Criptosistemas basados en el problema de la mochila

Trabajo Fin de Grado del
Doble Grado en Ingeniería Informática y Matemáticas

Juan Manuel Mateos Pérez

Universidad de Granada

Curso 2023-2024

Objetivos

- Compresión del problema de la mochila.
- Análisis de los criptosistemas de Merkle-Hellman y Chor-Rivest.
- Estudio de los ataques de Shamir, Lagarias-Odlyzko y Coster et al.

Tabla de contenidos

1. Criptografía básica
   - Introducción a la criptografía
   - Criptografía simétrica vs asimétrica
2. Problema de la mochila
3. Criptosistema de Merkle-Hellman
   - Método básico
   - Método iterativo
4. Ataques a este criptosistema
   - Shamir
   - Lagarias-Odlyzko
   - Coster et al
5. Criptosistema de Chor-Rivest
6. Conclusiones

Tabla de contenidos

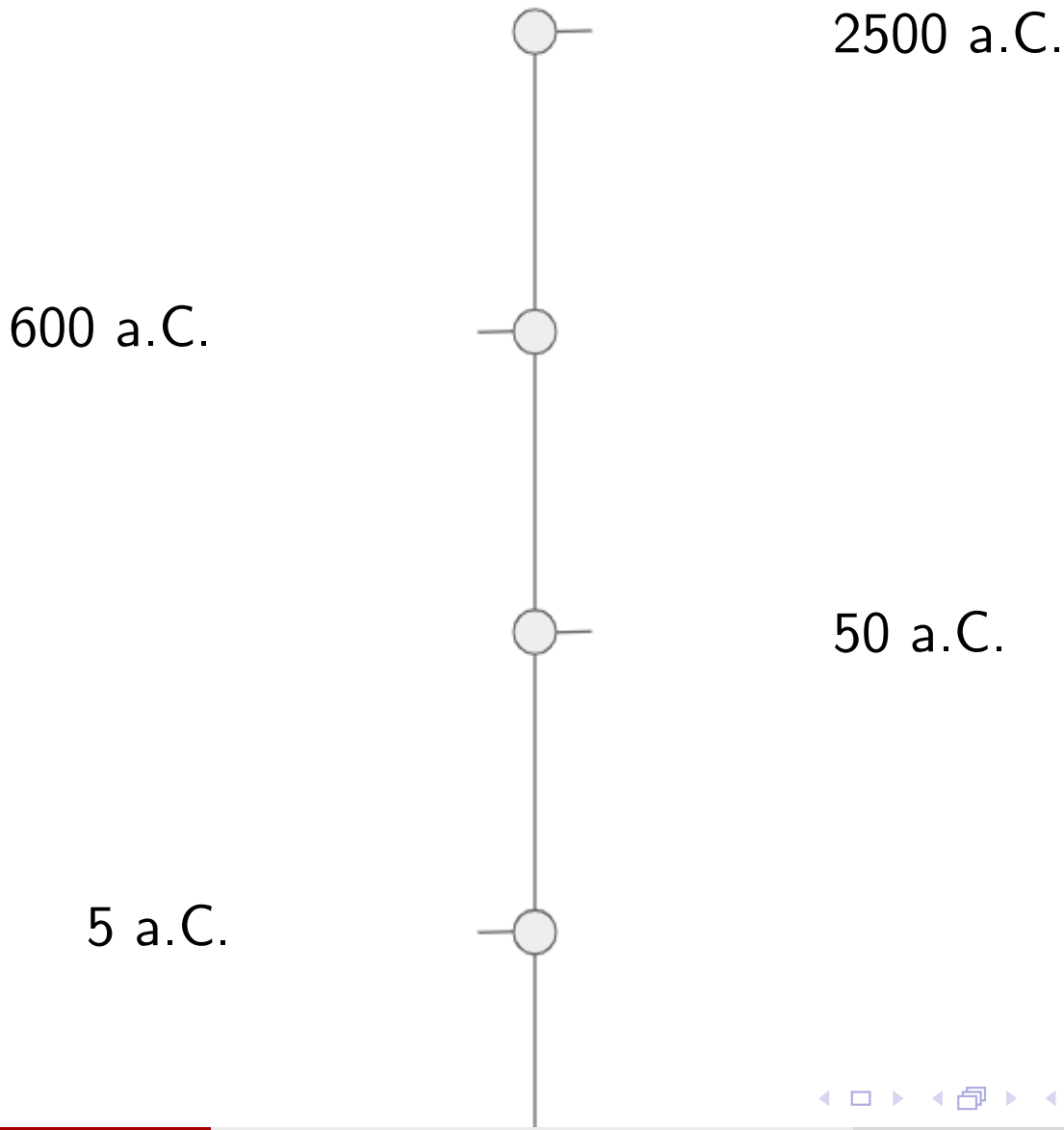
1. Criptografía básica
   - Introducción a la criptografía
   - Criptografía simétrica vs asimétrica
2. Problema de la mochila
3. Criptosistema de Merkle-Hellman
   - Método básico
   - Método iterativo
4. Ataques a este criptosistema
   - Shamir
   - Lagarias-Odlyzko
   - Coster et al
5. Criptosistema de Chor-Rivest
6. Conclusiones

Criptografía

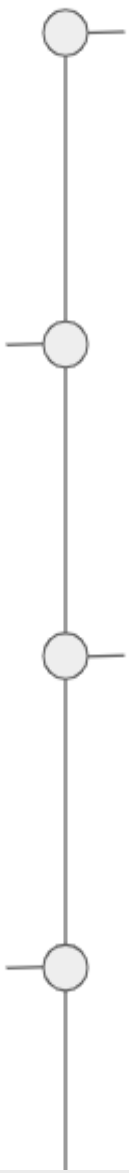
Definición

La criptografía (del griego kryptós, «secreto», y graphé, «grafo», literalmente «escritura secreta») es una disciplina que se ocupa de la seguridad de la información en la comunicación a través de canales inseguros.

Historia de la criptografía



Historia de la criptografía



Egipcios, 2500 a.C.

600 a.C.

50 a.C.

5 a.C.

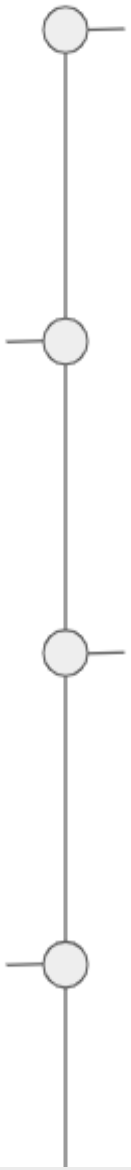
Historia de la criptografía

Egipcios, 2500 a.C.

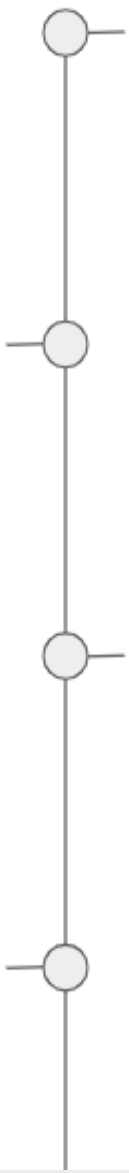
Hebreos, 600 a.C.

50 a.C.

5 a.C.



Historia de la criptografía



Egipcios, 2500 a.C.

Hebreos, 600 a.C.

Romanos, 50 a.C.

5 a.C.

Historia de la criptografía

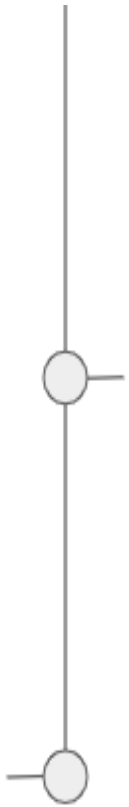
Egipcios, 2500 a.C.

Hebreos, 600 a.C.

Romanos, 50 a.C.

Griegos, 5 a.C.

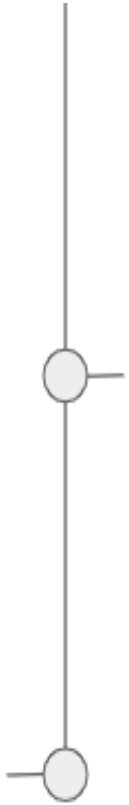
Desarrollo de la criptografía



1939 d.C.

1976 d.C.

Desarrollo de la criptografía

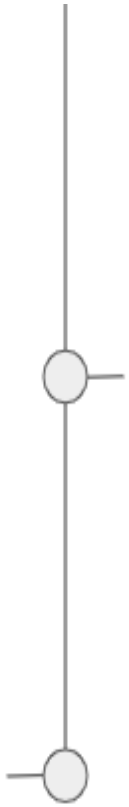


Segunda Guerra Mundial,
1939 d.C.

- Enigma
- Maquinas de Turing

1976 d.C.

Desarrollo de la criptografía



Segunda Guerra Mundial,
1939 d.C.

Diffie-Hellman,
1976 d.C.

