Experiencias Docentes

Una práctica para fomentar el trabajo en equipo secuencial en materias matemáticas

A practice to enhance sequential team work in mathematical topics

Javier Rodrigo Hitos

Susana Merchán Rubira

Revista de Investigación

Volumen XII, Número 1, pp. 077–083, ISSN 2174-0410
Recepción: 1 Abr'21; Aceptación: 7 ene'22

1 de abril de 2022

Resumen

Este artículo presenta la experiencia de la realización de una práctica con ordenador en la que los estudiantes de la clase se dividieron en grupos y cada grupo de estudiantes, de segundo curso de ingeniería informática, necesitaba el resultado del grupo anterior para hacer su parte. La práctica fomentaba, por tanto, el trabajo secuencial en equipo, que es el que los alumnos se van a encontrar en el futuro cuando trabajen en empresas de ingeniería, lo que pone en valor a la experiencia didáctica.

La práctica, encuadrada en la asignatura de Matemática Discreta, consistía en el cifrado y descifrado de un mensaje utilizando el algoritmo RSA y un software matemático del grupo Wolfram, como es el Mathematica. Este algoritmo se estudió en las clases de teoría dentro del tema dedicado a la teoría de números, como un ejemplo de "aplicación a la vida real" de conceptos clásicos que se estudian en este tema, como los números primos, la aritmética modular o el teorema de Euler. Por tanto, además de su importancia pedagógica, la práctica proporcionó a los alumnos los medios para implementar esta aplicación.

Palabras Clave: Trabajo en equipo, prácticas con ordenador, Matemática Discreta, algoritmos.

Abstract

This paper presents the work performed by the authors with the objective of carrying out a practical experience with the students of the second course of Computer Engineering degree in the computer room. In this experience, firstly, the students are divided into groups. Due to the construction of the exercise, each group of students needed the results of the previous group to do its part of the work. In this way, the practical session improves the ability of the students to work by teams in a sequenced way. Since team working is one of the main abilities that Engineering Companies value in their workers, this didactic experience could be an interesting opportunity to enhance this skill in future engineers.

The practice is framed in the field of Discrete Mathematics. It consists in encoding and decoding a message by applying the RSA algorithm by means of Mathematica (the math software of the Wolfram team). The algorithm was developed in the theoretical sessions within the topic dedicated to the Number Theory as an example of the real life application of classical concepts that are studied in this field, such as the prime numbers, the modular arithmetic and the Euler theorem. Therefore, besides its didactical importance, the practice also provides resources for the students to implement this application.

Keywords: Team working, practice with computers, Discrete Mathematics, algorithms.

1. Introducción

La realización de prácticas con ordenador es útil en las asignaturas con contenido matemático, ya que sirven para ilustrar con ejemplos algunos de los contenidos que se explican en la clase teórica. El ordenador permite, además, la realización de problemas con números altos, lo que a veces se ajusta más a casos de la vida real. Se fomenta además el desarrollo de algunas competencias, como pueden ser el trabajo en grupo, la capacidad de comunicación, el uso del lenguaje matemático o científico y la participación en clase.

La práctica que se comenta en este artículo tuvo la particularidad de que los grupos de trabajo buscaban un objetivo común, para el que cada uno tenía que realizar la parte que le correspondía, no pudiendo cada grupo realizar su cometido hasta que no tuviera el resultado del grupo anterior, teniendo que comunicarse entre sí para completar el ejercicio. Esto hizo que el trabajo en equipo no se limitara al realizado en los distintos grupos constituidos, ya que cada grupo debía interactuar con los demás, en lo que resultó una simulación de la forma de trabajar en las empresas, en las que se realizan proyectos donde diversos subgrupos hacen partes del trabajo (tareas) que luego se ponen en común. Esto resulta útil para los estudiantes, porque les adelanta el modo de trabajar que pueden tener en su vida profesional y porque les prepara también a nivel personal para enfrentarse a situaciones en las que hay que trabajar en común por el bien de la comunidad.

