Interactive tools for Discrete Mathematics e-learning

CARMEN ESCRIBANO IGLESIAS
ANTONIO GIRALDO CARBAJO
MARÍA ASUNCIÓN SASTRE ROSA
Applied Mathematics Department – Computer Science Faculty - Technical University of Madrid
Campus de Montegancedo – Boadilla del Monte – 28660 Madrid - SPAIN
cescribano@fi.upm, agiraldo@fi.upm, masastre@fi.upm.es
http://www.dma.fi.upm.es/carmen, http://www.dma.fi.upm.es/antonio, http://www.dma.fi.upm.es/sonia

Abstract: - Education is a dynamical and complex area. Research in education increases year by year. This increase is an important factor in the development of new educational techniques. Nowadays, the information society in which we live needs wider educational spaces, and internet provides a powerful tool to introduce new educational technologies and to use online applications. Indeed, TICs (technologies for informatics and communication) provide a very positive aid to the learning tasks. Interactive tutorials allow access to a big amount of information in a multi-sequential way, by using specifically designed Java applets suitable for the learning of a specific knowledge. Due to these facts, the use of these tools has many advantages for learning mathematics. In this sense, we present here a hypertext with many interactive java applets, developed to show the main applications of Integer and Modular Arithmetic in a brief theoretical environment.

Key-Words: - Modular Arithmetic, Interactive Tutorials, Hypertext, Java Applets, World Wide Web, RSA Cryptosystem.

1 Introduction

In modern society computers provide access to an increasing number of sources of information. This dynamical and fast development of knowledge forces that high education needs training students to manage vast amounts of information. Internet and the computers programs offer not only the access to information but also give the users powerful capabilities for information manipulation and for the learning task.

This changing society requires an evolution out of the traditional ways of teaching. Moreover, the fast development of knowledge and technology reduces the life span of some concepts, while it increases the necessity of being able to revise and update the formation throughout the professional life. On the other hand, the development of technologies for informatics and communication provides a very positive aid to the learning tasks [4, 11, 14, 15].

One of the most common uses of technology in education appears in the form of learning interactive tools [3, 5, 6, 10]. These have great advantages over the traditional learning material (notes, books,…). The reading by exploration or navigation of a hypertext is multi-sequential and interactive. The reader makes visual sweepings and searches of fragments of interest. It is recommendable to use textual or graphical tools that appear in the screen and that allow the user to identify and to distinguish the contents in the hypertext. Navigation has replaced linear reading, the information is a space to travel, a path to explore.

In this sense, we present here a new interactive tool for the subject “Integer and Modular Arithmetic”[18]. Apart for reinforcing the concepts and techniques learnt at the classroom, we hope it may train the student in its necessary self-learning and use of technology, as well as in the search and management of information in the world wide web.

Designed as a hypertext, it includes several Java applets, to be used by teachers in the classroom lectures and by the students when learning by themselves. This hypertext summarizes the subject “Integer and Modular Arithmetic”, which is part of the syllabus of the course “Discrete Mathematics” [7, 13], taught in the first semester of Computer Science at the Technical University of Madrid.

The hypertext includes all the definitions, theorems and the most important results, along with some practical applications. For the latter, we have designed several interactive applets that allow the reader to experience a high degree of interactivity, offering him the freedom to generate his own examples. He may also use them as a revising tool, to review his homework. These applets are made using programming standards for the World Wide Web, like Java or JavaScript.

We have been working since many years ago, developing interactive tools to help the teacher to present and display, in an animated and interactive way, many mathematical notions and algorithms in the classroom. These tools can be also used by the students through the web page of the Department to experiment, with the contents of the various courses taught by us, in a virtual way.

