Implementación del sistema de cifrado Merkle-Hellman

Manuel Rábade García

Facultad de Ingeniería

Universidad Nacional Autónoma de México

Los sistemas de cifrado de llave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí [1].

En 1976 W. Diffie y M. Hellman introdujeron el concepto de cifrado de llave pública. Dos años después R. Merkle y M. Hellman publicaron un sistema de cifrado basado en el problema de la suma de subconjuntos [2]. En su tiempo este sistema fue la única alternativa al sistema de cifrado RSA.

El problema de la suma de subconjuntos podemos enunciarlo como: dado un conjunto de enteros A y un entero s, ¿existe algún subconjunto cuya suma sea s? La suma de subconjuntos también puede verse como un caso especial del problema knapsack o de la mochila.

Existen vectores knapsack tales que la solución de un problema (A, s) se puede calcular fácil y eficientemente como es el caso de los vectores knapsack super incrementales [3]. Por el otro lado puede ser muy difícil obtener una solución para (A, s) si A no es super incremental. Merkle y Hellman utilizaron este hecho para construir un sistema de cifrado basado en el problema de la suma de subconjuntos.

Empezando con un vector knapsack super incremental A, un segundo vector B es generado ocultado la propiedad super incremental de A. El vector knapsack A es parte de la llave privada mientras el vector knapsack B es la llave pública. Un mensaje p es cifrado calculando la suma $c = pB = b_1p_1 + ... + b_np_n$, donde p_i representa el bit i de p.

Cualquiera en posesión de la llave c se encuentra con el difícil problema (B, c). En cambio el propietario de la llave privada puede determinar fácilmente el mensaje original porque conoce la secuencia secreta super incremental A.

El sistema de cifrado Merkle-Hellman consiste en lo siguiente:

1. Generación de llaves

- Un parámetro n es fijado especificando el número de componentes en A y B.
- Se elige un vector super incremental $A = (a_1, ..., a_n)$.
- Se elige un entero M tal que $M > SUM_{i=1...n}(a_i)$. M es llamado el módulo.
- Se elige un multiplicador W tal que $mcd(M, W) = 1$ y $1 < W < M$. Esta elección de W garantiza que existe un elemento inverso U: $UW = 1 \pmod M$.
- Para obtener los componentes b_i de la llave pública B se calcula:

$$b_i = a_{pi(i)} W \bmod M, \; i = 1 \ldots n$$

La propiedad super incremental de A es oculta por la multiplicación modular.

- B representa la llave pública y la tupla (A, M, W) la llave privada.

2. Cifrado

- La longitud del mensaje p es determinada por el parámetro n. Es posible cifrar un mensaje p mas largo dividiéndolo en grupos de n-bits.
- Sea $p = (p_1, p_2, ..., p_n)$ el mensaje a cifrar, la clave c se obtiene calculando:

