ A \to 0100\,0001$

* Reagrupamos en bloques de 5 dígitos, añadiendo 1s si es necesario:

01001 00001 00111 10100 11000 10000 01111

* Sustituimos en la mochila

$01001 \to 4 + 25 = 29$
$00001 \to 25$
$00111 \to 6 + 13 + 25 = 44$
$10100 \to 1 + 6 = 7$

$11000 \to 1 + 4 = 5$
$10000 \to 1$
$01111 \to 4 + 6 + 13 + 25 = 48$

Texto cifrado: 29 25 44 7 5 1 48

Ejemplo: descifrado

Texto cifrado: $29\ 25\ 44\ 7\ 5\ 1\ 48$

Clave: $(1, 4, 6, 13, 25)$

Ejemplo: descifrado

Texto cifrado: $29\ 25\ 44\ 7\ 5\ 1\ 48$

Clave: $(1, 4, 6, 13, 25)$

- Comprobamos que la mochila es supercreciente.

Ejemplo: descifrado

Texto cifrado: $29\ 25\ 44\ 7\ 5\ 1\ 48$

Clave: $(1, 4, 6, 13, 25)$

- Comprobamos que la mochila es supercreciente.
- Para cada valor de la clave hallamos los elementos de la mochila que lo satisfacen:

$29 \to 25 + 4 \to 01001$
$25 \to 25 \to 00001$
$44 \to 25 + 13 + 6 \to 00111$
$7 \to 6 + 1 \to 10100$

$5 \to 4 + 1 \to 11000$
$1 \to 1 \to 10000$
$48 \to 25 + 13 + 6 + 4 \to 01111$

Ejemplo: descifrado

Texto cifrado: 29 25 44 7 5 1 48

Clave: $(1, 4, 6, 13, 25)$

- Comprobamos que la mochila es supercreciente.
- Para cada valor de la clave hallamos los elementos de la mochila que lo satisfacen:

$29 \to 25 + 4 \to 01001$
$25 \to 25 \to 00001$
$44 \to 25 + 13 + 6 \to 00111$
$7 \to 6 + 1 \to 10100$

$5 \to 4 + 1 \to 11000$
$1 \to 1 \to 10000$
$48 \to 25 + 13 + 6 + 4 \to 01111$

- Agrupamos en bloques de 8 dígitos (eliminando los que sobren en su caso):

$$0100\,1000 \quad 0100\,1111 \quad 0100\,1100 \quad 0100\,0001 \quad 111$$

Ejemplo: descifrado

Texto cifrado: $29\ 25\ 44\ 7\ 5\ 1\ 48$

Clave: $(1, 4, 6, 13, 25)$

- Comprobamos que la mochila es supercreciente.
- Para cada valor de la clave hallamos los elementos de la mochila que lo satisfacen:

$29 \to 25 + 4 \to 01001$
$25 \to 25 \to 00001$
$44 \to 25 + 13 + 6 \to 00111$
$7 \to 6 + 1 \to 10100$

$5 \to 4 + 1 \to 11000$
$1 \to 1 \to 10000$
$48 \to 25 + 13 + 6 + 4 \to 01111$

- Agrupamos en bloques de 8 dígitos (eliminando los que sobren en su caso):

$$0100\,1000 \quad 0100\,1111 \quad 0100\,1100 \quad 0100\,0001 \quad 111$$

- Convertimos en caracteres según el código ASCII:

$$0100\,1000 \to H \quad 0100\,1111 \to O \quad 0100\,1100 \to L \quad 0100\,0001 \to A$$

Ejemplo: descifrado

Texto cifrado: 29 25 44 7 5 1 48

Clave: $(1, 4, 6, 13, 25)$

- Comprobamos que la mochila es supercreciente.
- Para cada valor de la clave hallamos los elementos de la mochila que lo satisfacen:

$29 \to 25 + 4 \to 01001$
$25 \to 25 \to 00001$
$44 \to 25 + 13 + 6 \to 00111$
$7 \to 6 + 1 \to 10100$

$5 \to 4 + 1 \to 11000$
$1 \to 1 \to 10000$
$48 \to 25 + 13 + 6 + 4 \to 01111$

- Agrupamos en bloques de 8 dígitos (eliminando los que sobren en su caso):

$$0100\,1000 \quad 0100\,1111 \quad 0100\,1100 \quad 0100\,0001 \quad 111$$

- Convertimos en caracteres según el código ASCII:

$$0100\,1000 \to H \quad 0100\,1111 \to O \quad 0100\,1100 \to L \quad 0100\,0001 \to A$$

Texto llano: H O L A

Mochila Trampa de Merkle y Hellman

- En 1978 Ralph Merkle y Martin Hellman proponen un sistema de cifrado de clave pública o asimétrico denominado Mochila con Trampa.