2 Objectives

The main objective of this work is to develop interactive tools for the subject “Integer and Modular Arithmetic” to be used both by teachers on classroom lectures and by students when learning by themselves. As most mathematical subjects, this is difficult for students. To make it as friendly and attractive for students as possible, we have given special attention to the following properties of these tools:

- A graphical interface for the hypertext which can be easily handled by the user. It allows the visualization of the contents and the organization of the information in an immediate way through pull-down menus. One of our goals is that the different applications which are presented in the tutorial can be easily and quickly found within each section.
- Fast access to bibliography, books and numerous related web pages. This information points are indicated by the symbol

  📜

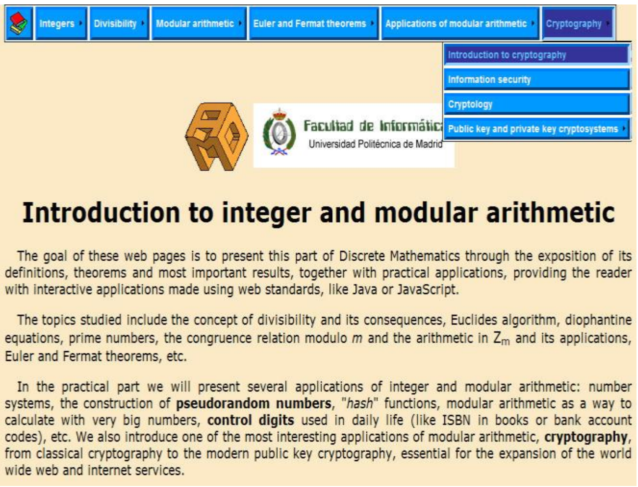
  to help the student to locate additional information and to manage information from the world wide web.
- Implementation of didactic applets for the most relevant algorithms of Integer and Modular Arithmetic, which have provided many important applications, most of them widely used nowadays. These applets are immersed in a theoretical framework in which the several notions and results are presented. Therefore, as we pretended, the user can interact with the tutorial, so that its use is more attractive and interesting.
- Inclusion, following this didactic direction, of historical references and anecdotes about some of the excellent mathematicians who helped to develop this subject. Those are referred in the hypertext with an icon.
- Accessibility from the web page of the department, as additional documentation for the course “Discrete Mathematics”. This is also integrated in a b-learning moodle context.
- Design of the applets using programming standards for the World Wide Web, to avoid incompatibilities.
- Facility to include new functionalities and algorithms in the future, if desired.

3 Description of the interactive tutorial

Modular Arithmetic, already well-known by the old Greek and Chinese mathematicians, has found its greatest applications in the second half of the 20th century, with the appearance of Computer Science. In particular, it has obtained a great relevance with the invention of public key crypto-systems.

This interactive tutorial focuses on its theoretical as well as on its practical aspects. Numerous examples are included, as well within the texts as in the form of interactive applications for the World Wide Web. These applications have been implemented using technologies characteristic of the Web, in the form of Java applets or as dynamical web pages using Javascript.

The following figure shows the page from which the reader can access the different sections that we describe next.


Integers
Divisibility
Modular arithmetic
Euler and Fermat theorems
Applications of modular arithmetic
Cryptography
Introduction to cryptography
Information security
Cryptology
Public key and private key cryptosystems
Facultad de Informática
Universidad Politécnica de Madrid

Introduction to integer and modular arithmetic

The goal of these web pages is to present this part of Discrete Mathematics through the exposition of its definitions, theorems and most important results, together with practical applications, providing the reader with interactive applications made using web standards, like Java or JavaScript.

The topics studied include the concept of divisibility and its consequences, Euclides algorithm, diophantine equations, prime numbers, the congruence relation modulo *m* and the arithmetic in Z_m and its applications, Euler and Fermat theorems, etc.

In the practical part we will present several applications of integer and modular arithmetic: number systems, the construction of **pseudorandom numbers**, "*hash*" functions, modular arithmetic as a way to calculate with very big numbers, **control digits** used in daily life (like ISBN in books or bank account codes), etc. We also introduce one of the most interesting applications of modular arithmetic, **cryptography**, from classical cryptography to the modern public key cryptography, essential for the expansion of the world wide web and internet services.

The tutorial is structured into the following pull-down menus.

- *Integers: Integers and their ordering – Induction principle.* This theoretical part begins with the basic notions about the integers and the induction principles. As an example, we prove, using the strong induction principle that a winner strategy for the Nim Game works.