2. La práctica puesta en contexto

La práctica que se comenta en la introducción se realizó el curso 2008-2009 en la asignatura Matemática Discreta, perteneciente al segundo curso de la titulación superior de Ingeniería Informática impartida en la Universidad Pontificia Comillas.

El objetivo de la práctica era llevar a cabo un algoritmo de codificación que se estudiaba en las clases teóricas como una aplicación de la teoría de números, la parte más clásica de la Matemática Discreta. De esta forma, los estudiantes conocían una aplicación actual de conceptos, en principio muy teóricos, y ajenos a toda aplicación práctica.

En concreto, las definiciones y resultados de la teoría de números que se explicaban en el tema y se utilizan en el algoritmo son (ver [1], [2] y [3]):

-Número primo: número divisible sólo por él mismo y por la unidad (por ejemplo, 3 es primo, 4 no es primo, 5 es primo…)

-Números primos relativos: números que no tienen ningún factor primo común (por ejemplo, 3 y 8 son primos relativos, 6 y 10 no son primos relativos)

-Números congruentes módulo *n*: dos números cuya diferencia es múltiplo de *n* (por ejemplo 2 y 7 son congruentes módulo 5 y se escribe 2 ≡ 7 (5), 3 y 7 no son congruentes módulo 5)

- Inverso de *a* módulo *n*: un número *b* entre 1 y *n* tal que $a\,b$ es congruente con 1 módulo *n* (es decir, un número *b* mayor o igual que 1 y menor que *n* tal que al dividir $a\,b$ entre *n* dé resto 1. Por ejemplo, 3 es el inverso de 2 módulo 5)

- Función φ de Euler: función que a cada n le asigna el número de números que hay menores que *n* y primos relativos con *n* (por ejemplo, $\varphi(4)=2$)

- Teorema: *a* tiene inverso módulo *n* si y sólo si *a* y $\varphi(n)$ son primos relativos

- Teorema de Euler: si elevamos un número *a*, primo relativo con *n*, a $\varphi(n)$, queda un número congruente con 1 módulo *n* (por ejemplo, 3 es primo relativo con 4 y $3^{\varphi(4)}=3^2=9$ es congruente con 1 módulo 4).

El algoritmo que se implementó en la práctica y que se comenta en la siguiente sección es un algoritmo de cifrado y descifrado conocido como algoritmo RSA (ver [4]).

3. El algoritmo RSA

Este algoritmo surgió por la necesidad de cifrar mensajes de una forma más segura que la que se hacía hasta ese momento, ya que la irrupción de los ordenadores y la necesidad de enviar desde ellos números privados, como números de tarjetas de crédito, pins,… hacía que fuera importante el crear un sistema de cifrado mediante una clave pública en el que sólo el interesado, con una clave privada, pudiera descifrar el mensaje.

Debe su nombre a las iniciales de los autores del algoritmo: Rivest, Shamir y Adleman, investigadores del MIT (Instituto Tecnológico de Massachussets). Antes de describirlo, necesitamos definir de forma rigurosa los conceptos de clave pública y clave privada mencionados anteriormente:

Definición. Clave pública

Una clave pública es un par (e,n) donde $n=p\,q$ para dos números primos determinados, $e>1$ es cualquier número primo relativo con $\varphi(n)=(p-1)(q-1)$

Definición. Clave privada

Una clave privada es un par (d,n) donde n es como en la definición anterior, d es el inverso de e módulo $\varphi(n)$ (existe porque e , $\varphi(n)$ son primos relativos).

El algoritmo tiene dos partes, generación de claves y cifrado y descifrado del mensaje (un número *m*). Sus pasos son:

-Generación de claves

Paso 1: Tomamos dos primos mayores que *m*, *p* y *q*, y definimos $n=p\,q$

Paso 2: Hallamos $\varphi(n)=(p-1)(q-1)$

Paso 3: Hallamos un número $e > 1$ primo relativo con $\varphi(n)$

Paso 4: Hallamos el inverso de *e* módulo $\varphi(n)$ (le llamamos *d*)

Output: La clave pública es (e, n) y la privada (d, n), para los *e*, *d*, *n* hallados.