Mochila Trampa de Merkle y Hellman

- En 1978 Ralph Merkle y Martin Hellman proponen un sistema de cifrado de clave pública o asimétrico denominado Mochila con Trampa.
- Se basa en crear una mochila *difícil* a partir de una mochila supercreciente de forma que el cifrado se haga con la primera y el descifrado con la segunda.

Mochila Trampa de Merkle y Hellman

- En 1978 Ralph Merkle y Martin Hellman proponen un sistema de cifrado de clave pública o asimétrico denominado Mochila con Trampa.
- Se basa en crear una mochila *difícil* a partir de una mochila supercreciente de forma que el cifrado se haga con la primera y el descifrado con la segunda.
- Se puede pasar de una mochila a la otra, y viceversa, usando una *trampa*.

Mochila Trampa de Merkle y Hellman

- En 1978 Ralph Merkle y Martin Hellman proponen un sistema de cifrado de clave pública o asimétrico denominado Mochila con Trampa.
- Se basa en crear una mochila *difícil* a partir de una mochila supercreciente de forma que el cifrado se haga con la primera y el descifrado con la segunda.
- Se puede pasar de una mochila a la otra, y viceversa, usando una *trampa*.
- La trampa y la mochila supercreciente serán la clave secreta o privada y la mochila *difícil* la clave pública.

Transición entre las mochilas

- Se necesita:

Transición entre las mochilas

- Se necesita: una mochila supercreciente $(a_1, a_2, ..., a_n)$

Transición entre las mochilas

- Se necesita: una mochila supercreciente $(a_1, a_2, ..., a_n)$, un número m mayor que la suma de los elementos de la mochila (para ello basta con que $m \geq 2a_n$)

Transición entre las mochilas

- Se necesita: una mochila supercreciente $(a_1, a_2, ..., a_n)$, un número m mayor que la suma de los elementos de la mochila (para ello basta con que $m \geq 2a_n$) , y un número natural w de modo que $\text{M.C.D.}(m, w) = 1$.

Transición entre las mochilas

- Se necesita: una mochila supercreciente $(a_1, a_2, ..., a_n)$, un número m mayor que la suma de los elementos de la mochila (para ello basta con que $m \geq 2a_n$) , y un número natural w de modo que $\text{M.C.D.}(m, w) = 1$.

- Se construye la nueva mochila $(b_1, b_2, ..., b_n)$ con $b_i = w\, a_i$ módulo m.

Transición entre las mochilas

- Se necesita: una mochila supercreciente $(a_1, a_2, ..., a_n)$, un número m mayor que la suma de los elementos de la mochila (para ello basta con que $m \geq 2a_n$) , y un número natural w de modo que M.C.D.$(m, w) = 1$.
- Se construye la nueva mochila $(b_1, b_2, ..., b_n)$ con $b_i = w\, a_i$ módulo m.
- Por ser M.C.D.$(m, w) = 1$, existe el inverso modular de w y se puede revertir el proceso.

Mochila Trampa

Datos secretos: una mochila supercreciente $(a_1, a_2, ..., a_n)$, y dos números m y w con $m > \sum_{i=1}^{n} a_i$ y M.C.D.$(m, w) = 1$.

Mochila Trampa

Datos secretos: una mochila supercreciente $(a_1, a_2, ..., a_n)$, y dos números m y w con $m > \sum_{i=1}^{n} a_i$ y M.C.D.$(m, w) = 1$.

Datos públicos: la nueva mochila $(b_1, b_2, ..., b_n)$ tal que $b_i = w\, a_i$ módulo m.

Mochila Trampa

Datos secretos: una mochila supercreciente $(a_1, a_2, ..., a_n)$, y dos números m y w con $m > \sum_{i=1}^{n} a_i$ y M.C.D.$(m, w) = 1$.

Datos públicos: la nueva mochila $(b_1, b_2, ..., b_n)$ tal que $b_i = w\, a_i$ módulo m.

Mochila Trampa

Datos secretos: una mochila supercreciente $(a_1, a_2, ..., a_n)$, y dos números m y w con $m > \sum_{i=1}^{n} a_i$ y M.C.D.$(m, w) = 1$.

Datos públicos: la nueva mochila $(b_1, b_2, ..., b_n)$ tal que $b_i = w\, a_i$ módulo m.

Cifrado

El cifrado se realiza con la mochila $(b_1, b_2, ..., b_n)$ del modo que se ha descrito antes.

Mochila Trampa

Datos secretos: una mochila supercreciente $(a_1, a_2, ..., a_n)$, y dos números m y w con $m > \sum_{i=1}^{n} a_i$ y M.C.D.$(m, w) = 1$.