- *Divisibility: Divisors and multiples - Numbers systems - Greatest common divisor - Diophantine equations - Prime numbers.* These theoretical notions are complemented with applications, in the form of applets, for changing the expression of numbers in decimal basis to other bases, to compute the greatest common divisor of two numbers using Euclid algorithm, or to find prime numbers in a given rank using the Sieve of Eratosthenes.

- *Modular arithmetic: Congruence relation – Arithmetic in Z_n – Operations in Z_n – Modular exponentation – Linear congruences – Systems of congruences.* Modular Arithmetic is introduced from the congruence relation, showing next the methods to solve linear congruence equations and congruence systems. All this is also supported by some applications like an applet that shows the most common operations in Modular Arithmetic, the fast modular exponentiation and an application to solve systems of congruence equations.

- *Euler and Fermat theorems: Units in Z_n - Euler and Fermat theorems.* In this section, the units of Z_m, Euler function and Euler theorem, and Fermat little theorem are briefly introduced. Primality tests and the usual methods to generate big prime numbers are also presented. A very interesting application of the notions studied so far is the cryptosystem RSA.

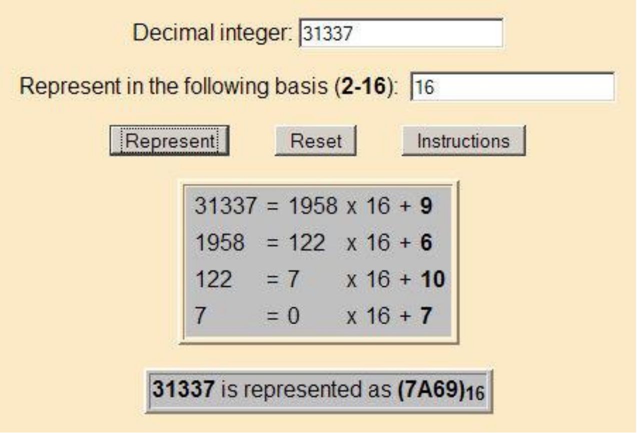
- *Applications of modular arithmetic: Arithmetic with big numbers – Random numbers – Hash tables – Control digits.* The tutorial shows several very important applications of the calculus with congruencies in Computer Science, like the Arithmetic with very great numbers, the hash tables used in programming when it is necessary to quickly find a data registry in a very great table, the simple generation of random numbers in a computer science system (that is deterministic by nature), or the control digits that are used in systems widely used in the daily life (the Spanish ID or DNI, the codes of client accounts in banks, or the ISBN, an identification code for printed books). An applet to generate pseudorandom numbers and another to verify control digits, are included here.

- *Cryptography: Introduction to cryptography – Information security – Cryptology – Public key and private key cryptosystems.* The last part of the tutorial is devoted to one of the most important applications of Modular Arithmetic nowadays: Cryptography [19, 21]. An historical introduction is included. Different cryptosystems, like Cesar coding or the coding by poly-alphabetical substitution are presented, along with their corresponding applets to practice coding with them. Finally, the most important public key cryptosystem, the RSA algorithm, is studied. This algorithm uses as coding and decoding transformation the operation of modular exponentiation. Its security is based in the computational complexity that supposes the factorization of the product of two big prime numbers.

We describe next some of the applets.

3.1 The application “change of basis"

This application, written in dynamic HTML with Javascript, shows how to convert a nonnegative integer from decimal basis to any other basis. Any basis between 2 (binary representation) and 16 (hexadecimal) can be chosen for the conversion. For the cases of basis greater than 10, the letters A to F are used, as usual, to represent the digits 10 to 15.



