Algoritmia básica
3^o Grado en Ingeniería en Informática. Itinerario Computación
Curso 2022/23

Práctica 1: Algoritmos voraces

16 de febrero de 2023

Organización general de las prácticas.

Equipos de trabajo

Se han formado equipos de dos personas. Si una de las dos abandona la asignatura, la otra deberá terminar en solitario.

Entrega de la práctica

Las entregas de prácticas se realizarán en el computador `hendrix`.

- La entrega de la práctica mediante la ejecución de:

  ```
  someter ab_22 practica.tar
  ```

El fichero `practica.tar` contendrá **un directorio denominado practica_NIA1_NIA2** (siendo NIA1 y NIA2 los números identificadores de cada estudiante asignados por la Universidad de Zaragoza, y NIA1 será el NIA menor. En el caso de un grupo de prácticas formado por un único alumno, la carpeta tendrá como nombre practica_NIA con el identificador de ese alumno) con los ficheros de texto incluyendo:

- Descripción general del programa: cómo está organizado, qué se puede y qué no se puede hacer (tiene que llamarse **LEEME**).

  Contendrá en sus primeras líneas la lista de integrantes del grupo, con el siguiente formato:

  ```
  Apellido1 Apellido2, Nombre [tab] correo@electronico [tab] login en hendrix
  Apellido1 Apellido2, Nombre [tab] correo@electronico [tab] login en hendrix
  ```

  en orden alfabético. Donde [tab] representa el caracter tabulador.

- Listados del código debidamente comentados y dispuestos para ser compilados y utilizados. Deberán seguir una estructura lógica para poder encontrar y navegar adecuadamente cada una de las partes de la práctica.

- Un programa para la *shell* denominado `ejecutar.sh` que automatice la compilación y ejecución de los programas entregados con algunos casos de prueba. Deberá funcionar en hendrix. Idealmente, este *script* llamaría a otro por cada una de las partes de la práctica, que deberían poder ejecutarse de manera independiente.
- Los ficheros auxiliares de entrada necesarios para ejecutar las pruebas del punto anterior.
- Un fichero en formato PDF con el análisis de las pruebas realizadas (máximo 3 páginas, sin portada). Indicar: nombre, apellidos y NIA de cada miembro del grupo de prácticas.

Evaluación

- En la calificación se tendrán en cuenta los siguientes aspectos: documentación, funcionamiento, implementación, diseño de tests de pruebas, análisis de las pruebas realizadas y facilidad para la repetición de las pruebas por los profesores.
- Se aplicarán las reglas de tratamiento de casos de plagio explicadas en la presentación de la asignatura.

Aproximación a la criptogafía

Vamos a desarrollar un sistema de cifrado de clave pública sencillo. Se trata del sistema descrito por Merkle y Hellman [MH78], y está basado en el problema de la mochila.

Para empezar, vamos a recordar una versión simple del problema generalizado de la mochila: "Dados una mochila de capacidad N y un número de 'objetos' de volúmenes e_i, $i \in \{1, 2, ..., n\}$, el objetivo consiste en llenar completamente la mochila con los objetos siempre que sea posible; esto es, se trata de encontrar un subconjunto $I \subseteq \{1, 2, ..., n\}$ tal que $\sum_{i \in I} e_i = N$, si es que existe tal subconjunto." Más formalmente: "Dado un conjunto $\{e_i\}$ con n enteros positivos y un entero N, encontrar un entero k que expresado en binario con n bits, $k = (b_n, ..., b_2, b_1)$ y tal que $\sum_{i \in I} b_i \cdot e_i = N$ (el bit i, b_i, representa si el entero e_i se incluye o no)."

El problema de la mochila generalizada tiene un caso especial: cuando los valores e_i, ordenados de forma creciente, cumplen la propiedad de que cada uno es mayor que la suma de los anteriores ($e_i > \sum_{j=1}^{i-1} e_j$), hablamos de la mochila fácil[1]. Mientras que el problema de la mochila general es muy difícil (de hecho es NP–completo), el de la mochila fácil se resuelve de modo trivial aplicando un esquema voraz.