Datos públicos: la nueva mochila $(b_1, b_2, ..., b_n)$ tal que $b_i = w\, a_i$ módulo m.

Cifrado

El cifrado se realiza con la mochila $(b_1, b_2, ..., b_n)$ del modo que se ha descrito antes.

Descifrado

- El texto cifrado es un vector de objetivos de $(b_1, b_2, ..., b_n)$.

Mochila Trampa

Datos secretos: una mochila supercreciente $(a_1, a_2, ..., a_n)$, y dos números m y w con $m > \sum_{i=1}^{n} a_i$ y M.C.D.$(m, w) = 1$.

Datos públicos: la nueva mochila $(b_1, b_2, ..., b_n)$ tal que $b_i = w\, a_i$ módulo m.

Cifrado

El cifrado se realiza con la mochila $(b_1, b_2, ..., b_n)$ del modo que se ha descrito antes.

Descifrado

- El texto cifrado es un vector de objetivos de $(b_1, b_2, ..., b_n)$.
- Se multiplican los elementos del vector por w^{-1} mod m.

Mochila Trampa

Datos secretos: una mochila supercreciente $(a_1, a_2, ..., a_n)$, y dos números m y w con $m > \sum_{i=1}^{n} a_i$ y M.C.D.$(m, w) = 1$.

Datos públicos: la nueva mochila $(b_1, b_2, ..., b_n)$ tal que $b_i = w\, a_i$ módulo m.

Cifrado

El cifrado se realiza con la mochila $(b_1, b_2, ..., b_n)$ del modo que se ha descrito antes.

Descifrado

- El texto cifrado es un vector de objetivos de $(b_1, b_2, ..., b_n)$.
- Se multiplican los elementos del vector por w^{-1} mod m.
- Obtenemos un vector de objetivos de la mochila supercreciente $(a_1, a_2, ..., a_n)$.

Mochila Trampa

Datos secretos: una mochila supercreciente $(a_1, a_2, ..., a_n)$, y dos números m y w con $m > \sum_{i=1}^{n} a_i$ y M.C.D.$(m, w) = 1$.

Datos públicos: la nueva mochila $(b_1, b_2, ..., b_n)$ tal que $b_i = w\, a_i$ módulo m.

Cifrado

El cifrado se realiza con la mochila $(b_1, b_2, ..., b_n)$ del modo que se ha descrito antes.

Descifrado

- El texto cifrado es un vector de objetivos de $(b_1, b_2, ..., b_n)$.
- Se multiplican los elementos del vector por w^{-1} mod m.
- Obtenemos un vector de objetivos de la mochila supercreciente $(a_1, a_2, ..., a_n)$.
- Se descifra con la mochila supercreciente y los objetivos nuevos.

Ejemplo: cifrado

Mochila supercreciente: $(3, 5, 11, 21)$
Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Ejemplo: cifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Ejemplo: cifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto llano: SOL

Ejemplo: cifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto llano: SOL

- Escribimos el texto llano en código ASCII:

$$S \to 0101\,0011 \quad O \to 0110\,1111 \quad L \to 0110\,1100$$

Ejemplo: cifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto llano: SOL

- Escribimos el texto llano en código ASCII:

$$S \to 0101\,0011 \quad O \to 0110\,1111 \quad L \to 0110\,1100$$

- Agrupamos en bloques de tamaño 4:

$$0101 \quad 0011 \quad 0110 \quad 1111 \quad 0110 \quad 1100$$

Ejemplo: cifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto llano: SOL

- Escribimos el texto llano en código ASCII:

$$S \to 0101\,0011 \quad O \to 0110\,1111 \quad L \to 0110\,1100$$

- Agrupamos en bloques de tamaño 4:

$$0101 \quad 0011 \quad 0110 \quad 1111 \quad 0110 \quad 1100$$

- Evaluamos cada bloque en la mochila difícil:

$0101 \to 13 + 35 = 48$
$0011 \to 9 + 35 = 44$
$0110 \to 13 + 9 = 22$
$1111 \to 47 + 13 + 9 + 35 = 104$
$0110 \to 13 + 9 = 22$
$1100 \to 47 + 13 = 60$

Ejemplo: cifrado

Mochila supercreciente: $(3, 5, 11, 21)$
Módulo: $m = 49$, elemento multiplicativo: $w = 32$
Mochila difícil: $(47, 13, 9, 35)$
Texto llano: SOL

- Escribimos el texto llano en código ASCII:

$$S \to 0101\,0011 \quad O \to 0110\,1111 \quad L \to 0110\,1100$$

- Agrupamos en bloques de tamaño 4:

$$0101 \quad 0011 \quad 0110 \quad 1111 \quad 0110 \quad 1100$$

- Evaluamos cada bloque en la mochila difícil:

$0101 \to 13 + 35 = 48$
$0011 \to 9 + 35 = 44$
$0110 \to 13 + 9 = 22$
$1111 \to 47 + 13 + 9 + 35 = 104$
$0110 \to 13 + 9 = 22$
$1100 \to 47 + 13 = 60$

Texto cifrado: 48 44 22 104 22 60

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto cifrado: 48 44 22 104 22 60

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto cifrado: 48 44 22 104 22 60

- Calculamos el inverso de $w = 32$ módulo $m = 49$

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto cifrado: 48 44 22 104 22 60

- Calculamos el inverso de $w = 32$ módulo $m = 49$: $w^{-1} = 23$.