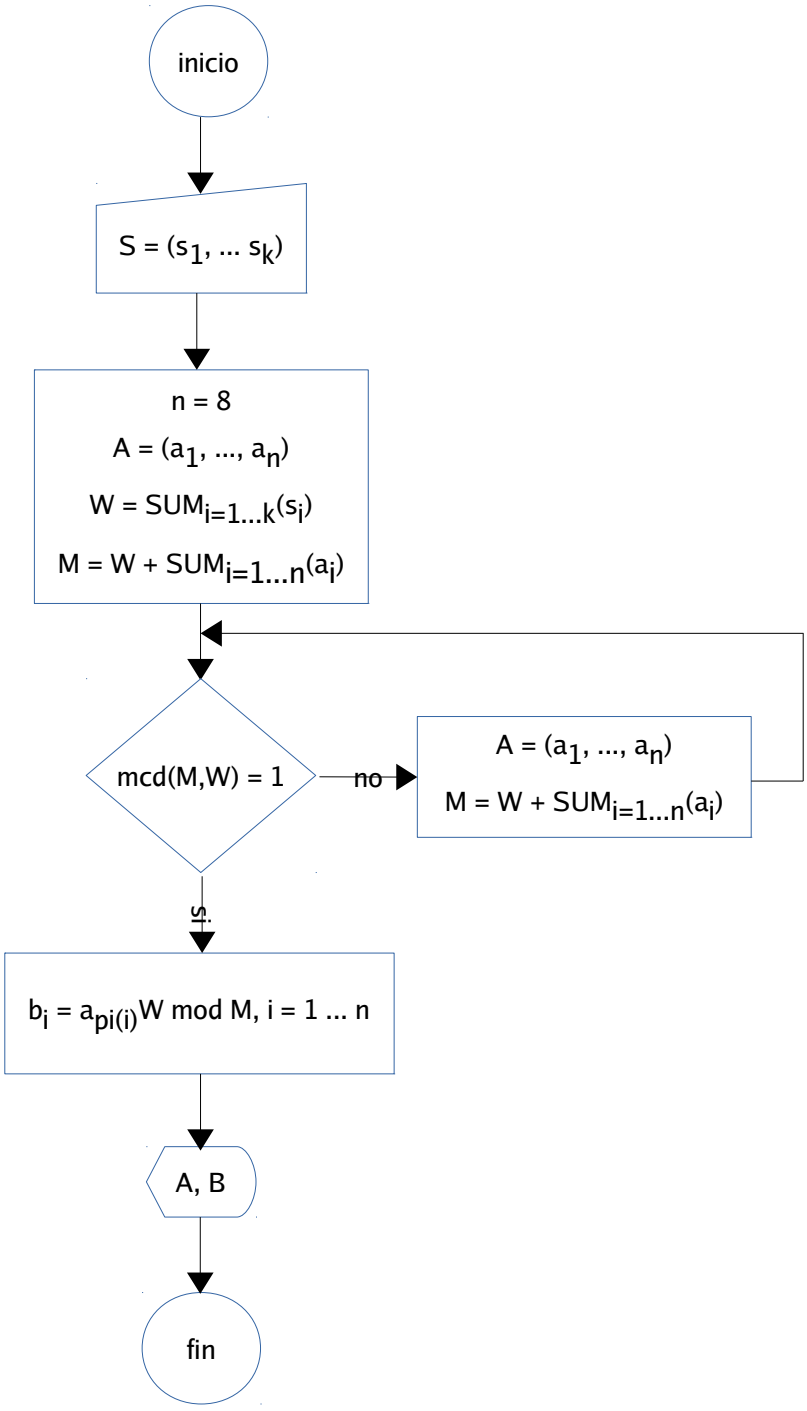
$$c = b_1 p_1 + b_2 p_2 + \ldots + b_n p_n$$

La componente i de B es sumada si el bit i de p es uno.