El criptosistema de Merkle–Hellman se basa en algunas propiedades interesantes de este problema. Consideremos que el mensaje que se desea codificar está representado en binario, y dividido en bloques de tamaño n, donde cada bloque se denota como M y n es un entero escogido por el usuario.

1. El usuario elige una mochila fácil $\{e_1, e_2, ..., e_n\}$, un entero N mayor que $\sum_{i \in I} e_i$, y un entero grande w primo[2] con N y tal que $0 < w < N$.

2. El usuario calcula $w^{-1}(mod\ N)$[3]. Después calcula la tupla $\{a_1, a_2, ..., a_n\}$, definida mediante $a_i = w \cdot e_i (mod\ N)$. Los números e_i, N, w, w^{-1} son secretos y se publica la tupla a_i. La clave de cifrado entonces es $K_{pub} = \{a_1, a_2, ..., a_n\}$, y la de descifrado es $k_{priv} = (w, N)$.

3. El que quiera enviarnos un bloque de mensaje binario $M = (M_1, M_2, ..., M_n)$ tiene que calcular $C = \sum_{i=1}^{n} M_i \cdot a_i$ y trasmitir ese entero.

4. Para descifrar el mensaje, deberemos calcular $w^{-1} \cdot C(mod\ N)$ que corresponde a: $V = \sum_{i=1}^{n} M_i \cdot e_i$ (ya que $\sum_{i=1}^{n} M_i \cdot e_i \leq \sum_{i=1}^{n} e_i \leq N$. Entonces, utilizar el algoritmo de resolu-

[1] *superincreasing knapsack*

[2] dos enteros, w y N, se dicen primos entre sí si su máximo común divisor es 1

[3] $w^{-1}(mod\ N) = w'$ si y sólo si $w \cdot w' = 1(mod\ N)$; por ejemplo, el inverso de $3(mod\ 7)$ es 5 porque $3 \cdot 5 = 15$ y $15(mod\ 7) = 1$

ción de la mochila fácil para encontrar la solución única $M = (M_1, ..., M_n)$, recuperando de esta forma el mensaje.

Veamos un ejemplo. Se toman como unidades del mensaje original las letras del alfabeto de 26 letras y se utiliza una codificación binaria (de longitud 5). Si la clave secreta es la 5-tupla $(2, 3, 7, 15, 31)$ y se escoge $N = 61$ y $w = 17$, entonces se calcula $w^{-1} = 18 = 17^{-1}(mod\ 61)$. Mediante $a_1 = 17 \cdot 2 = 34(mod\ 61)$, $a_2 = 17 \cdot 3 = 51(mod\ 61)$, $a_3 = 17 \cdot 7 = 58(mod\ 61)$, $a_4 = 17 \cdot 15 = 11(mod\ 61)$ y $a_5 = 17 \cdot 31 = 39(mod\ 61)$, se obtiene la clave de cifrado $(34, 51, 58, 11, 39)$. Para enviar el mensaje "HAY"se utiliza la siguiente correspondencia:

$$\begin{array}{ll} H = (01000) \longrightarrow & 0 \cdot 34 + 1 \cdot 51 + 0 \cdot 58 + 0 \cdot 11 + 0 \cdot 39 = 51 \\ A = (00001) \longrightarrow & 0 \cdot 34 + 0 \cdot 51 + 0 \cdot 58 + 0 \cdot 11 + 1 \cdot 39 = 39 \\ Y = (11001) \longrightarrow & 1 \cdot 34 + 1 \cdot 51 + 0 \cdot 58 + 0 \cdot 11 + 1 \cdot 39 = 124 \end{array} \quad (1)$$

Para descifrar el mensaje (51, 39,124) primero se multiplica por 18 en módulo 61, obteniendose (3, 31, 36), y luego se resuelve el problema fácil de la mochila con la clave secreta (2,3,7,15,31) para cada uno de los tres casos, recuperando así el mensaje original.

Bibliografía

[MH78] R.C. Merkle and M.E. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*, IT–24:525–530, 1978.