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto cifrado: 48 44 22 104 22 60

- Calculamos el inverso de $w = 32$ módulo $m = 49$: $w^{-1} = 23$.
- Multiplicamos el texto cifrado por $w^{-1} = 23$ módulo $m = 49$:

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto cifrado: 48 44 22 104 22 60

- Calculamos el inverso de $w = 32$ módulo $m = 49$: $w^{-1} = 23$.
- Multiplicamos el texto cifrado por $w^{-1} = 23$ módulo $m = 49$:

  26 32 16 40 16 8.

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto cifrado: 48 44 22 104 22 60

- Calculamos el inverso de $w = 32$ módulo $m = 49$: $w^{-1} = 23$.
- Multiplicamos el texto cifrado por $w^{-1} = 23$ módulo $m = 49$:

  26 32 16 40 16 8.

- Resolvemos para cada uno de estos valores el problema de la mochila supercreciente:

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto cifrado: 48 44 22 104 22 60

- Calculamos el inverso de $w = 32$ módulo $m = 49$: $w^{-1} = 23$.
- Multiplicamos el texto cifrado por $w^{-1} = 23$ módulo $m = 49$:

  26 32 16 40 16 8.

- Resolvemos para cada uno de estos valores el problema de la mochila supercreciente:

$26 \to 21 + 5 \to 0101$

$32 \to 21 + 11 \to 0011$

$16 \to 11 + 5 \to 0110$

$40 \to 21 + 11 + 5 + 3 \to 1111$

$16 \to 11 + 5 \to 0110$

$8 \to 3 + 5 \to 1100$

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto cifrado: 48 44 22 104 22 60

- Calculamos el inverso de $w = 32$ módulo $m = 49$: $w^{-1} = 23$.
- Multiplicamos el texto cifrado por $w^{-1} = 23$ módulo $m = 49$:

  26 32 16 40 16 8.

- Resolvemos para cada uno de estos valores el problema de la mochila supercreciente:

$26 \to 21 + 5 \to 0101$

$32 \to 21 + 11 \to 0011$

$16 \to 11 + 5 \to 0110$

$40 \to 21 + 11 + 5 + 3 \to 1111$

$16 \to 11 + 5 \to 0110$

$8 \to 3 + 5 \to 1100$

- Agrupamos en bloques de 8 bits y aplicamos el código ASCII:

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto cifrado: $48\ 44\ 22\ 104\ 22\ 60$

- Calculamos el inverso de $w = 32$ módulo $m = 49$: $w^{-1} = 23$.
- Multiplicamos el texto cifrado por $w^{-1} = 23$ módulo $m = 49$:

$$26\ 32\ 16\ 40\ 16\ 8.$$

- Resolvemos para cada uno de estos valores el problema de la mochila supercreciente:

$26 \to 21 + 5 \to 0101$
$32 \to 21 + 11 \to 0011$
$16 \to 11 + 5 \to 0110$
$40 \to 21 + 11 + 5 + 3 \to 1111$
$16 \to 11 + 5 \to 0110$
$8 \to 3 + 5 \to 1100$

- Agrupamos en bloques de 8 bits y aplicamos el código ASCII:

$$0101\,0011 \to S \quad 0110\,1111 \to O \quad 0110\,1100 \to L$$

Ejemplo: descifrado

Mochila supercreciente: $(3, 5, 11, 21)$

Módulo: $m = 49$, elemento multiplicativo: $w = 32$

Mochila difícil: $(47, 13, 9, 35)$

Texto cifrado: $48\ 44\ 22\ 104\ 22\ 60$

- Calculamos el inverso de $w = 32$ módulo $m = 49$: $w^{-1} = 23$.
- Multiplicamos el texto cifrado por $w^{-1} = 23$ módulo $m = 49$:

$$26\ 32\ 16\ 40\ 16\ 8.$$

- Resolvemos para cada uno de estos valores el problema de la mochila supercreciente:

$26 \to 21 + 5 \to 0101$
$32 \to 21 + 11 \to 0011$
$16 \to 11 + 5 \to 0110$
$40 \to 21 + 11 + 5 + 3 \to 1111$
$16 \to 11 + 5 \to 0110$
$8 \to 3 + 5 \to 1100$

- Agrupamos en bloques de 8 bits y aplicamos el código ASCII:

$$0101\,0011 \to S \quad 0110\,1111 \to O \quad 0110\,1100 \to L$$

Texto llano: SOL

Valores de diseño de mochilas Merkle-Hellman

- Merkle y Hellman propusieron los siguientes parámetros en la elección de la mochila:

Valores de diseño de mochilas Merkle-Hellman

- Merkle y Hellman propusieron los siguientes parámetros en la elección de la mochila:

* Tamaño de la mochila: $n \geq 100$.