Decimal integer: 31337

Represent in the following basis (**2-16**): 16

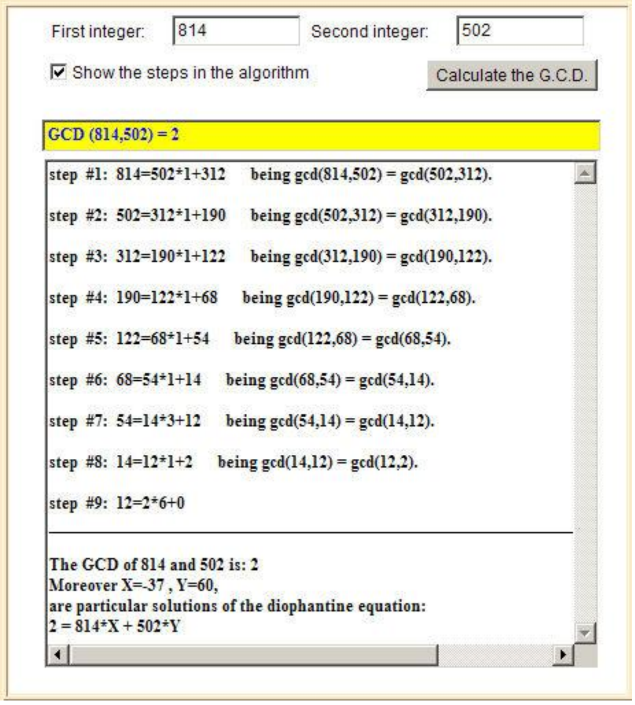
```
31337 = 1958 x 16 + 9
1958  = 122  x 16 + 6
122   = 7    x 16 + 10
7     = 0    x 16 + 7
```

31337 is represented as **(7A69)$_{16}$**

There are two text fields to enter the number in decimal basis and the new basis in which it is desired to express the number. Aside from both text fields, there are three buttons to indicate the desired action. The button “Represent” makes two text areas appear in the lower half of the user window. Those are the exits of the interface. The first area displays the process of conversion, and the second shows the final results, i.e., the representation of the input integer in the desired basis. The “Reset” button erase the contents of the text fields and the two output areas. The button “Instructions” opens a new navigator window with the instructions to use the program.

3.2 Euclid algorithm

This Java application shows the steps followed in Euclid algorithm to find the greatest common divisor (gcd) of two positive integers a y b. Moreover, the applet computes a solution for the Diophantine equation aX + bY = gcd (a,b)



First integer: 814 Second integer: 502

☑ Show the steps in the algorithm

GCD (814,502) = 2

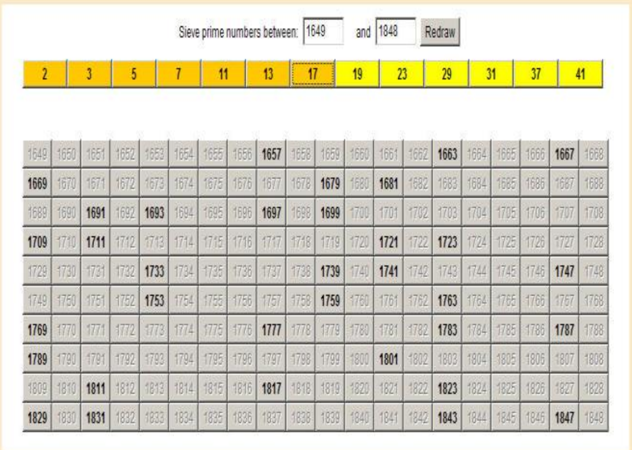
```
step #1: 814=502*1+312    being gcd(814,502) = gcd(502,312).
step #2: 502=312*1+190    being gcd(502,312) = gcd(312,190).
step #3: 312=190*1+122    being gcd(312,190) = gcd(190,122).
step #4: 190=122*1+68    being gcd(190,122) = gcd(122,68).
step #5: 122=68*1+54    being gcd(122,68) = gcd(68,54).
step #6: 68=54*1+14    being gcd(68,54) = gcd(54,14).
step #7: 54=14*3+12    being gcd(54,14) = gcd(14,12).
step #8: 14=12*1+2    being gcd(14,12) = gcd(12,2).
step #9: 12=2*6+0

The GCD of 814 and 502 is: 2
Moreover X=-37 , Y=60,
are particular solutions of the diophantine equation:
2 = 814*X + 502*Y
```

There are two text fields to enter the numbers whose greatest common divisor we want to compute and a box to indicate if the applet must show or not the different steps in the execution of the algorithm. There is an activation button to tell the applet to begin the execution of the algorithm from the entrances indicated in the text fields. Finally, there is an output text window to show the error messages or, if no error has been found in the input data, the different steps in the execution of the algorithm (if the corresponding box has been checked), the greatest common divisor of a and b, and the particular solution obtained for the diophantine equation aX+bY = gcd (a, b).