- Criptografía simétrica
- Criptografía asimétrica

Criptografía simétrica vs asimétrica

Criptografía simétrica

- Clave única (necesidad de compartirla)
- Más velocidad
- No se necesita comprobar autenticación

vs

Criptografía asimétrica

- Dos claves por usuario (existencia de clave pública)
- Menos velocidad
- Se necesita comprobar autenticación

Criptografía simétrica vs asimétrica

Criptografía simétrica vs Criptografía asimétrica

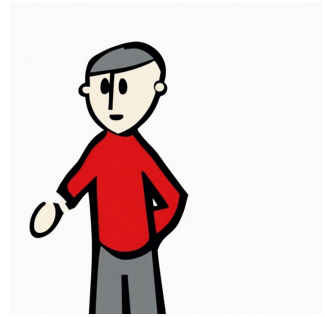
- **Clave única (necesidad de compartirla)**
- **Más velocidad**
- **No se necesita comprobar autenticación**

- Dos claves por usuario (existencia de clave pública)
- Menos velocidad
- Se necesita comprobar autenticación

Cifrado simétrico

Alice

mensaje



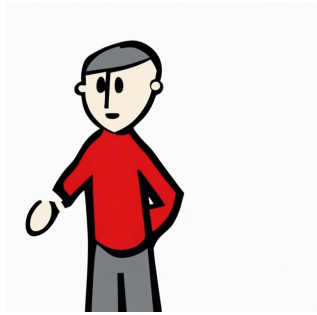
Bob

Cifrado simétrico

Eva

Alice

mensaje

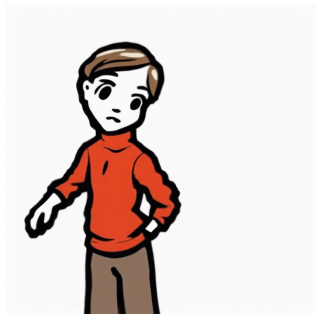


Bob

Cifrado simétrico

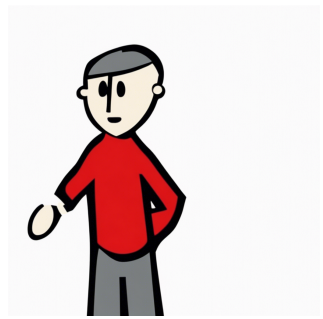
$enc_k(mensaje) = x$

Alice



Eva

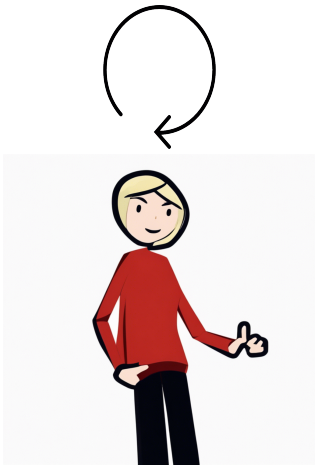
x



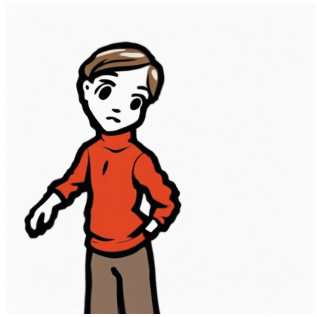
Bob

Cifrado simétrico

$enc_k(mensaje) = x$



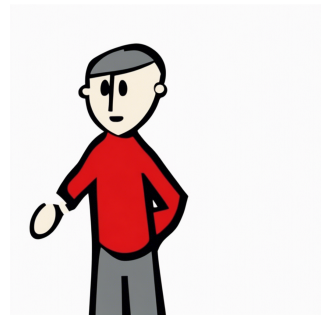
Alice



Eva

x

$dec_k(x) = mensaje$



Bob

Criptografía simétrica vs asimétrica

Criptografía simétrica

- Clave única (necesidad de compartirla)
- Más velocidad
- No se necesita comprobar autenticación

vs

Criptografía asimétrica

- Dos claves por usuario (existencia de clave pública)
- Menos velocidad
- Se necesita comprobar autenticación

Criptografía simétrica vs asimétrica

Criptografía simétrica

- Clave única (necesidad de compartirla)
- Más velocidad
- No se necesita comprobar autenticación

vs

Criptografía asimétrica

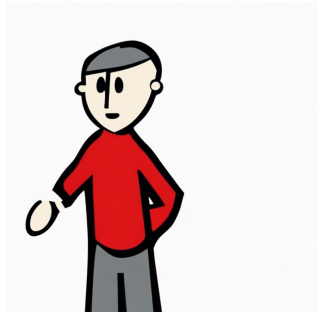
- **Dos claves por usuario (existencia de clave pública)**
- **Menos velocidad**
- **Se necesita comprobar autenticación**

Cifrado asimétrico

Eva

Alice

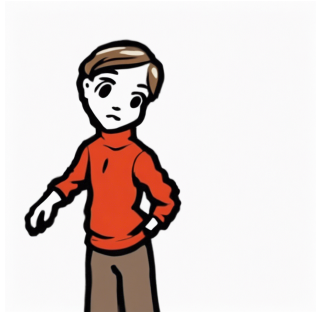
mensaje



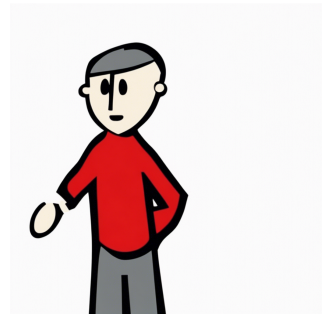
Bob

Cifrado asimétrico

Alice



Eva



Bob

mensaje

skA

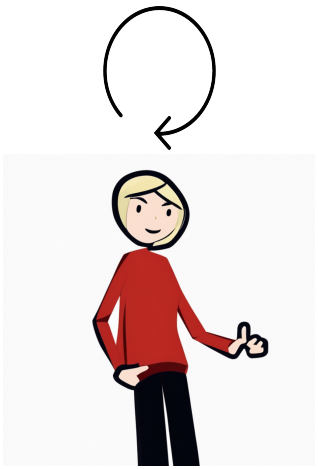
pkA

pkB

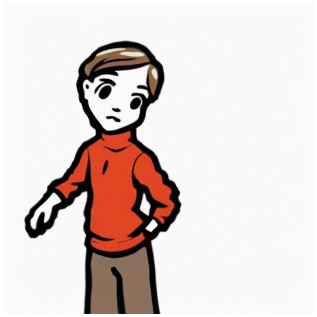
skB

Cifrado asimétrico

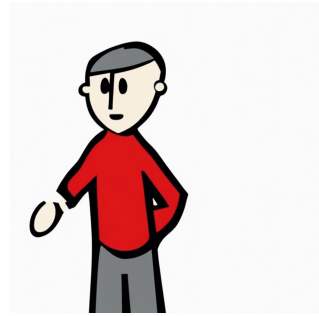
$enc_{pkB}(mensaje) = x$



Alice



Eva



Bob

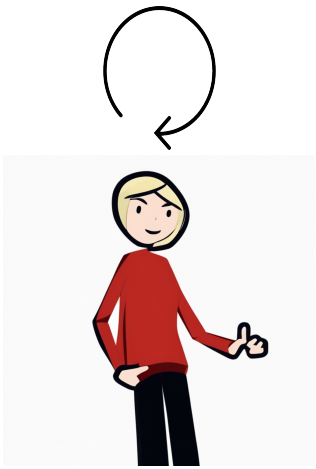
skA pkA

x

pkB skB

Cifrado asimétrico

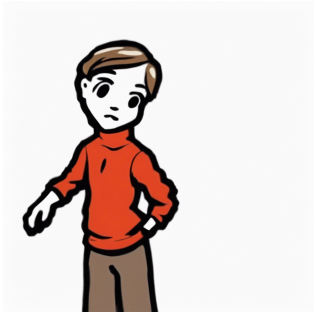
$enc_{pkB}(mensaje) = x$



Alice

skA

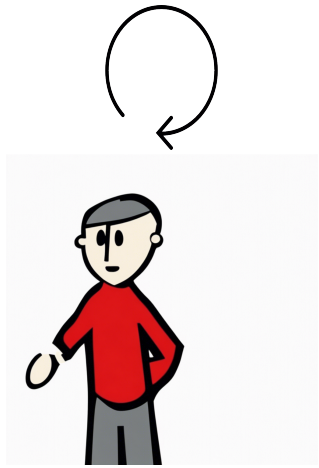
pkA



Eva

x

$dec_{skB}(x) = mensaje$



Bob

pkB

skB

Clasificación de los criptosistemas asimétricos

Algunas metodologías son:

1. Basados en el problema de la mochila
2. Basados en retículos
3. Basados en códigos
4. Basados en curvas elípticas
5. Basados en funciones hash
6. Basados en ecuaciones cuadráticas multivariantes

Clasificación de los criptosistemas asimétricos

Algunas metodologías son:

1. Basados en el problema de la mochila
2. Basados en retículos
3. Basados en códigos
4. Basados en curvas elípticas
5. Basados en funciones hash
6. Basados en ecuaciones cuadráticas multivariantes

Aunque, actualmente:

1. Criptosistemas resistentes a ataques cuánticos
2. Criptosistemas no resistentes a estos ataques

Tabla de contenidos

1. Criptografía básica
   - Introducción a la criptografía
   - Criptografía simétrica vs asimétrica
2. Problema de la mochila
3. Criptosistema de Merkle-Hellman
   - Método básico
   - Método iterativo
4. Ataques a este criptosistema
   - Shamir
   - Lagarias-Odlyzko
   - Coster et al
5. Criptosistema de Chor-Rivest
6. Conclusiones