Valores de diseño de mochilas Merkle-Hellman

- Merkle y Hellman propusieron los siguientes parámetros en la elección de la mochila:

* Tamaño de la mochila: $n \geq 100$.

* Módulo: $m \in [2^{2n+1} + 1, 2^{2n+2} - 1]$. ($m$ tiene $(2n + 2)$ bits).

Valores de diseño de mochilas Merkle-Hellman

- Merkle y Hellman propusieron los siguientes parámetros en la elección de la mochila:

* Tamaño de la mochila: $n \geq 100$.
* Módulo: $m \in [2^{2n+1} + 1, 2^{2n+2} - 1]$. ($m$ tiene $(2n + 2)$ bits).
* Mochila supercreciente: $a_i \in [(2^{i-1} - 1)2^n + 1, 2^{i-1}2^n]$.

Valores de diseño de mochilas Merkle-Hellman

- Merkle y Hellman propusieron los siguientes parámetros en la elección de la mochila:

* Tamaño de la mochila: $n \geq 100$.
* Módulo: $m \in [2^{2n+1} + 1, 2^{2n+2} - 1]$. ($m$ tiene $(2n + 2)$ bits).
* Mochila supercreciente: $a_i \in [(2^{i-1} - 1)2^n + 1, 2^{i-1}2^n]$.
* Elegimos $x \in [2, m - 2]$ y tomamos $w = \dfrac{x}{\text{M.C.D.}(m, x)}$.

Debilidades de la Mochila Trampa

- En 1982 Adi Shamir y Richard Zippel encontraron debilidades en el método de la Mochila Trampa siempre y cuando:

Debilidades de la Mochila Trampa

- En 1982 Adi Shamir y Richard Zippel encontraron debilidades en el método de la Mochila Trampa siempre y cuando:

  1. Se conozca el módulo m (o se pueda deducir).

Debilidades de la Mochila Trampa

- En 1982 Adi Shamir y Richard Zippel encontraron debilidades en el método de la Mochila Trampa siempre y cuando:

  1. Se conozca el módulo m (o se pueda deducir).

  2. Los dos primeros elementos b_1 y b_2 de la mochila difícil se correspondan con los primeros de la mochila supercreciente a_1 y a_2 y sean primos con m.

Debilidades de la Mochila Trampa

- En 1982 Adi Shamir y Richard Zippel encontraron debilidades en el método de la Mochila Trampa siempre y cuando:

  1. Se conozca el módulo m (o se pueda deducir).

  2. Los dos primeros elementos b_1 y b_2 de la mochila difícil se correspondan con los primeros de la mochila supercreciente a_1 y a_2 y sean primos con m.

- En este caso podremos encontrar w^{-1} y por tanto generar la mochila supercreciente a partir de la difícil.

Criptoanálisis de Shamir y Zimmel

- Es necesario que:

1. Se conozca el módulo m.
2. b_1 y b_2 se correspondan con a_1 y a_2 (y sean primos con m).

Criptoanálisis de Shamir y Zimmel

- Es necesario que:

1. Se conozca el módulo m.
2. b_1 y b_2 se correspondan con a_1 y a_2 (y sean primos con m).
3. Los dos primeros elementos deben ser mucho más pequeños que el módulo. Por ejemplo de 100 y 101 bits, teniendo m 202 bits.

Criptoanálisis de Shamir y Zimmel

- Es necesario que:

1. Se conozca el módulo m.
2. b_1 y b_2 se correspondan con a_1 y a_2 (y sean primos con m).
3. Los dos primeros elementos deben ser mucho más pequeños que el módulo. Por ejemplo de 100 y 101 bits, teniendo m 202 bits.
   * Esto se cumple, por ejemplo, con los valores de diseño.

Criptoanálisis de Shamir y Zimmel

- Es necesario que:

1. Se conozca el módulo m.
2. b_1 y b_2 se correspondan con a_1 y a_2 (y sean primos con m).
3. Los dos primeros elementos deben ser mucho más pequeños que el módulo. Por ejemplo de 100 y 101 bits, teniendo m 202 bits.
   - Esto se cumple, por ejemplo, con los valores de diseño.