- Cifrado y descifrado

Paso 1 (para cifrar, a partir de la clave pública): elevamos *m* (el número que queremos cifrar) a *e* y tomamos módulo *n* (para que no quede muy grande)

Paso 2 (para descifrar, a partir de la clave privada): elevamos el número cifrado a *d* y tomamos módulo *n* (obtenemos así *m*)

Demostramos que el procedimiento para encontrar *m* es correcto utilizando el teorema de Euler:

Tenemos que $(m^e)^d = m^{e\,d}$. Como *d* es el inverso de *e* módulo $\varphi(n)$, tenemos que $e\,d \equiv 1(\varphi(n))$, por lo que $e\,d = k\,\varphi(n)+1$ para cierto natural *k*. Entonces:

$m^{e\,d} = m^{k\,\varphi(n)+1} = (m^{\varphi(n)})^k\ m$. Por otro lado, como *m* y *n* son primos relativos, por el teorema de Euler tenemos que $m^{\varphi(n)} \equiv 1(n)$, por lo que $m^{e\,d} = (m^{\varphi(n)})^k\ m \equiv m(n)$ y así al elevar el número cifrado a *d* y tomar módulo *n*, efectivamente da *m*.

Ejemplo

Supongamos que queremos cifrar *m*=2. Generamos primero las claves:

Paso 1: Tomamos, por ejemplo *p*=5 y *q*=11, y definimos $n = 5 \times 11 = 55$

Paso 2: Tenemos que $\varphi(n) = 4 \times 10 = 40$

Paso 3: Tomamos, por ejemplo, $e = 7$ (primo relativo con 40).

Paso 4: Hallamos el inverso de *e* módulo 40: *d*=23

Entonces, la clave pública es (7, 55) y la privada (23, 55)

Cifrado: elevamos 2 a $e = 7$ y da 128, que módulo *n*=55 es 18: éste es el número en clave

Descifrado: elevamos el número cifrado: 18 a *d*=23 y tomamos módulo *n*=55. Efectivamente da 2.

Observación

En el ejemplo es fácil descifrar porque *n* es el producto de dos primos pequeños, luego es fácil hallar $\varphi(n)$, fundamental para descifrar porque te da la clave privada. En cambio si *p* y *q* son grandes, es difícil factorizar *n* para poder hallar $\varphi(n)$. Es por esto que son muy valiosos los primos grandes.

4. Desarrollo de la práctica

La práctica se llevó a cabo en una sesión de clase de 50 minutos, en un aula de ordenadores. Para la misma se utilizó el software Mathematica 5.0, de Wolfram, del que se hizo una breve introducción al principio de la práctica.

Se hicieron cuatro grupos de tres o cuatro alumnos cada uno: el primer grupo creó n y halló $\varphi(n)$, el segundo creó la clave pública y la privada, el tercero cifró y el cuarto descifró.

Al primer y tercer grupo se les dio el número a cifrar (m). El primer grupo tuvo que hacer las siguientes tareas:

1) Definir el número n. Para ello, encontró dos primos p y q mayores que m utilizando dos veces el comando NextPrime y los multiplicó

2) Hallar $\varphi(n)$. Para ello, multiplicó los números p-1 y q-1

Un representante del grupo dio la información de los números n y $\varphi(n)$ al segundo grupo y la de p y q al profesor (para que éste pudiera comprobar los resultados). El segundo grupo tuvo que realizar lo siguiente:

3) Hallar un número primo relativo con $\varphi(n)$. Para ello, utilizó el comando FactorInteger y buscó un primo que no estuviera en la factorización en primos de $\varphi(n)$. Se definió este número como e.