Siete problemas del milenio

1. La conjetura de Hodge
2. La conjetura de Poincaré
3. La hipótesis de Riemann
4. Las ecuaciones de Navier-Stokes
5. Existencia de Yang-Mills y del salto de masa
6. La conjetura de Birch y Swinnerton-Dyer
7. El problema P vs NP

Siete problemas del milenio

1. La conjetura de Hodge
2. La conjetura de Poincaré
3. La hipótesis de Riemann
4. Las ecuaciones de Navier-Stokes
5. Existencia de Yang-Mills y del salto de masa
6. La conjetura de Birch y Swinnerton-Dyer
7. **El problema P vs NP**

Conjuntos P y NP

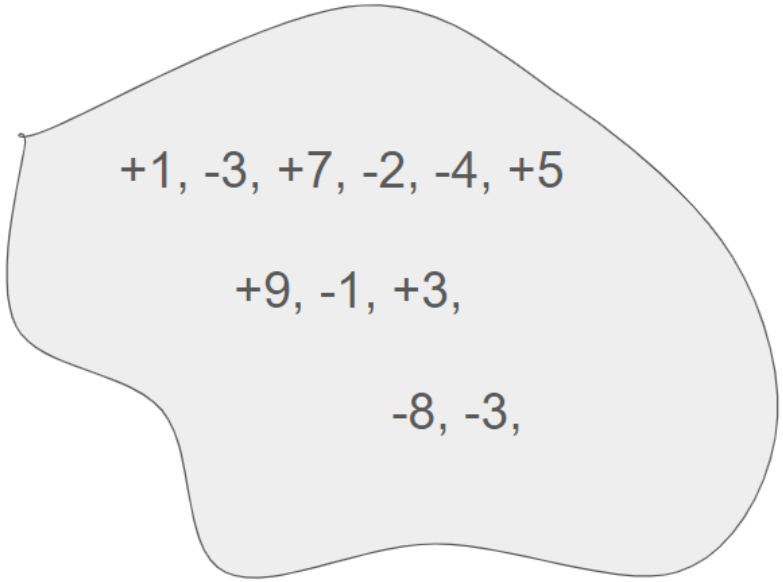
Conjunto NP

Denominamos *NP* al conjunto de problemas en los que podemos comprobar si una respuesta dada es correcta o no, en tiempo polinomial.

Conjunto P

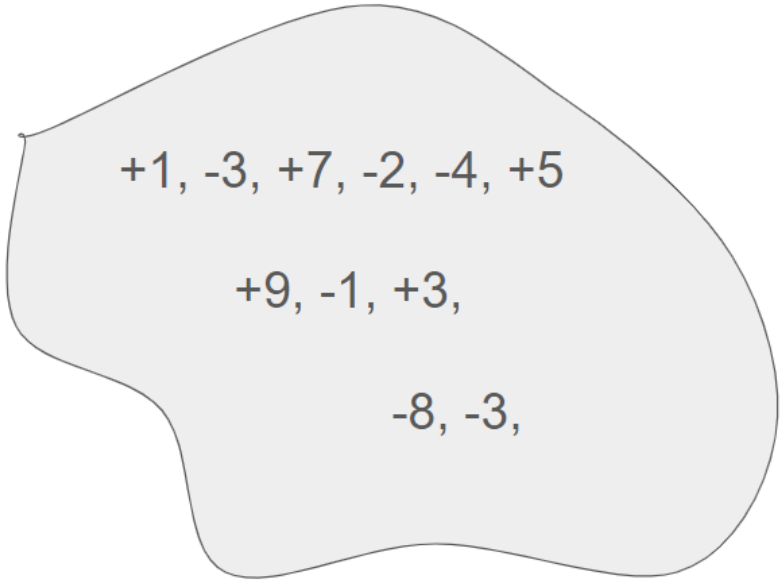
Denominamos *P* al conjunto de problemas en los que podemos encontrar una respuesta al problema, en tiempo polinomial.

P vs NP



Tomar varios de estos números tal que su suma sea 0

P vs NP

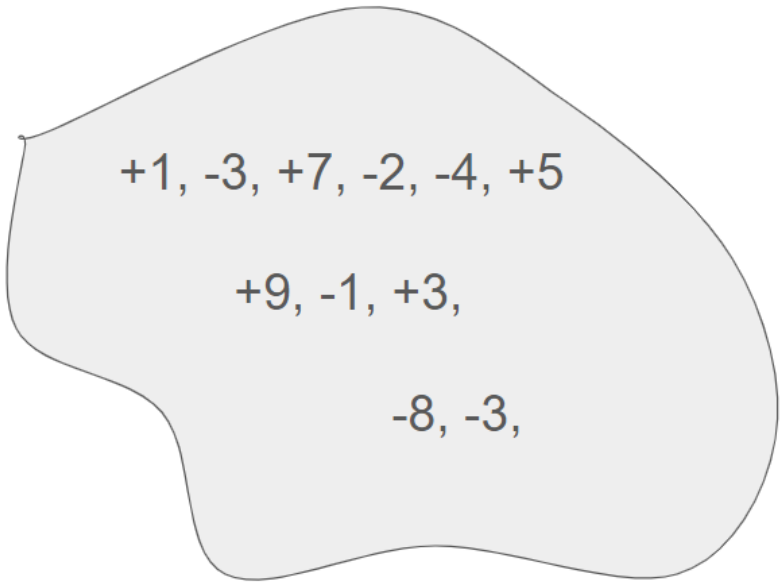


$$\{-3, +7, -4\}$$

$$\Downarrow$$

$$-3 + 7 - 4 = 0$$

P vs NP



$$\{-3, +7, -4\}$$

$$\Downarrow$$

$$-3 + 7 - 4 = 0$$

Es claro que $P \subset NP$, pero ¿$NP \subset P$?

Problema P vs NP

¿P = NP?

Problemas NP-Completos (I)

Reducción

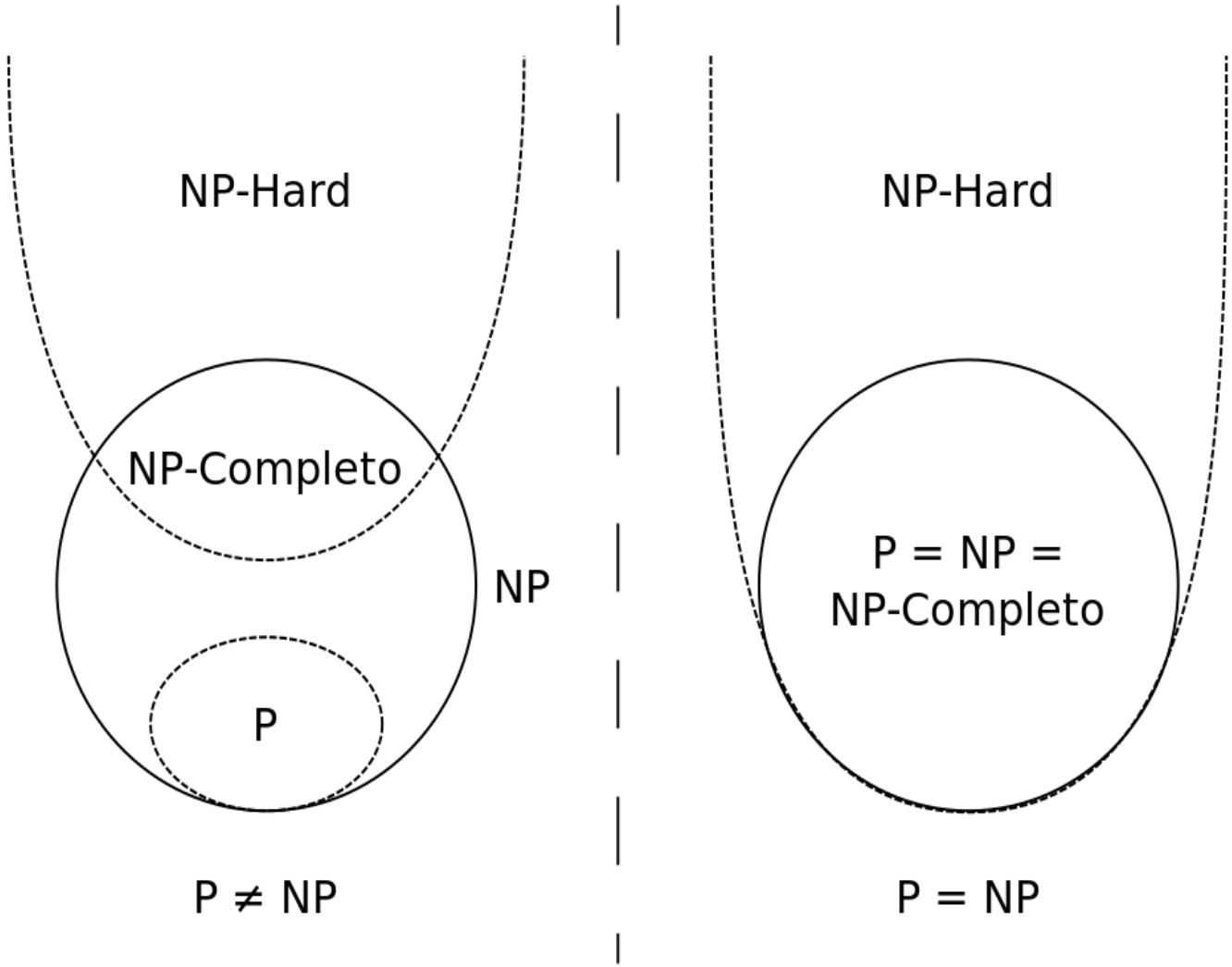
Llamamos *reducción* a una transformación en tiempo polinomial, de un problema de decisión en otro equivalente. Esto es, sea A el conjunto de instancias del primer problema, y B el conjunto de instancias del segundo, definimos una reducción r como $r : A \to B$ tal que:

$$a \in A \text{ es sí} \iff r(a) \in B \text{ es sí}$$

Problema NP-Completo

Diremos que un problema es *NP-completo* si es un problema de decisión perteneciente a *NP*, que además verifica que existe una reducción de cada problema de *NP* a él.