- El objetivo es hallar w para poder generar la mochila supercreciente.

Criptoanálisis de Shamir y Zimmel

- Es necesario que:

1. Se conozca el módulo m.
2. b_1 y b_2 se correspondan con a_1 y a_2 (y sean primos con m).
3. Los dos primeros elementos deben ser mucho más pequeños que el módulo. Por ejemplo de 100 y 101 bits, teniendo m 202 bits.
   - Esto se cumple, por ejemplo, con los valores de diseño.

- El objetivo es hallar w para poder generar la mochila supercreciente.

Criptoanálisis

- Calculamos $q = b_1 * b_2^{-1} \bmod m$.

Criptoanálisis de Shamir y Zimmel

- Es necesario que:

1. Se conozca el módulo m.
2. b_1 y b_2 se correspondan con a_1 y a_2 (y sean primos con m).
3. Los dos primeros elementos deben ser mucho más pequeños que el módulo. Por ejemplo de 100 y 101 bits, teniendo m 202 bits.
   - Esto se cumple, por ejemplo, con los valores de diseño.

- El objetivo es hallar w para poder generar la mochila supercreciente.

Criptoanálisis

- Calculamos $q = b_1 * b_2^{-1} \mod m$. Para esto es importante que M.C.D.$(b_2, m) = 1$.

Criptoanálisis de Shamir y Zimmel

- Es necesario que:

1. Se conozca el módulo m.
2. b_1 y b_2 se correspondan con a_1 y a_2 (y sean primos con m).
3. Los dos primeros elementos deben ser mucho más pequeños que el módulo. Por ejemplo de 100 y 101 bits, teniendo m 202 bits.
   - Esto se cumple, por ejemplo, con los valores de diseño.

- El objetivo es hallar w para poder generar la mochila supercreciente.

Criptoanálisis

- Calculamos $q = b_1 * b_2^{-1} \bmod m$. Para esto es importante que $\text{M.C.D.}(b_2, m) = 1$.
- Como $b_i = w\, a_i$, si $\text{M.C.D.}(a_2, m) = 1$ se tiene $b_1 * b_2^{-1} = a_1 * a_2^{-1}$. Luego $a_1 = q\, a_2 \bmod m$ es un múltiplo de q.

Criptoanálisis de Shamir y Zimmel

- Es necesario que:

1. Se conozca el módulo m.
2. b_1 y b_2 se correspondan con a_1 y a_2 (y sean primos con m).
3. Los dos primeros elementos deben ser mucho más pequeños que el módulo. Por ejemplo de 100 y 101 bits, teniendo m 202 bits.
   - Esto se cumple, por ejemplo, con los valores de diseño.

- El objetivo es hallar w para poder generar la mochila supercreciente.

Criptoanálisis

- Calculamos $q = b_1 * b_2^{-1} \bmod m$. Para esto es importante que M.C.D.$(b_2, m) = 1$.
- Como $b_i = w\, a_i$, si M.C.D.$(a_2, m) = 1$ se tiene $b_1 * b_2^{-1} = a_1 * a_2^{-1}$. Luego $a_1 = q\, a_2 \bmod m$ es un múltiplo de q.
- Calculamos los primeros 2^{n+1} múltiplos modulares de q, (con n el número de elementos de la mochila).

Criptoanálisis de Shamir y Zimmel

Criptoanálisis

* El candidato para a_1 será el valor más pequeño de la lista anterior.

Criptoanálisis de Shamir y Zimmel

Criptoanálisis

- El candidato para a_1 será el valor más pequeño de la lista anterior.
- Calculamos $w = b_1 * a_1^{-1} \mod m$.

Criptoanálisis de Shamir y Zimmel

Criptoanálisis

- El candidato para a_1 será el valor más pequeño de la lista anterior.
- Calculamos $w = b_1 * a_1^{-1} \mod m$. Para ello es necesario que M.C.D.$(a_1, m) = 1$.

Criptoanálisis de Shamir y Zimmel

Criptoanálisis

- El candidato para a_1 será el valor más pequeño de la lista anterior.
- Calculamos $w = b_1 * a_1^{-1} \mod m$. Para ello es necesario que M.C.D.$(a_1, m) = 1$.
- Calculamos w^{-1} como el inverso de w mod m y calculamos los elementos $a_i = w^{-1} b_i \mod m$.

Criptoanálisis de Shamir y Zimmel

Criptoanálisis

- El candidato para a_1 será el valor más pequeño de la lista anterior.
- Calculamos $w = b_1 * a_1^{-1} \mod m$. Para ello es necesario que M.C.D.$(a_1, m) = 1$.
- Calculamos w^{-1} como el inverso de w mod m y calculamos los elementos $a_i = w^{-1} b_i \mod m$.
- Si el resultado es una mochila supercreciente hemos acabado.