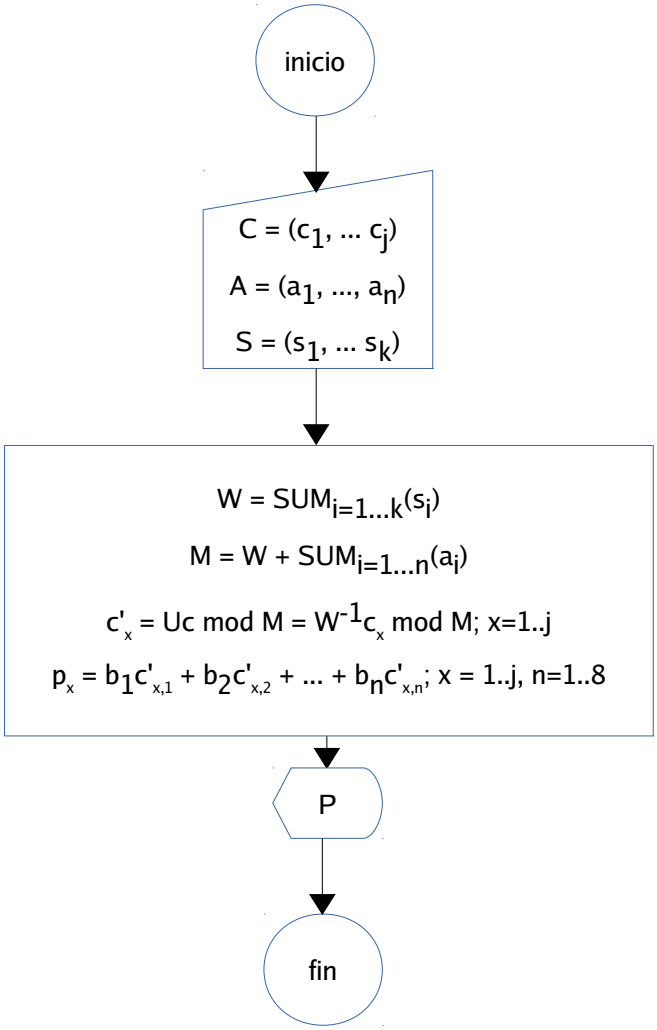
3. Descifrado

- Se debe calcular el inverso del multiplicador: q.
- Ahora resuelve el problema (A, c'). Como A es super incremental, (A, c') es fácilmente resuelto. Sea $X = (x_1, ..., x_n)$ el vector de resultado, $p_i = x_i$ y $p = (p_1, ..., p_n)$ es el mensaje en texto plano.

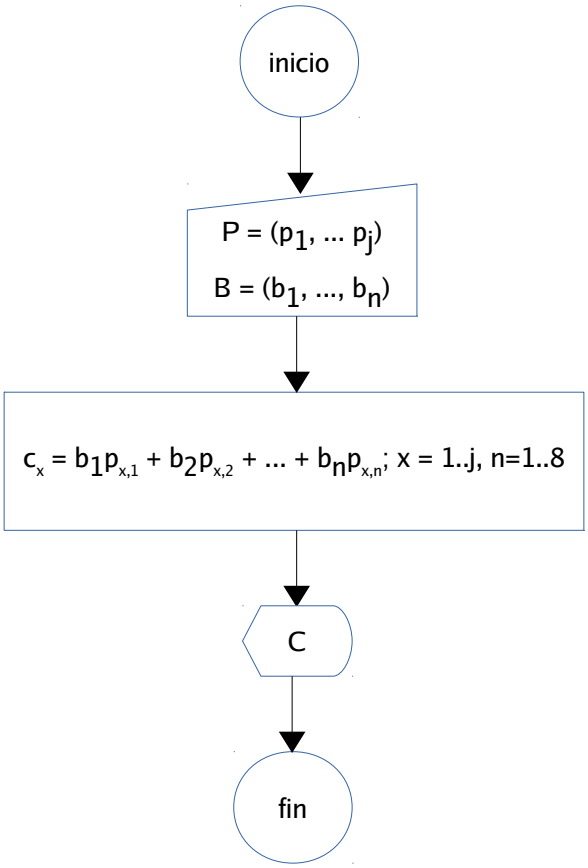
Algoritmos



Generación de llaves


inicio
C = (c1, ... cj)
A = (a1, ..., an)
S = (s1, ... sk)
W = SUMi=1...k(si)
M = W + SUMi=1...n(ai)
c'x = Uc mod M = W-1cx mod M; x=1..j
px = b1c'x,1 + b2c'x,2 + ... + bnc'x,n; x = 1..j, n=1..8
P
fin

Cifrado



Descifrado

Implementación

- La llave privada consiste en números aleatorios provenientes del generador de entropía del núcleo Linux.

- El multiplicador es la sumatoria del código ASCII correspondiente a los caracteres de la llave secreta proporcionada por el usuario.

- El módulo es la adición del multiplicador y la sumatoria de todos los elementos de la llave privada.

- El multiplicador y módulo deben ser primos entre si, en caso contrario se genera un nuevo vector super incremental y se calcula nuevamente el módulo y multiplicador repitiendo este proceso hasta que el mínimo común divisor entre ambos sea la unidad.

- La longitud de las llaves es de 8 enteros y el mensaje es dividido en el código ASCII correspondiente a cada carácter.

Referencias

[1] Simmons, G.J. "A survey of Information Authentication", Contemporary Cryptology: The science of information integrity, 1992.

[2] Merkle, R.; Hellman, M.E. "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Transactions on. Information Theory, Volumen 24 Publicación 5, Septiembre 1978.

[3] Reinhardt, K. "The Subset Sum Problem ", Kryptologie und Komplexitat interaktiv, 2004.