3.3 The Sieve of Eratosthenes

In order to illustrate the section dedicated to obtain prime numbers by means of the Sieve of Eratosthenes, two applets have been made. The second one allows to look for (by means of the Sieve of Eratosthenes) all the prime numbers in a prescribed interval of integers (the maximum interval size is 500, for reasons of spatial representation in the screen) contained in [101, 9999].

The applet interface is as follows. The text windows to input the end points of the interval where to look for prime numbers are in the upper part of the panel. In the following line there is a line of buttons corresponding to all prime numbers lower or equal than the square root of the upper end of the interval. Initially, all these buttons are active (yellow). When one of these buttons is pressed by the user, that button passes to a inactive state (orange) and all their multiples disappear from the table, as if they had been "sieved".



Sieve prime numbers between: 1649 and 1848

2	3	5	7	11	13	17	19	23	29	31	37	41

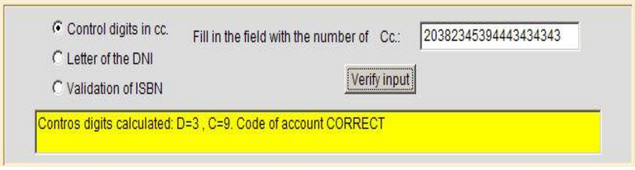
1649	1650	1651	1652	1653	1654	1655	1656	**1657**	1658	1659	1660	1661	1662	**1663**	1664	1665	1666	**1667**	1668
1669	1670	1671	1672	1673	1674	1675	1676	1677	1678	**1679**	1680	**1681**	1682	1683	1684	1685	1686	1687	1688
1689	1690	**1691**	1692	**1693**	1694	1695	1696	**1697**	1698	**1699**	1700	1701	1702	1703	1704	1705	1706	1707	1708
1709	1710	**1711**	1712	1713	1714	1715	1716	1717	1718	1719	1720	**1721**	1722	**1723**	1724	1725	1726	1727	1728
1729	1730	1731	1732	**1733**	1734	1735	1736	1737	1738	**1739**	1740	**1741**	1742	1743	1744	1745	1746	**1747**	1748
1749	1750	1751	1752	**1753**	1754	1755	1756	1757	1758	**1759**	1760	1761	1762	**1763**	1764	1765	1766	1767	1768
1769	1770	1771	1772	1773	1774	1775	1776	**1777**	1778	1779	1780	1781	1782	**1783**	1784	1785	1786	**1787**	1788
1789	1790	1791	1792	1793	1794	1795	1796	1797	1798	1799	1800	**1801**	1802	1803	1804	1805	1806	1807	1808
1809	1810	**1811**	1812	1813	1814	1815	1816	**1817**	1818	1819	1820	1821	1822	**1823**	1824	1825	1826	1827	1828
1829	1830	**1831**	1832	1833	1834	1835	1836	1837	1838	1839	1840	1841	1842	**1843**	1844	1845	1846	**1847**	1848

3.4 Modular Arithmetic

This section consists on two applets designed to show how to do the more common operations in Modular Arithmetic. The user must choose a number between 2 and 31 and one of the four operations: addition, difference, multiplication and division. The second applet shows how to make the exponentiation in an easy way.

3.5 Control Digits

This is a simple applet showing how the control digits in a number of account in a bank, the DNI or the ISBN work.