Criptoanálisis de Shamir y Zimmel

Criptoanálisis

- El candidato para a_1 será el valor más pequeño de la lista anterior.
- Calculamos $w = b_1 * a_1^{-1} \mod m$. Para ello es necesario que M.C.D.$(a_1, m) = 1$.
- Calculamos w^{-1} como el inverso de w mod m y calculamos los elementos $a_i = w^{-1} b_i \mod m$.
- Si el resultado es una mochila supercreciente hemos acabado.
- Si no, probamos con el siguiente valor más pequeño.

Criptoanálisis de Shamir y Zimmel

Criptoanálisis

- El candidato para a_1 será el valor más pequeño de la lista anterior.
- Calculamos $w = b_1 * a_1^{-1} \mod m$. Para ello es necesario que M.C.D.$(a_1, m) = 1$.
- Calculamos w^{-1} como el inverso de w mod m y calculamos los elementos $a_i = w^{-1}\, b_i \mod m$.
- Si el resultado es una mochila supercreciente hemos acabado.
- Si no, probamos con el siguiente valor más pequeño.
- Si recorremos toda la lista y no obtenemos ninguna mochila supercreciente volvemos a calcular los siguientes 2^{n+1} múltiplos de q módulo m, y así sucesivamente...

Criptoanálisis de Shamir y Zimmel

Criptoanálisis

- El candidato para a_1 será el valor más pequeño de la lista anterior.
- Calculamos $w = b_1 * a_1^{-1} \mod m$. Para ello es necesario que M.C.D.$(a_1, m) = 1$.
- Calculamos w^{-1} como el inverso de w mod m y calculamos los elementos $a_i = w^{-1}\, b_i \mod m$.
- Si el resultado es una mochila supercreciente hemos acabado.
- Si no, probamos con el siguiente valor más pequeño.
- Si recorremos toda la lista y no obtenemos ninguna mochila supercreciente volvemos a calcular los siguientes 2^{n+1} múltiplos de q módulo m, y así sucesivamente...

- Normalmente el ataque prospera con pocos pasos.

Ejemplo

Clave pública (mochila difícil):

$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$

Módulo: $m = 4089$

Ejemplo

Clave pública (mochila difícil):
$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$
Módulo: $m = 4089$

- Hallamos el inverso de b_2 mod m y $q = b_1 b_2^{-1}$ mod m:

Ejemplo

Clave pública (mochila difícil):

$$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$$

Módulo: $m = 4089$

- Hallamos el inverso de b_2 mod m y $q = b_1 b_2^{-1}$ mod m:

$$b_2^{-1} = 2309, \qquad q = 599.$$

Ejemplo

Clave pública (mochila difícil):

$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$

Módulo: $m = 4089$

- Hallamos el inverso de b_2 mod m y $q = b_1 b_2^{-1}$ mod m:

$$b_2^{-1} = 2309, \qquad q = 599.$$

- Como $n = 5$, hallamos $\{q, 2q, ..., 2^{5+1}q\}$ mod m:

Ejemplo

Clave pública (mochila difícil):

$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$

Módulo: $m = 4089$

- Hallamos el inverso de b_2 mod m y $q = b_1 b_2^{-1}$ mod m:

$$b_2^{-1} = 2309, \qquad q = 599.$$

- Como $n = 5$, hallamos $\{q, 2q, ..., 2^{5+1}q\}$ mod m:

$\{599, 1198, 1797, 2396, 2995, 3594, 104, 703, 1302, 1901, 2500, 3099,$
$3698, 208, 807, 1406, 2005, 2604, 3203, 3802, 312, 911, 1510, 2109,$
$2708, 3307, 3906, 416, 1015, 1614, 2213, 2812, 3411, 4010, 520, 1119,$
$1718, 2317, 2916, 3515, 25, 624, 1223, 1822, 2421, 3020, 3619, 129,$
$728, 1327, 1926, 2525, 3124, 3723, 233, 832, 1431, 2030, 2629, 3228,$
$3827, 337, 936, 1535\}$

Ejemplo

Clave pública (mochila difícil):
$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$
Módulo: $m = 4089$

- Hallamos el inverso de b_2 mod m y $q = b_1 b_2^{-1}$ mod m:
$$b_2^{-1} = 2309, \qquad q = 599.$$

- Como $n = 5$, hallamos $\{q, 2q, ..., 2^{5+1}q\}$ mod m:
$\{599, 1198, 1797, 2396, 2995, 3594, 104, 703, 1302, 1901, 2500, 3099,$
$3698, 208, 807, 1406, 2005, 2604, 3203, 3802, 312, 911, 1510, 2109,$
$2708, 3307, 3906, 416, 1015, 1614, 2213, 2812, 3411, 4010, 520, 1119,$
$1718, 2317, 2916, 3515, 25, 624, 1223, 1822, 2421, 3020, 3619, 129,$
$728, 1327, 1926, 2525, 3124, 3723, 233, 832, 1431, 2030, 2629, 3228,$
$3827, 337, 936, 1535\}$

Ejemplo

Clave pública (mochila difícil):
$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$
Módulo: $m = 4089$

- Tomamos como candidato $a_1 = 25$.