Problemas NP-Completos (II)



Problema de la mochila (I)

Tamaño = 7
Peso = 2

Tamaño = 6
Peso = 4

Problema de la mochila (I)

Tamaño = 7
Peso = 2

Tamaño = 6
Peso = 4

Problema de la mochila (II)

Definición

Sean $a = \{a_1, ..., a_n\} \subseteq \mathbb{N}^*$ un *conjunto de pesos* y $S \in \mathbb{N}^*$ la *capacidad total*, el *problema de la mochila* busca encontrar el *vector de soluciones* $x = \{x_1, ..., x_n\} \subseteq \mathbb{N}^*$ que maximice el valor de la mochila y verifique:

$$\sum_{i=1}^{n} a_i \cdot x_i \leq S$$

En particular, nosotros nos centraremos en:

$$\sum_{i=1}^{n} a_i \cdot x_i = S$$

Tabla de contenidos

1. Criptografía básica
   - Introducción a la criptografía
   - Criptografía simétrica vs asimétrica
2. Problema de la mochila
3. Criptosistema de Merkle-Hellman
   - Método básico
   - Método iterativo
4. Ataques a este criptosistema
   - Shamir
   - Lagarias-Odlyzko
   - Coster et al
5. Criptosistema de Chor-Rivest
6. Conclusiones

Sucesión supercreciente

Definición

Diremos que una sucesión $\{a_i\}_{i=1}^n$ es *supercreciente* si verifica que:

$$a_i > \sum_{j=1}^{i-1} a_j \text{ , para } i = 2, ..., n$$

Por ejemplo, $\{a_n\} = 1, 3, 8, 16, ...$ es supercreciente ya que:

$$a_2 = 3 > a_1 = 1$$

$$a_3 = 8 > \sum_{i=1}^{2} a_i = 3 + 1 = 4$$

$$a_4 = 16 > \sum_{i=1}^{3} a_i = 4 + 8 = 12$$

Idea del método básico

$$S' = a' \cdot mensaje$$

$$\Downarrow$$

$$S = a \cdot mensaje$$

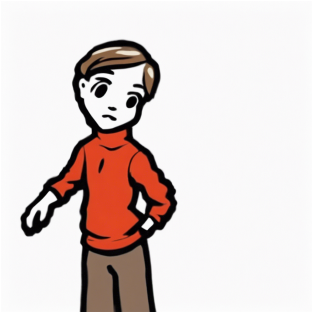
Idea del método básico

$$S' = a' \cdot mensaje$$

$$\Uparrow$$

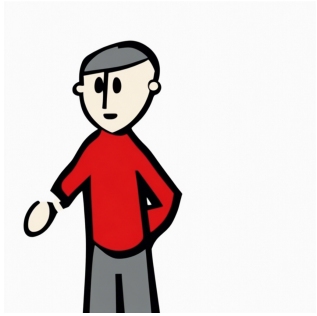
$$S = a \cdot mensaje$$

Método básico



Eva

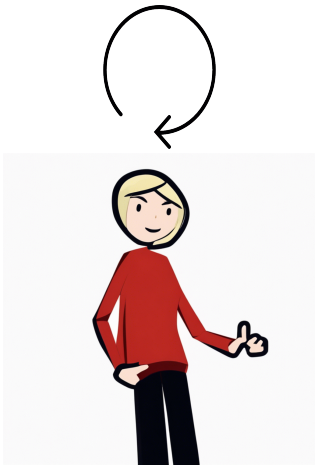
Alice



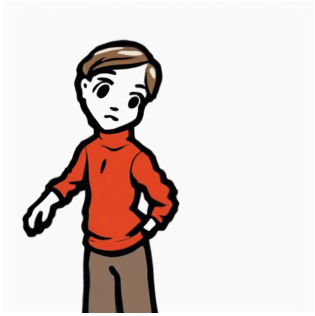
Bob

Método básico

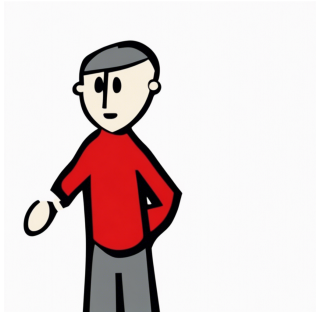
Generación claves



Alice



Eva



Bob

Generación de claves

- Generación de clave privada

- Generación de clave pública

Generación de claves

- **Generación de clave privada**
  - Valores coprimos m y w, esto es, $mcd(m, w) = 1$
  - Sucesión supercreciente a'

$$sk = (m, w, a')$$

- Generación de clave pública

Generación de claves

- Generación de clave privada
  - Valores coprimos m y w, esto es, $mcd(m, w) = 1$
  - Sucesión supercreciente a'

$$sk = (m, w, a')$$

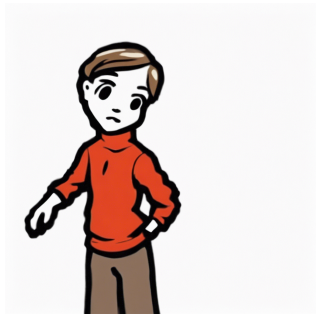
- **Generación de clave pública**

$$a_i \equiv w \cdot a'_i \pmod{m}, \text{ con } i = 1, ..., n$$

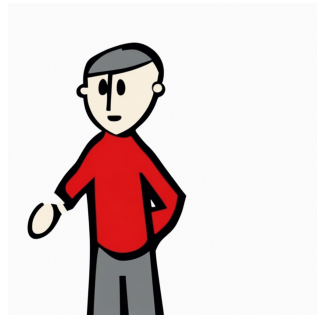
$$pk = a$$

Método básico

Alice



Eva



Bob

sk

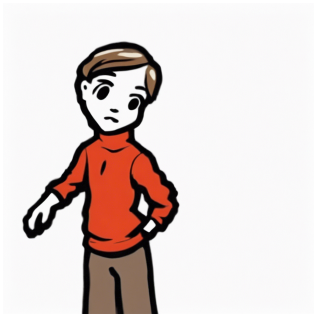
pk

Método básico

Alice

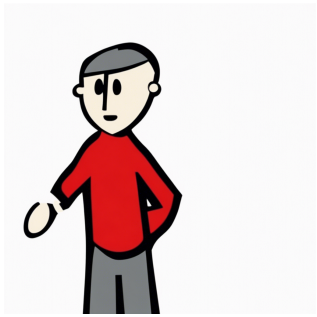
sk

pk



Eva

Cifrado



Bob

Cifrado

Se necesita:

- Clave pública $pk = (a_1, ..., a_n)$
- Mensaje $m = (m_1, ..., m_n)$

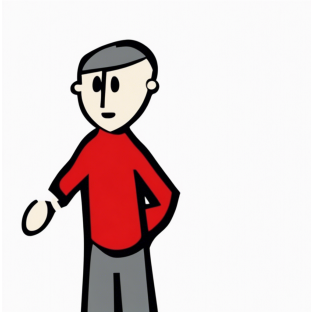
Cálculo del mensaje cifrado:

$$S = pk \cdot m = \sum_{i=1}^{n} a_i \cdot m_i$$

Método básico

Eva

Alice

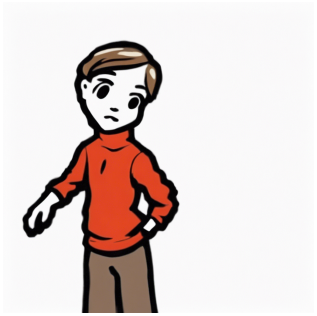


Bob

sk	pk

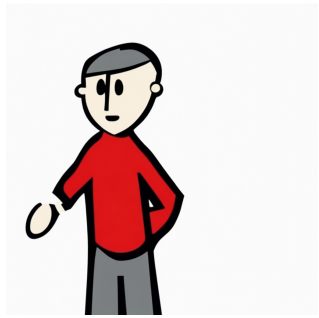
Método básico

Alice



Eva

S



Bob

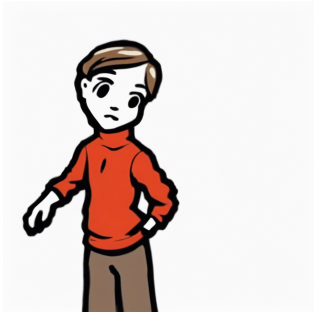
sk

pk

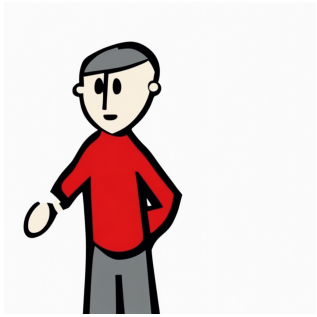
Método básico

Descifrado

Alice



Eva



Bob

sk

pk

S

Descifrado (I)

Se necesita:

- Clave privada $sk = (m, w, a')$
- Mensaje cifrado S

Cálculo del mensaje descifrado:

$$S' = w^{-1} \cdot S \pmod{m}$$

Descifrado (II)

Conseguir el mensaje $x = (x_1, ..., x_n)$ descifrado a partir de S':

$$x_n = 1 \iff S' \geq a'_n$$

$$x_i = 1 \iff S' \geq a'_i + \sum_{j=i+1}^{n} a'_j \cdot x_j$$

con $i = n - 1, ..., 1$.