● Control digits in cc.
○ Letter of the DNI
○ Validation of ISBN

Fill in the field with the number of Cc.: 20382345394443434343

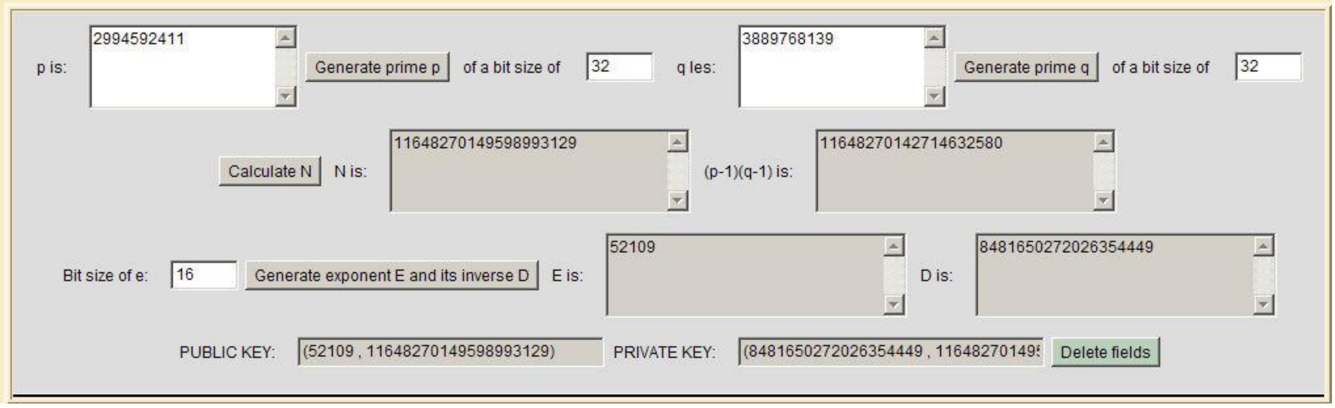
Contros digits calculated: D=3 , C=9. Code of account CORRECT

3.6 The cryptosystem RSA

This applet allows to encrypt or to sign a short text message using the algorithm RSA. The applet is divided in three areas:

Area 1 – Generation of the pair of keys RSA

First, the pair of keys (public and private) for the user has to be generated. For this, the applet asks for a pair of prime numbers p and q. The application itself can generate these two prime numbers. Then, the values of the module n=p·q and of the public exponent E, which is generated randomly by the applet with the



p is: 2994592411 of a bit size of 32

q les: 3889768139 of a bit size of 32

N is: 11648270149598993129

(p-1)(q-1) is: 11648270142714632580

Bit size of e: 16

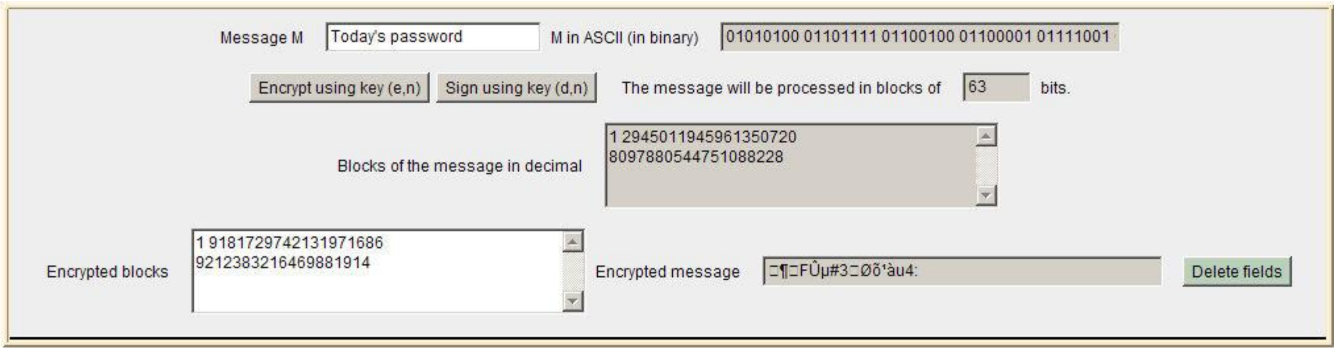
E is: 52109

D is: 8481650272026354449

PUBLIC KEY: (52109 , 11648270149598993129)

PRIVATE KEY: (8481650272026354449 , 11648270149!