Ejemplo

Clave pública (mochila difícil):
$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$
Módulo: $m = 4089$

- Tomamos como candidato $a_1 = 25$.
- El factor de multiplicación sería $w = b_1 a_1^{-1} \bmod m$:

Ejemplo

Clave pública (mochila difícil):

$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$

Módulo: $m = 4089$

- Tomamos como candidato $a_1 = 25$.
- El factor de multiplicación sería $w = b_1 a_1^{-1} \bmod m$:

$$a_1^{-1} = 2617, \qquad w = 3241 \cdot 2617 \bmod 4089 = 1111.$$

Ejemplo

Clave pública (mochila difícil):
$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$
Módulo: $m = 4089$

- Tomamos como candidato $a_1 = 25$.
- El factor de multiplicación sería $w = b_1 a_1^{-1} \bmod m$:

$$a_1^{-1} = 2617, \qquad w = 3241 \cdot 2617 \bmod 4089 = 1111.$$

- Por tanto, $w^{-1} = 622 \bmod 4089$.

Ejemplo

Clave pública (mochila difícil):

$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$

Módulo: $m = 4089$

- Tomamos como candidato $a_1 = 25$.
- El factor de multiplicación sería $w = b_1 a_1^{-1} \bmod m$:

$$a_1^{-1} = 2617, \qquad w = 3241 \cdot 2617 \bmod 4089 = 1111.$$

- Por tanto, $w^{-1} = 622 \bmod 4089$.
- Hallamos el resto de valores a ver si obtenemos una mochila supercreciente, $a_i = w^{-1} b_i \bmod m$:

$$\begin{aligned} a_2 &= 622 \cdot 572 \bmod 4089 = 41 \\ a_3 &= 622 \cdot 2163 \bmod 4089 = 105 \\ a_4 &= 622 \cdot 1256 \bmod 4089 = 233 \\ a_5 &= 622 \cdot 3531 \bmod 4089 = 489 \end{aligned}$$

Ejemplo

Clave pública (mochila difícil):
$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$
Módulo: $m = 4089$

- Tomamos como candidato $a_1 = 25$.
- El factor de multiplicación sería $w = b_1 a_1^{-1} \bmod m$:

$$a_1^{-1} = 2617, \qquad w = 3241 \cdot 2617 \bmod 4089 = 1111.$$

- Por tanto, $w^{-1} = 622 \bmod 4089$.
- Hallamos el resto de valores a ver si obtenemos una mochila supercreciente, $a_i = w^{-1} b_i \bmod m$:

$$\begin{aligned} a_2 &= 622 \cdot 572 \bmod 4089 = 41 \\ a_3 &= 622 \cdot 2163 \bmod 4089 = 105 \\ a_4 &= 622 \cdot 1256 \bmod 4089 = 233 \\ a_5 &= 622 \cdot 3531 \bmod 4089 = 489 \end{aligned}$$

- Comprobamos que es supercreciente (se puede hacer paso a paso).

Ejemplo

Clave pública (mochila difícil):
$(b_1, b_2, b_3, b_4, b_5) = (3241, 572, 2163, 1256, 3531)$
Módulo: $m = 4089$

- Tomamos como candidato $a_1 = 25$.
- El factor de multiplicación sería $w = b_1 a_1^{-1} \bmod m$:

$$a_1^{-1} = 2617, \qquad w = 3241 \cdot 2617 \bmod 4089 = 1111.$$

- Por tanto, $w^{-1} = 622 \bmod 4089$.
- Hallamos el resto de valores a ver si obtenemos una mochila supercreciente, $a_i = w^{-1} b_i \bmod m$:

$$\begin{aligned} a_2 &= 622 \cdot 572 \bmod 4089 = 41 \\ a_3 &= 622 \cdot 2163 \bmod 4089 = 105 \\ a_4 &= 622 \cdot 1256 \bmod 4089 = 233 \\ a_5 &= 622 \cdot 3531 \bmod 4089 = 489 \end{aligned}$$

- Comprobamos que es supercreciente (se puede hacer paso a paso).

Clave privada (mochila supercreciente):
$(a_1, a_2, a_3, a_4, a_5) = (25, 41, 105, 233, 489)$