Ejemplo de descifrado

Ejemplo

Para el mensaje $= (0, 0, 0, 1, 1)$, generamos:

$S' = 744$, $n = 5$, y $a' = (3, 42, 105, 249, 495)$

$$S' = 744 \geq a'_5 = 495 \Rightarrow x_5 = 1$$
$$S' = 744 \geq a'_5 + a'_4 = 744 \Rightarrow x_4 = 1$$
$$S' = 744 \ngeq a'_5 + a'_4 + a'_3 = 849 \Rightarrow x_3 = 0$$
$$\vdots$$

Finalmente, obtenemos $x = (0, 0, 0, 1, 1)$.

Idea del método iterativo

Datos generados

- Valores coprimos: m, w
- Sucesión supercreciente: a'

Datos recibidos

- Mensaje cifrado: S

Datos objetivo

- Clave pública: a
- Mensaje transformado: S'

$$S' = a' \cdot mensaje$$

$$\Downarrow$$

$$S = a \cdot mensaje$$

Idea del método iterativo

Datos generados

- Valores coprimos: m, w
- Sucesión supercreciente: a'

Datos recibidos

- Mensaje cifrado: S

Datos objetivo

- Clave pública: a
- Mensaje transformado: S'

$$S'' = a'' \cdot mensaje$$

$$\Downarrow$$

$$S' = a' \cdot mensaje$$

$$\Downarrow$$

$$S = a \cdot mensaje$$

Idea del método iterativo

Datos generados

- Valores coprimos: m, w
- Sucesión supercreciente: a'

Datos recibidos

- Mensaje cifrado: S

Datos objetivo

- Clave pública: a
- Mensaje transformado: S'

$$S''' = a''' \cdot mensaje$$

$$\Downarrow$$

$$S'' = a'' \cdot mensaje$$

$$\Downarrow$$

$$S' = a' \cdot mensaje$$

$$\Downarrow$$

$$S = a \cdot mensaje$$

Idea del método iterativo

Datos generados

- Valores coprimos: m, w
- Sucesión supercreciente: a'

Datos recibidos

- Mensaje cifrado: S

Datos objetivo

- Clave pública: a
- Mensaje transformado: S'

$$\vdots$$

$$\Downarrow$$

$$S''' = a''' \cdot mensaje$$

$$\Downarrow$$

$$S'' = a'' \cdot mensaje$$

$$\Downarrow$$

$$S' = a' \cdot mensaje$$

$$\Downarrow$$

$$S = a \cdot mensaje$$

Método iterativo

Método Iterativo

Cálculo de la clave pública:

$$a = w^{-1} \cdot a^{'} \pmod{m}$$

Cálculo del mensaje transformado:

$$S^{'} = w \cdot S \pmod{m}$$

Método Básico

Cálculo de la clave pública:

$$a = w \cdot a^{'} \pmod{m}$$

Cálculo del mensaje transformado:

$$S^{'} = w^{-1} \cdot S \pmod{m}$$

Tabla de contenidos

1. Criptografía básica
   - Introducción a la criptografía
   - Criptografía simétrica vs asimétrica
2. Problema de la mochila
3. Criptosistema de Merkle-Hellman
   - Método básico
   - Método iterativo
4. Ataques a este criptosistema
   - Shamir
   - Lagarias-Odlyzko
   - Coster et al
5. Criptosistema de Chor-Rivest
6. Conclusiones