4) Hallar el inverso de e módulo $\varphi(n)$. Para ello, utilizó el comando PowerMod. Se definió este número como d.

Un representante del grupo publicó la clave (e, n) en la pizarra y pasó la clave privada (d, n) al grupo cuatro. El grupo tres se encargó de:

5) Hallar m^e y pasarlo a módulo n. Para ello, utilizó el comando Mod.

Un representante del grupo puso el número hallado (número cifrado) en la pizarra. El grupo cuatro tuvo que hacer lo siguiente:

6) Elevar el número cifrado a d y tomar módulo n.

Un representante del grupo dijo el número obtenido, que efectivamente era m, como comprobaron los grupos primero y tercero y el profesor.

Observación

El número que se dio al grupo uno fue m=1532, para el que el grupo eligió p=1543, q=1549, con los que obtuvo n=2390107, $\varphi(n) = 2387016$. El segundo grupo consiguió entonces los valores e=5, d=1909693, por lo que el número cifrado escrito en la pizarra por el tercer grupo fue 897447

5. Conclusiones y líneas de mejora futura

Las sesiones prácticas con ordenador realizadas en aulas de informática constituyen siempre una experiencia docente positiva, especialmente indicada en titulaciones con alto contenido tecnológico como la Ingeniería Informática.

La puesta en escena de la práctica sujeta a estudio tuvo como aspectos notables el hecho de que se realizara en grupos y de manera secuencial, ya que resultó ser una simulación de la forma de trabajar en los proyectos de las empresas de ingeniería, donde cada grupo de trabajo depende de la calidad de los resultados que recibe del grupo anterior y debe enviar sus resultados correctos al grupo siguiente, en busca de un objetivo final común.

En los comentarios realizados por los alumnos sobre el desarrollo de la práctica en una tutoría llevada a cabo por el profesor de la asignatura, estos manifestaron su satisfacción con la experiencia, ya que les ayudó a tener una comprensión más profunda de los conceptos explicados en las sesiones teóricas y les dio una visión más práctica de la teoría de números, el tema más árido de la asignatura para la mayoría de los estudiantes. Trazaron sin embargo unas líneas de mejora a tener en cuenta en el futuro y que se comentan a continuación.

Como principal línea de mejora, destacar que la carga de trabajo no fue del todo homogénea, no teniendo tanta actividad los grupos tres y cuatro como los dos primeros grupos. Además, un efecto negativo del trabajo secuencial fue la pasividad de los grupos cuando no les tocaba hacer su parte. A pesar de que se les animó a que fueran partícipes de todo el proceso, los grupos se relajaban antes de hacer su parte y se desentendían del resto del proceso una vez realizado su trabajo.

Para paliar esas deficiencias en el futuro, se propone llevar a cabo otro tipo de actividades con contenido matemático realizadas en grupos que trabajan persiguiendo un objetivo común, en las que cada grupo dependa en parte del trabajo del anterior pero a su vez tenga asignadas unas tareas propias que pueda realizar independientemente de los demás grupos.

Referencias

[1] CILLERUELO, Javier, CÓRDOBA, Antonio. *La teoría de los números*, Mondadori, España, 1991.

[2] HARDY, Godfrey Harold, WRIGHT, Edward Maitland. *An introduction to the theory of numbers*, Oxford Mathematics, UK, 2009.

[3] ROSEN, K. H. *Discrete Mathematics*, Mc Graw- Hill, USA, 1999.

[4] RIVEST, R., SHAMIR, A.., ADLEMAN, L. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, pp. 120–126, Communications of the ACM, Vol. 21 (2), USA, 1978.

Sobre el/los autor/es:
Nombre: Javier Rodrigo
Correo Electrónico: jrodrigo@comillas.edu
Institución: Universidad Pontificia
Comillas.

Nombre: Susana Merchán Rubira
Correo Electrónico: susana.merchan1@upm.es
Institución: Universidad Politécnica de Madrid.