Area 1 of RSA applet – Generation of the pair of keys



Message M: Today's password

M in ASCII (in binary): 01010100 01101111 01100100 01100001 01111001

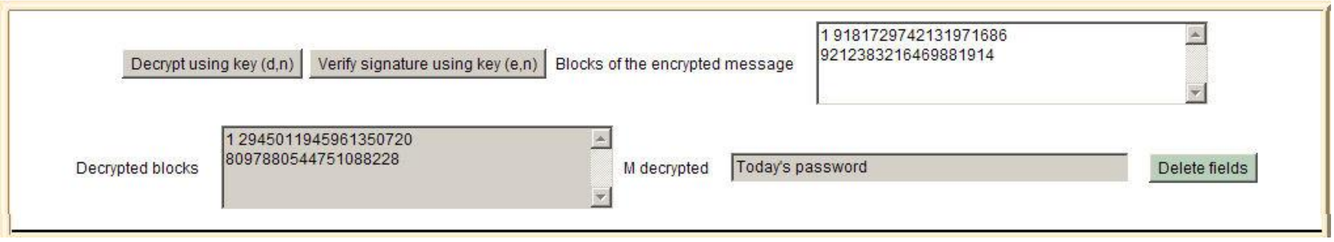
The message will be processed in blocks of 63 bits.

Blocks of the message in decimal:
1 2945011945961350720
8097880544751088228

Encrypted blocks:
1 9181729742131971686
9212383216469881914

Encrypted message: □¶□FÛµ#3□Øõ'àu4:

Area 2 of RSA applet – Encrypting and signing the message



Blocks of the encrypted message:
1 9181729742131971686
9212383216469881914

Decrypted blocks:
1 2945011945961350720
8097880544751088228

M decrypted: Today's password

Area 3 of RSA applet – Decrypting the message and verifying signature

size in bits indicated by the user, are computed. The value of the exponent D is calculated automatically by the applet. These values determine the public key (E,n) and the private key (D,n) with which the user can encrypt/decrypt and sign messages.

Area 2 – Encrypting and signing the message

The message is written in the designed text field and then the “encrypt” button has to be pressed. If the text is very long it will be encrypted by blocks.

Area 3 – Decrypting the message and signature verification

Here the inverse process of the previous step is made.

The numbers corresponding to the presumed encrypted message or to the presumed signature are introduced, and the modular exponentiation of the RSA algorithm is repeated using this time as exponent the private key (for decrypting) or the public key (for verifying the signature). In a real case, the verification of our signature would not be made by us, but by the receiver of the resume of our signed message, who would verify it using our public key.

4 Conclusions and future work

Although there are many studies comparing the effectiveness of online learning and of face-to-face learning, researchers haven’t demonstrated any significant difference. There are a great number of studies that have proved no significant differences between exam results of online students and those of face-to-face students [2], [9], [16]. However, there are cases in which online learning is reported to be more effective than face-to-face learning [8], while some research findings revealed that face-to-face learning is more effective than online learning [1]. These make us think that the best option is to use graphical and interactive tools in two ways. On one hand, these tools help the teacher in the classroom, while on the other hand, the students can work and experiment with them making their own examples, out the classroom.

The didactical benefits of this interactive tutorial for Modular Arithmetic, according to our experience in teaching these mathematical concepts, are:

- It helps the student to learn the subject.
- It helps the teachers in their lectures by navigating through the examples and the applications implemented along the hypertext.
- They offer the student the opportunity to experiment, increasing interactivity.

In general, interactive tutorials including Java applets are very good aids for learning mathematics, as they improve comprehension, engagement, memorization and the satisfaction of the students, as well as the interest and motivation amongst pupils when the teacher makes use of them.

Finally, as a future work, we continue developing interactive tutorials in different areas of Mathematics related to Computer Science (we have already made tutorials for some parts of Discrete Mathematics, Infinitesimal Calculus, Dynamical Systems, Fractal Geometry, Image Processing, …). Moreover, we are including some of them in the worldwide Open Courseware Consortium [20] (we have begun with Dynamical Systems and intend to progressively include the rest of the subjects). We intend also to elaborate interactive books.