Ataques a Merkle-Hellman

- Ataque de Shamir
- Ataques por baja densidad

Ataques a Merkle-Hellman

- **Ataque de Shamir**
- Ataques por baja densidad

Idea de Shamir

Objetivo Shamir

1. Encontrar m y w para generar a'

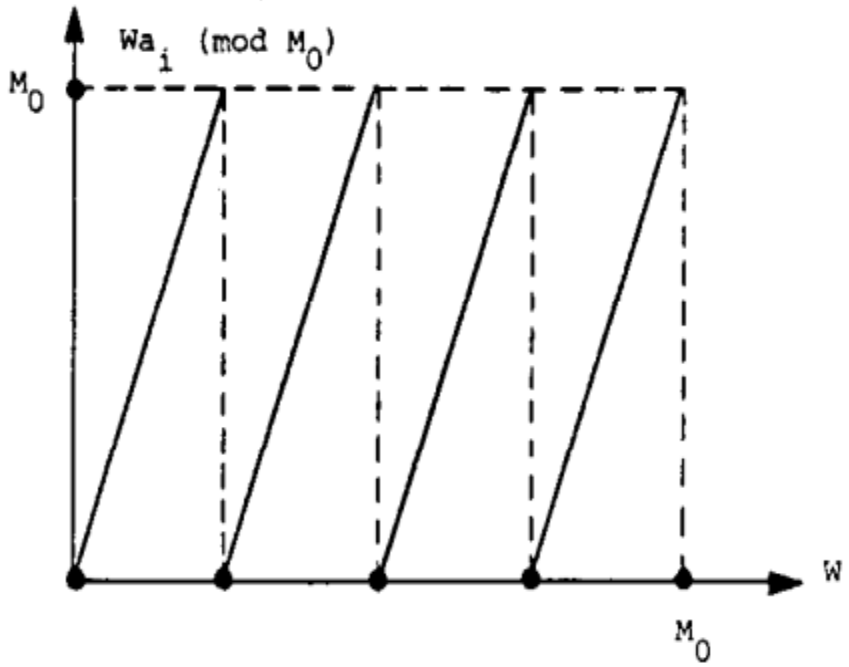
$$a'_i \equiv w \cdot a_i \bmod m$$

2. Obtener S' usando m, w y S:

$$S' = w^{-1} \cdot S \pmod{m}$$

3. Usar S' y a' para obtener el mensaje

Shamir



- Eje horizontal: W
- Eje vertical: M_0
- Pendiente: a_i

Figura: Gráfica de la función $W \cdot a_i \pmod{M_0}$

Shamir

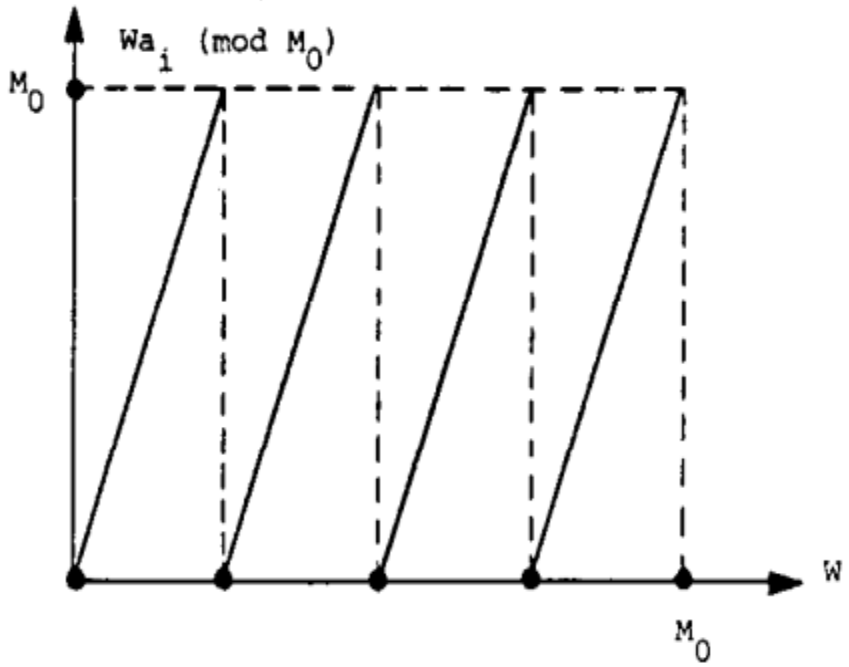


Figura: Gráfica de la función $W \cdot a_i \pmod{M_0}$

$$a_1' = W_0 \cdot a_1 \pmod{M_0}$$

$$\Downarrow$$

$$d(W_0, minimo\ a_1) \approx 2^{-n+1}$$

Shamir

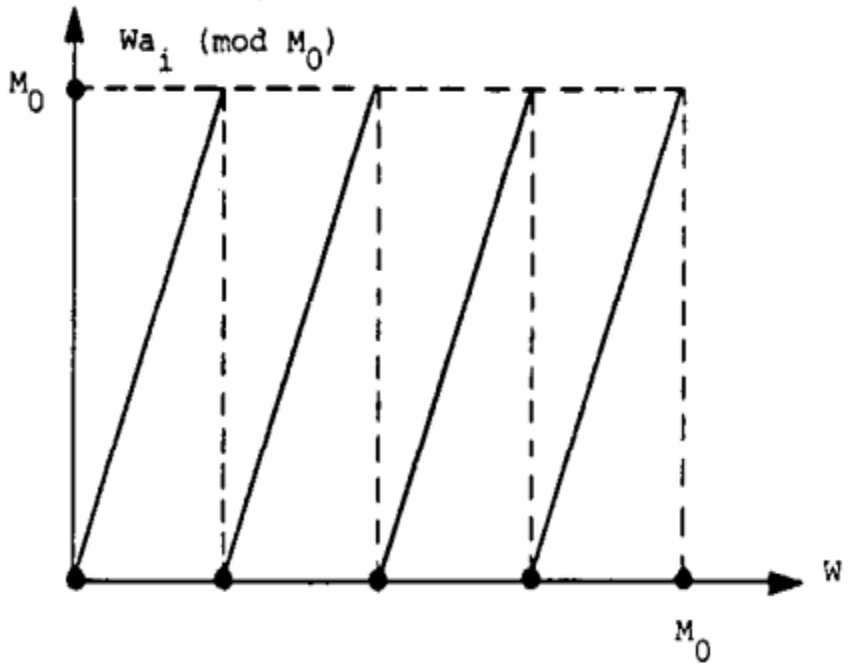


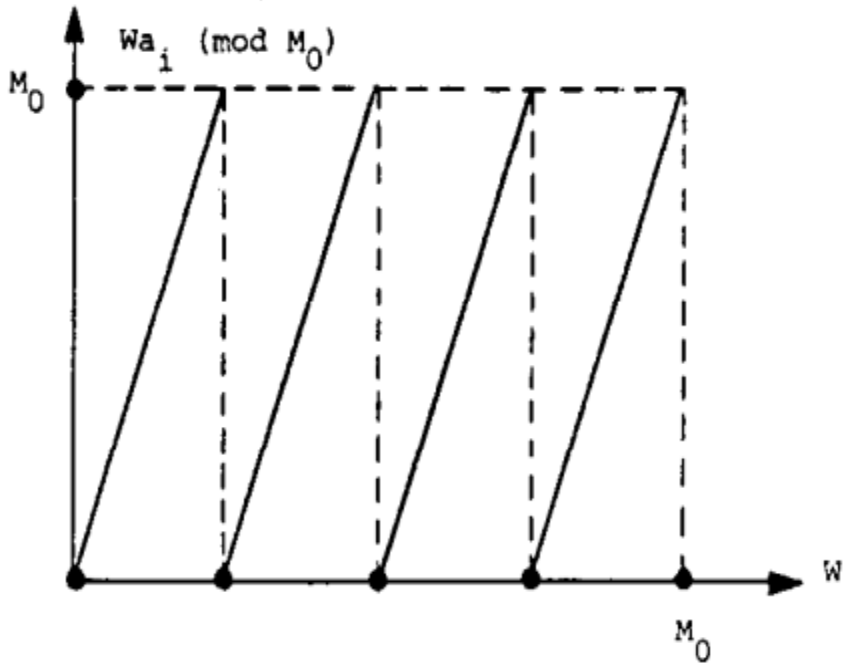
Figura: Gráfica de la función $W \cdot a_i \pmod{M_0}$

$$a_2' = W_0 \cdot a_2 \pmod{M_0}$$

$$\Downarrow$$

$$d(W_0, minimo\ a_2) \approx 2^{-n+1}$$

Shamir



...

Figura: Gráfica de la función $W \cdot a_i \pmod{M_0}$

Shamir

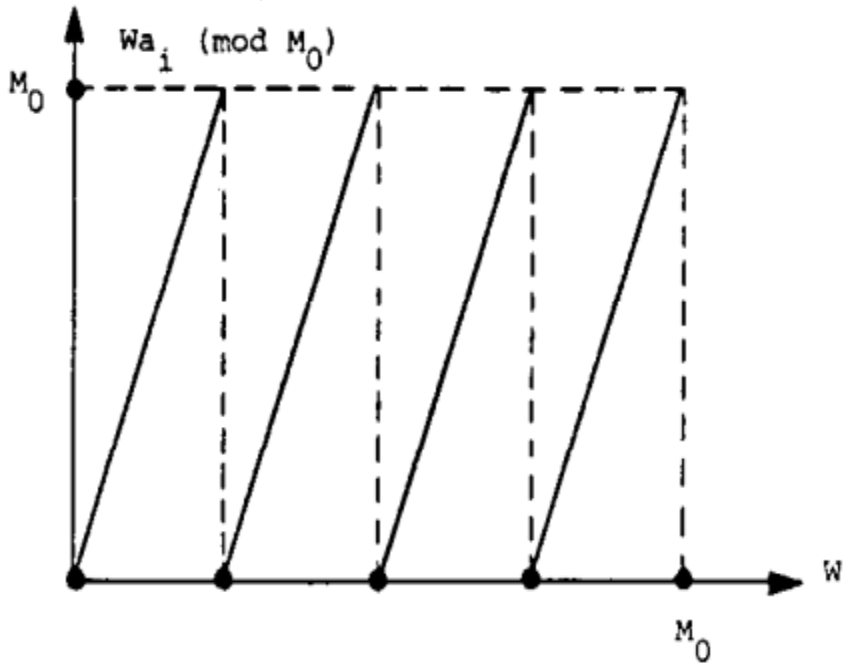


Figura: Gráfica de la función $W \cdot a_i \pmod{M_0}$

Puntos de acumulación

Shamir

Dividir por M_0

- l: nº curvas superpuestas
- k: nº puntos acumulación

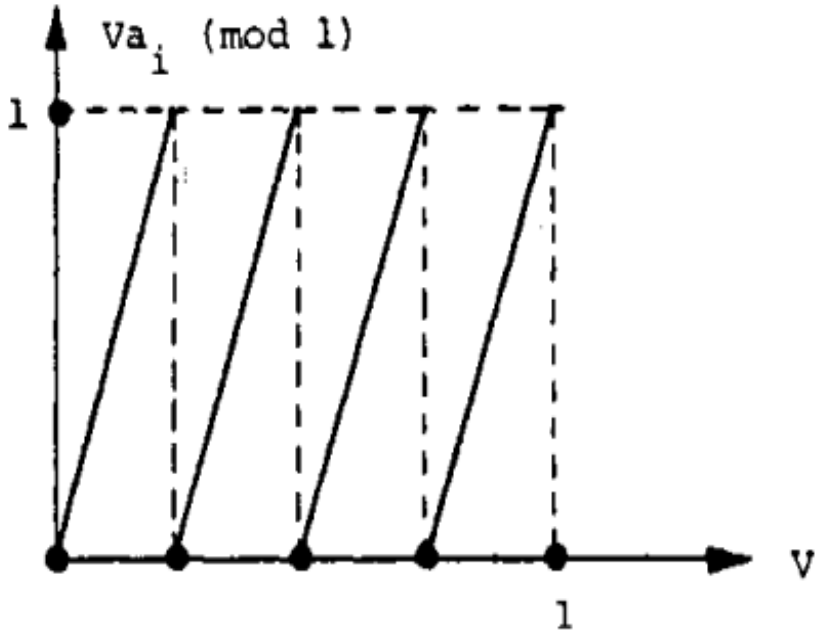


Figura: Gráfica de la función $V \cdot a_i \pmod 1$

Sean $p, q, r, \ldots,$ enteros,

$$1 \leq p \leq a_1 - 1$$

$$-\epsilon_2 \leq \frac{p}{a_1} - \frac{q}{a_2} \leq \epsilon_2' \qquad 1 \leq q \leq a_2 - 1$$

$$-\epsilon_3 \leq \frac{p}{a_1} - \frac{r}{a_3} \leq \epsilon_3' \qquad 1 \leq r \leq a_3 - 1$$

$$\Downarrow$$

$$-\delta_2 \leq pa_2 - qa_1 \leq \delta_2'$$

$$-\delta_3 \leq pa_3 - ra_1 \leq \delta_3'$$

$$\vdots$$

Algoritmo de programación entera de Lenstra

$$\Uparrow$$

$$-\delta_2 \leq pa_2 - qa_1 \leq \delta_2'$$
$$-\delta_3 \leq pa_3 - ra_1 \leq \delta_3'$$
$$\vdots$$

Algoritmo de programación entera de Lenstra

$$\Downarrow$$

Obtiene las soluciones enteras de un sistema de desigualdades, consiguiendo así M y W

Ataques a Merkle-Hellman

- Ataque de Shamir
- Ataques por baja densidad

Ataques a Merkle-Hellman

- Ataque de Shamir
- **Ataques por baja densidad**
  - Ataque Lagarias-Odlyzko
  - Ataque Coster et al

Densidad

Definición

Sea $a = (a_1, ..., a_n)$ un vector de pesos, definimos la *densidad del vector* a como:

$$d(a) = \frac{n}{log_2(max\ a_i)} \text{ , con } i = 1, ..., n$$

Este valor es una medida aproximada de la tasa de información a la que se transmiten los bits. Así, definimos la *densidad de un problema* como la densidad de su vector solución.

