Advance Access Published on 2 June 2006 doi:10.1093/teamat/hrl008

A cryptological way of teaching mathematics

Pino Caballero-Gil and Carlos Bruno-Castañeda

Submitted July 2005; *accepted* February 2006

Abstract

This work addresses the subject of mathematics education at secondary schools from a current and stimulating point of view intimately related to computational science. Cryptology is a captivating way of introducing into the classroom different mathematical subjects such as functions, matrices, modular arithmetic, combinatorics, equations, statistics and proofs, which usually are recognized as difficult for many students. Special attention is paid here to the concepts of proof and verification through the definition of zero-knowledge cryptographic protocols. Many other different cryptographic and cryptanalytic activities (building and breaking ciphers, respectively) and modern cryptographic applications such as secret-sharing protocols are also proposed as resources for motivating mathematics learning and for achieving a significant improvement in student understanding of several algebraic, analytical and statistical concepts.

1. Introduction

The two main objectives of this work are the enrichment of mathematics curricula and the popularization of mathematics among students. Cryptology is a common branch of mathematics and computational science, which is fairly well-known in the mathematics community as an excellent vehicle to introduce several fundamental mathematical concepts and to make their understanding easier to the students, (1).

One of the starting point ideas of this work is that the abilities required for this increasingly computerized world are essentially mathematical. So, computational science is viewed here as a great opportunity to state mathematics learning as accessible, colourful and interactive through cryptological concepts. Cryptology contains motivating and intriguing elements that may be used to promote problem-solving skills with collaborative work in groups. For example, suspense and espionage make cryptology be perceived by the students as an exciting game of defending their own groups' secrets while they try to break the other groups' secrets. If after many hours they finally develop a method to break a cipher, then they will be more likely to appreciate the power and beauty of mathematics. With complex ciphers and applications, a distinct pedagogical approach may be used: the teacher could first present the mystery and then show how mathematics can help to solve it. So, in both cases students take the learning task with enthusiasm. However, although stated as a game, it is interesting to remark the importance of cryptology in our Internet-based society because it offers a wonderful opportunity to students for

identifying the mathematics they are learning as applicable to the real world. So, through cryptology, students enjoy mathematics lessons and at the same time see the need for it in life (2).

Cryptography has a long and rich history with many interesting cipher schemes (3,4). Our experiences in computer science and discrete mathematics education through cryptology have shown us that the use of real-life examples usually receives positive feedback especially if it is integrated in an interdisciplinary project. For example, there are many historical examples of cryptography that make it possible to delve into different mathematical topics while learning history. Furthermore, many illustrations of the use of encryption from ancient times till the present have been documented on television, books and movies, and so the teacher may use some of these tools for the concepts being conveyed in the class. One of the most popular examples in films and books is from the Second World War: the Nazi Enigma machine and how the British and Polish mathematicians' efforts were useful to break it.

The teacher preparing mathematical lessons through cryptology has to answer two major questions: what to teach and how to teach it (5). In order to answer the first question, two factors the teacher has to take into account are the preliminary mathematical knowledge of the students and whether the class is homogeneous or not. On the other hand, since the range of numbers that can be computationally handled is finite, modular arithmetic is present at most cryptologic applications, so the most suitable mathematics to teach through cryptology is finite mathematics (6). After establishing the contents of the course, another serious problem arises: how to present the selected topics. A fine solution may be to orient the course, starting from the introduction of historical or current cryptologic examples and ending with the mathematics and computer science concepts on which they are based. Furthermore, the introduction of some simple cryptographic ideas may be effectively done by employing physical objects such as crayons, playing cards, coins or dice, which can help to make mathematics a more entertaining subject matter. For instance, crayons and coins are useful for introducing zero-knowledge proofs, playing cards may be used for defining some cryptographic protocols such as mental poker and dice are a fundamental tool for describing stream ciphers.

Regarding the role of computers in mathematics and computational science education, since many of the core ideas may be introduced without machines, we think that there are benefits and dangers in the emphasis on using computers (7). On the one hand, in this Internet era blackboard and chalk are no longer the only learning methods usually available to teachers and students, so it is natural to use such technology in the classroom. On the other hand, computers are an expensive learning tool, which usually accentuates the division between poor and rich schools. An advisable way to find a balance between both points of view consists of introducing ciphers and cryptologic applications in the classroom without computers, and then to use computational tools like spreadsheets as invaluable complements to mathematics courses. So, in the introduction the teacher should take much care to keep numbers to such a level that students can handle them with the only help of calculators. Afterwards, the educator should show students how easily computations with larger numbers become very difficult without computers, which might even be used to introduce the idea of computational complexity. Finally, teachers can use the Internet as a source of teaching tools where they may exchange complex cryptologic implementations.