References:

[1] B.W.Brown, C.E.Liedholm, *Can Web Course Replace The Classroom In Principles of Microeconomics?*, American Economics Review, Vol. 92, No.2, 2002, pp. 444-448.

[2] R.Carlisle, *A Four Year Study Comparing English Classes Online, Via Television, And Face-to-Face*, California State University, 2002.

[3] A.Dastfan, *Implementation and Assessment of Interactive Power Electronics Course*, WSEAS Transactions On Advances In Engineering Education, Vol.4, No 8, 2007, pp. 166-171.

[4] S.Encheva, S. Tumin, *Multimedia Factors Facilitating Learning*, WSEAS Transactions On Advances in Engineering Education, Vol. 4, No. 10, 2007, pp. 203-209.

[5] C.Escribano, M.Domingo, A.Giraldo, M.A.Sastre, *Interactive tools for Calculus e-learning*,. Proceedings of the 6th WSEAS International Conference on E-Activities, Tenerife, Spain, December 2007.

[6] R. Gonçalves, M. R. Rio de Pinho, J. Borges, *An Applet for Optimal Control Problems*, Proceedings of the 4th WSEAS/IASME International Conference on Engineering Education, Crete, Greece, July 2007.

[7] A.Giraldo, *Aritmética Entera y Modular*, http://www.dma.fi.upm.es/docencia/cursosanteriores/06-07/primerciclo/matdiscreta/12M-1/TeoriaAritmetica.pdf.

[8] J.L.Johnson, *Distance Education: The Complete Guide to Design, Delivery and Improvement*, Teachers College Pres, 2003.

[9] R.Leassure, L.Davis, S.Thievon, *Comparison Of Student Outcomes And Preferences In Traditional Vs World Wide Web-based Baccalaureate Nursing Research Course*, Journal of Nursing Education, Vol. 39, No. 4, 2001, pp. 149-154.

[10] E. Milková, *What can Multimedia add to Optimization of student' study habits?*, Proceedings of the 6Th WSEAS International Conference on Educational Technology, Venice, Italy, November 2007.

[11] T.L.Naps, G.Rößling, et al, *Exploring the Role of Visualization and Engagement in Computer Science Education.* Inroads - Paving the Way Towards Excellence in Computing Education. 35, 131-152, ACM Press, 2003.

[12] J.C.Orós, *Diseño de páginas Web interactivas con JavaScript*. RA-MA 1999.

[13] K.H.Rosen, *Discrete Mathematics and its Applications*, Mac Graw-Hill, 2007.

[14] M.G.Sánchez, M.A.Sastre, V.Giménez, C.Escribano, *Pedagogical impact of Interactive Tutorials in Visualization and Learning of Mathematical Concepts in Computer Science Curricula*,. Proceedings Conference on Informatics Education in Europe, Montpellier, November 2006.

[15] M.G.Sánchez, M.A.Sastre, V.Giménez, C.Escribano, *Visualization on Learning Mathematics Concepts for Engineering Education*, Proceedings of the 4th WSEAS / IASME International Conference on Engineering Education (EE'07), Crete, Greece, July 2007.

[16] S.Street, A.Goodman, *Some experimental Evidence on the Educational Value of Interactive Java Applets in Web-based Tutorials*, Proceedings of the 3rd Australasian Conference on Computer Science Education, ACM, 94-100, 1998.

[17] C.Wills, M.Stommel, M.Simmons, Implementing A Completely Web-based Nursing Research Course, Journal of Nursing Education, Vol. 40, No. 8, 2001, pp. 359-362.

[18] *Introducción a la aritmética entera y modular*, http://www.dma.fi.upm.es/java/matematicadiscreta/aritmeticamodular/. (English version: *Introduction to integer and modular arithmetic*, http://www.dma.fi.upm.es/java/matematicadiscreta/modulararithmetic/index.html.)

[19] *Crypto FAQ of RSA Laboratories* http://www.rsasecurity.com/rsalabs/node.asp?id=2152.

[20] *Open Courseware Consortium*, http://www.ocwconsortium.org/.

[21] *Revista independiente on-line sobre privacidad y seguridad en Internet*, http://www.kriptopolis.com.