Retículo

Definición

Un *retículo de enteros* L es un subgrupo aditivo de $\mathbb{Z}^n$, que contiene n vectores linealmente independientes sobre $\mathbb{R}^n$.

Definición

Una *base* $(v_1, ..., v_n)$ de un retículo de enteros L es un conjunto de elementos de L que verifica:

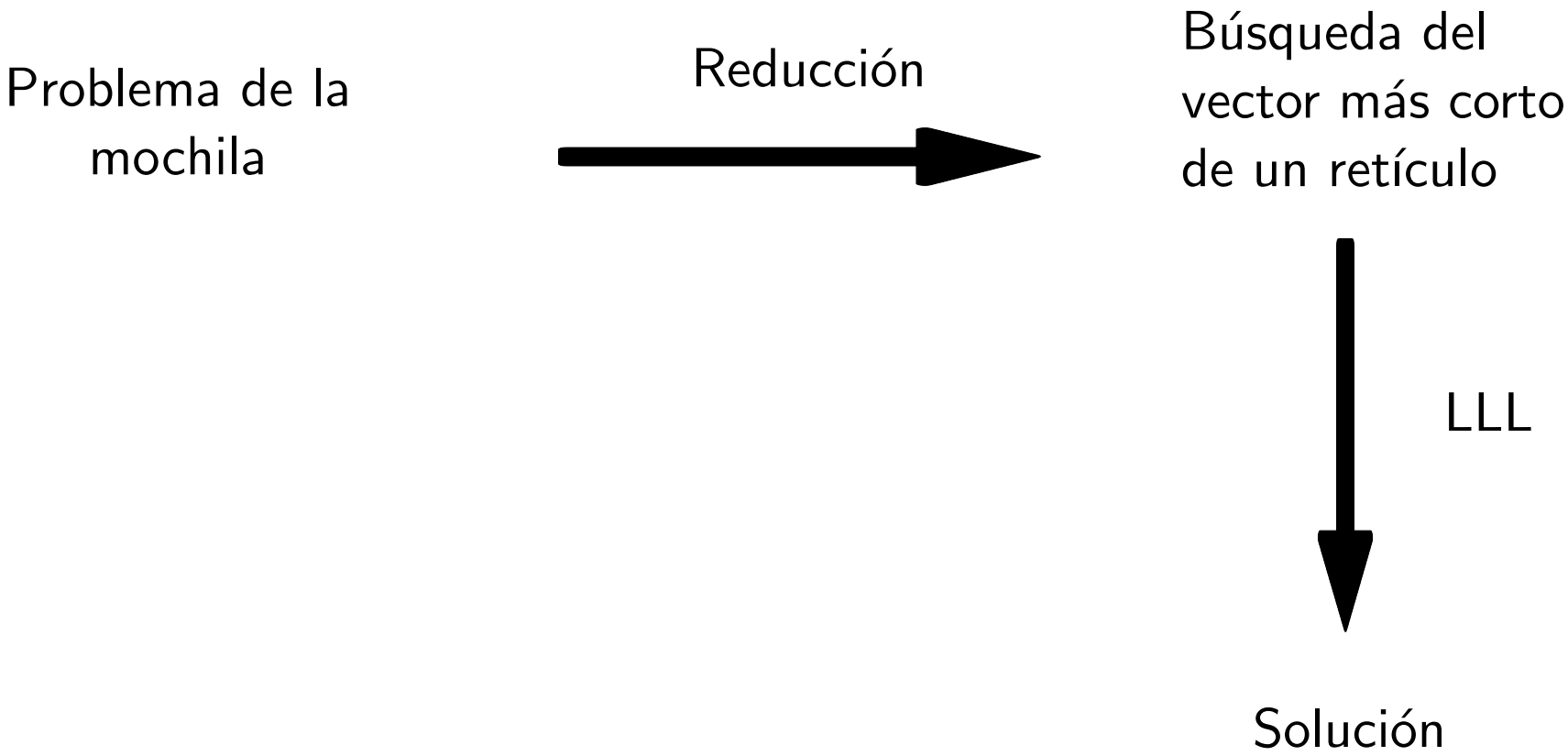
$$L = \sum_{i=1}^{n} \mathbb{Z}v_i = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$$

Algoritmo L^3

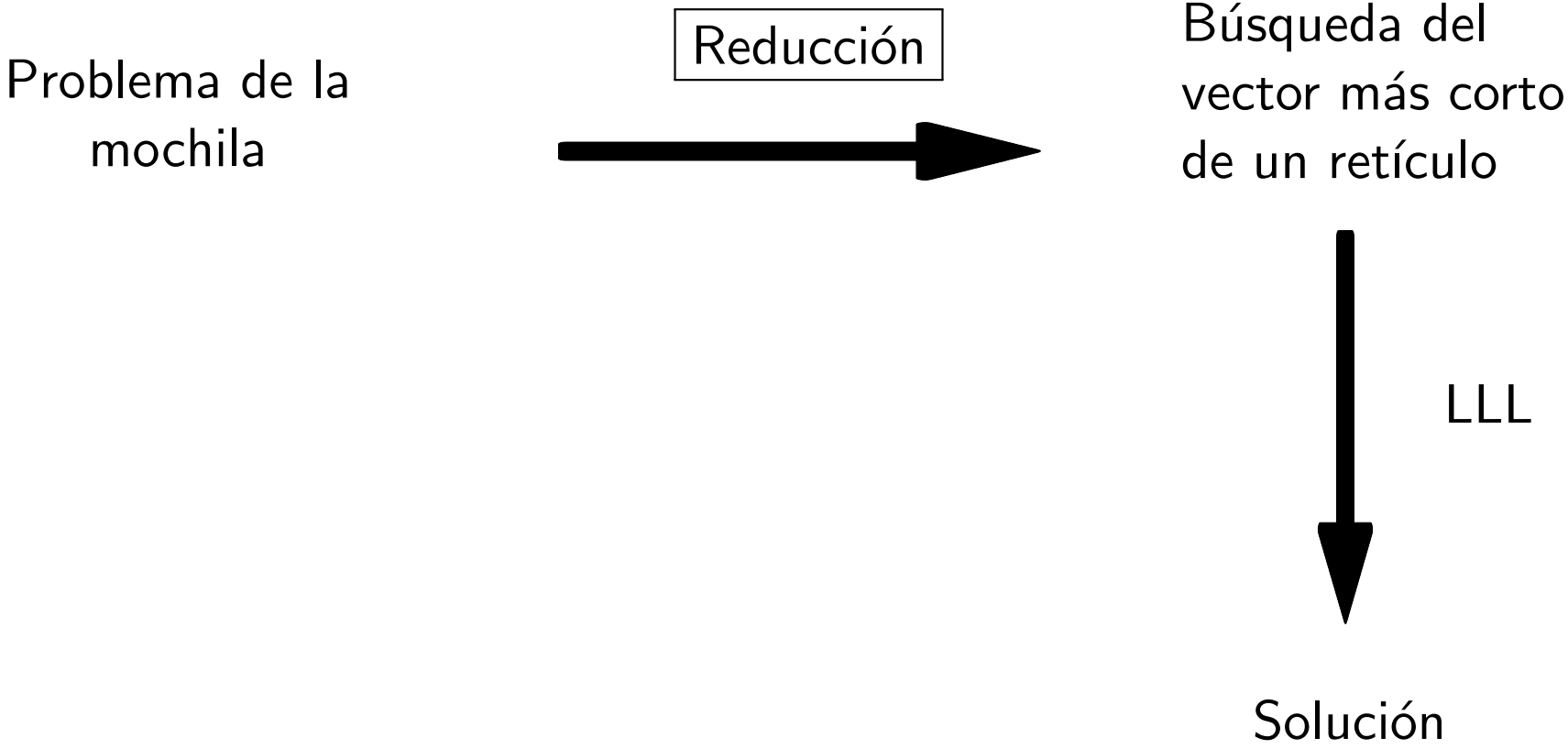
Base $b = (b_1, ..., b_n)$ del retículo $L \subset \mathbb{R}^n$

Base α-reducida del retículo $L \subset \mathbb{R}^n$

Ataques por baja densidad



Ataques por baja densidad



Ataques a Merkle-Hellman

- Ataque de Shamir
- Ataques por baja densidad
  - Ataque Lagarias-Odlyzko
  - Ataque Coster et al

Ataques a Merkle-Hellman

- Ataque de Shamir
- Ataques por baja densidad
  - **Ataque Lagarias-Odlyzko**
  - Ataque Coster et al

Reducción de Lagarias-Odlyzko

Sea la clave pública $a = (a_1, ..., a_n)$, y M la capacidad máxima de la mochila, esto es, el mensaje cifrado.

$$\begin{aligned} b_1 &= (1, 0, ..., 0, -a_1) \\ b_2 &= (0, 1, ..., 0, -a_2) \\ &\vdots \\ b_n &= (0, 0, ..., 1, -a_n) \\ b_{n+1} &= (0, 0, ..., 0, M) \end{aligned}$$

Ataques a Merkle-Hellman

- Ataque de Shamir
- Ataques por baja densidad
  - Ataque Lagarias-Odlyzko
  - Ataque Coster et al

Ataques a Merkle-Hellman

- Ataque de Shamir
- Ataques por baja densidad
  - Ataque Lagarias-Odlyzko
  - **Ataque Coster et al**

Reducción de Coster et al

Sea la clave pública $a = (a_1, ..., a_n)$, M la capacidad máxima de la mochila y un valor $N > \frac{1}{2}\sqrt{n}$.

$$\begin{aligned} b_1 &= (1, 0, ..., 0, N \cdot a_1) \\ b_2 &= (0, 1, ..., 0, N \cdot a_2) \\ &\vdots \\ b_n &= (0, 0, ..., 1, N \cdot a_n) \\ b_{n+1} &= (0, 0, ..., 0, N \cdot M) \end{aligned}$$

Resultados experimentales

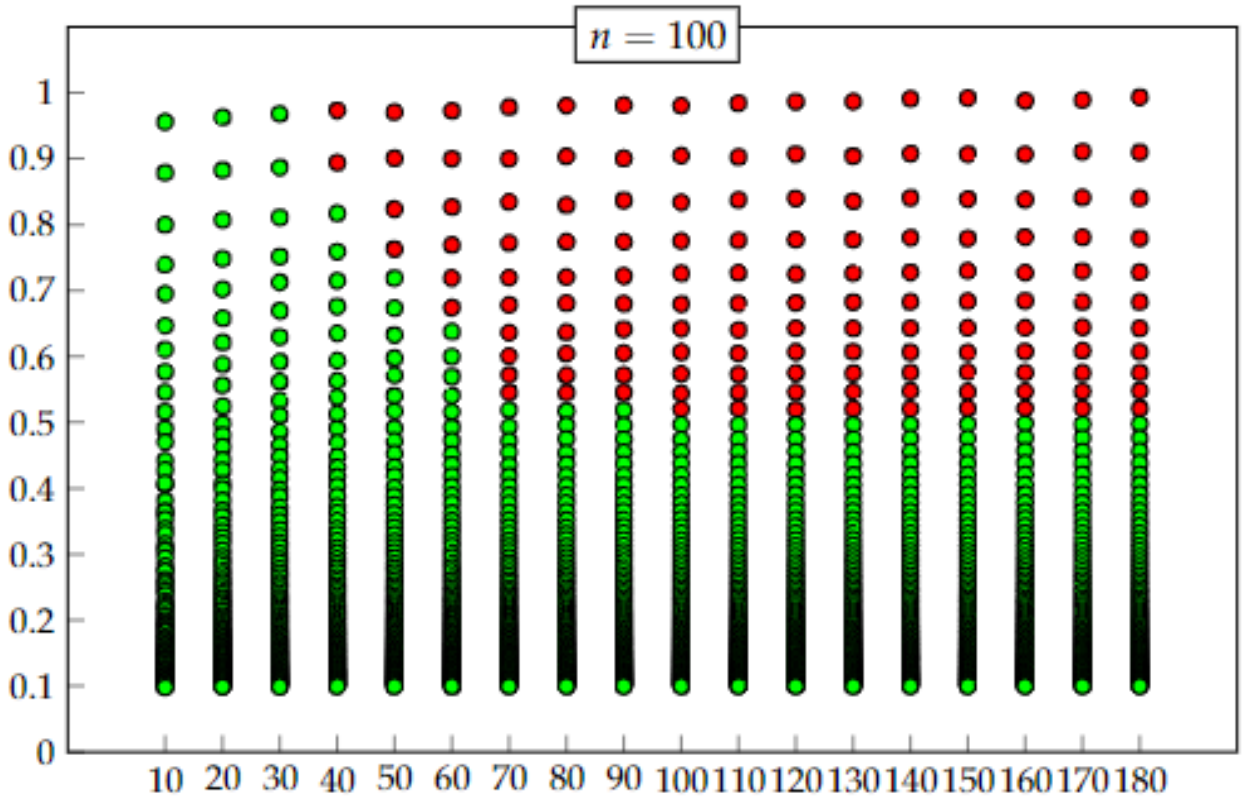


Figura: Relación tamaño-densidad

Tabla de contenidos

1. Criptografía básica
   - Introducción a la criptografía
   - Criptografía simétrica vs asimétrica
2. Problema de la mochila
3. Criptosistema de Merkle-Hellman
   - Método básico
   - Método iterativo
4. Ataques a este criptosistema
   - Shamir
   - Lagarias-Odlyzko
   - Coster et al
5. Criptosistema de Chor-Rivest
6. Conclusiones

Chor-Rivest

- Método de generación de claves
- Cifrado
- Descifrado

Chor-Rivest

- **Método de generación de claves**
- Cifrado
- Descifrado

Generación de claves (I)

Debemos tener en cuenta:

- Requiere computar logaritmos discretos en cuerpos finitos
- No se conoce un método para todos los casos, pero si para algunos (Pohlig-Hellman)

Comenzamos tomando:

- Potencia de un primo $q = p^{\lambda}$
- Entero positivo $h \leq q$

tal que sea fácil trabajar con logaritmos discretos en $\mathbb{F}_{q^h}$.

Generación de claves (II)

A continuación:

1. Elegir una raiz $t \in \mathbb{F}_{q^h}$ de un polinomio mónico irreducible de grado h, $F(x) \in \mathbb{F}_q[x]$.
2. Seleccionar un generador g, del grupo multiplicativo $\mathbb{F}^*_{q^h}$.
3. Calcular $a_i = log_g(t + \alpha_i)$, para todo $\alpha_i \in \mathbb{F}_q$.
4. Reordenar los elementos aplicando una permutación π.
5. Generar ruido aplicando:

$$c_i \equiv (b_i + r) \bmod (q^h - 1)$$

con $0 \leq r \leq q^h - 2$.

Generación de claves (III)

Obtendremos así:

- Clave privada

$$sk = (t, g, \pi, r)$$

- Clave pública

$$pk = (c_0, ..., c_{q-1}, q, h)$$

Chor-Rivest

- Método de generación de claves
- Cifrado
- Descifrado

Chor-Rivest

- Método de generación de claves
- **Cifrado**
- Descifrado

Cifrado

Se necesita:

- Clave pública $pk = (c_0, ..., c_{q-1}, q, h)$
- Mensaje $m = (m_0, ..., m_{q-1})$ con h unos.

Cálculo del mensaje cifrado:

$$y = \sum_{i=0}^{q-1} x_i \cdot c_i \pmod{q^h - 1}$$

Chor-Rivest

- Método de generación de claves
- Cifrado
- Descifrado

Chor-Rivest

- Método de generación de claves
- Cifrado
- **Descifrado**

Descifrado (I)

Se necesita:

- Clave privada $sk = (t, g, \pi, r)$
- Mensaje cifrado y

Descifrado (II)

Cálculo del mensaje descifrado:

1. Calcular:
$$y' \equiv y - h \cdot r \pmod{q^h - 1}.$$
2. Obtener $g^{y'}$ escrito como polinomio en x:
$$g^{y'} = g^y \cdot g^{-hr} = \ldots = \prod_{i \in I}(t + \alpha_{\pi(i)})$$
3. Obtener:
$$F(x) + Q(x) = \prod_{i \in I}(x + \alpha_{\pi(i)})$$
4. Sustituir los valores $\alpha_0, \ldots, \alpha_{q-1} \in \mathbb{F}_q$ para obtener las h raices de ese polinomio, que forman el mensaje.

Ataques principales

- Goldreich y Odlyzko
- Brickell
- Lagarias-Odlyzko
- Schnorr y Hörner
- Vaudenay

Ataques principales

- Goldreich y Odlyzko
- Brickell
- Lagarias-Odlyzko
- Schnorr y Hörner
- **Vaudenay**

Tabla de contenidos

1. Criptografía básica
   - Introducción a la criptografía
   - Criptografía simétrica vs asimétrica
2. Problema de la mochila
3. Criptosistema de Merkle-Hellman
   - Método básico
   - Método iterativo
4. Ataques a este criptosistema
   - Shamir
   - Lagarias-Odlyzko
   - Coster et al
5. Criptosistema de Chor-Rivest
6. Conclusiones

Conclusiones

- Hemos analizado los fundamento teóricos de diversos criptosistemas y sus ataques principales, y destacado su relevancia práctica mediante su implementación, plasmando el conocimiento estudiado en aplicaciones concretas.
- No se puede garantizar la total seguridad de un sistema criptográfico.
- Primer acercamiento profesional, y como tal, queda abierto ante futuras investigaciones en criptografía y computación cuántica.

Bibliografía fundamental

- Joachim von zur Gathen. CryptoSchool. Springer, 2016. pages 13-56
- Ralph C. Merkle and Martin E. Hellman. Hiding information and signatures in trapdoor knapsacks. IEEE Transactions on Information Theory, IT-24(5), Septiembre 1978.
- Adi Shamir. A polynomial-time algorithm for breaking the basic merkle-hellman cryptosystem. IEEE Transactions on Information Theory, IT-30(5), Septiembre 1984.
- Raul Durán Díaz, Luis Hernández-Álvarez, Luis Hernández Encinas, and Araceli Queiruga-Dios. Chor-rivest knapsack cryptosystem in a post-quantum world. Springer Nature Switzerland, Agosto 2021.