2. Functions and statistics through substitution

Functions are used as the basis of cryptography for encryption. It is easy to see that, for each plain letter (element of the domain), only one ciphered letter (element of the range) should exist in the deterministic and practical notion of encryption (Fig. 1). Furthermore, for enabling the

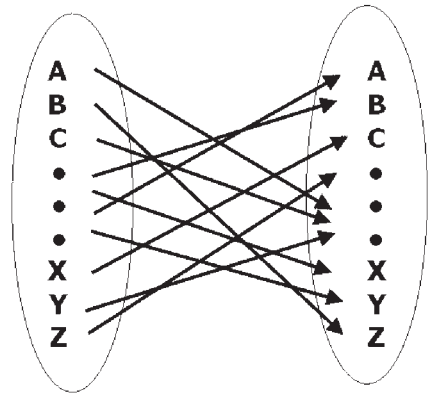

Fig. 1. Encryption vs. function.

unique decryption, the encryption transformation should be one-to-one in order to be invertible. So, from the introduction of an easy cipher like Caesar substitution, not only several basic analytical definitions of function, domain and range, and properties such as being one-to-one, onto, invertible or linear come up naturally, but also a basic knowledge on modular arithmetic is fundamental.

A substitution is a simple cipher whose key is based on a permutation of the alphabet. Those substitutions that use only the permutation of one alphabet (like Caesar cipher) are called monoalphabetic and are vulnerable to frequency analysis with letter counting, whereas polyalphabetic substitutions (like Vigenere cipher, Fig. 2), which use more than one permutation, are a bit safer because their cryptanalysis implies more work.

In order to involve pupils in the lessons on substitutions, they may construct their own ciphering devices like rotating wheels (Fig. 3) and sliding rules. The cryptanalysis of the substitution known as affine cipher is possible through coding the alphabet with decimal numbers, using frecuency counts and solving simple linear equations. The affine cipher may be described by the formula $C = aM + b$ (*mod* 26), where M and C denote the numerical coding of the plain and ciphered letters, respectively, and a and b are two integers such that $0 \leq a$, $b \leq 25$ and a and 26 are relatively primes.

Example of affine cipher:

Ciphered message: JQAXQDEJQ

Numerical coding: J = 9, Q = 16, A = 0, X = 23, D = 3, E = 4

Frecuencies: Q:3, J:2, A:1, X:1, D:1, E:1

English highest-frecuency letters: E = 4, T = 19, A = 0, O = 14, I = 8, N = 13

Linear equations: $a4 + b = 16$ (*mod* 26) and $a19 + b = 9$ (*mod* 26)

Solutions: $a = 19 \times 15 - 1 = 19 \times 7 = 133 = 3$ (*mod* 26) and $b = 16 - 12 = 4$

At this point it is natural to jump to the asymptotic version of the polyalphabetic cipher, the so-called one-time pad, where the key is a totally random binary sequence that is as long as the binary message sent (Fig. 4). It is interesting to remark that although one-time pad is the unique cipher that has been shown to be theoretically unbreakable since the cryptanalyst can do no

K	E	Y	K	E	Y	K	E	Y
M	E	S	S	A	G	E		
W	J	R						

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fig. 2. Vigenere cipher.

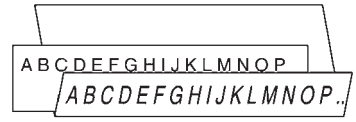

Fig. 3. Sliding rule.

better than guess at the plain text being a binary string, it is not practical because the key's length equals the secret message's length.

Consequently, the topic of substitution may be used to teach and consolidate statistical notions such as percentages, histograms, testing and randomness. Also, the number of keys available in a monoalphabetic substitution cipher (resulting from all the possible permutations of the alphabet) is a nice way to bring in factorials. On the other hand, it is also possible to introduce matrix manipulation through substitution ciphers. For instance, basic arithmetic matrix operations such as addition and subtraction may be used to define Hill substitution and its natural generalization to polynomial ciphers. While affine ciphers operate on letters, Hill cipher may be seen as its generalization to groups of letters, that is to say, the same formula $C = aM + b$ (*mod* 26) is applicable where M, C and b are integer columns and a is an integer matrix.

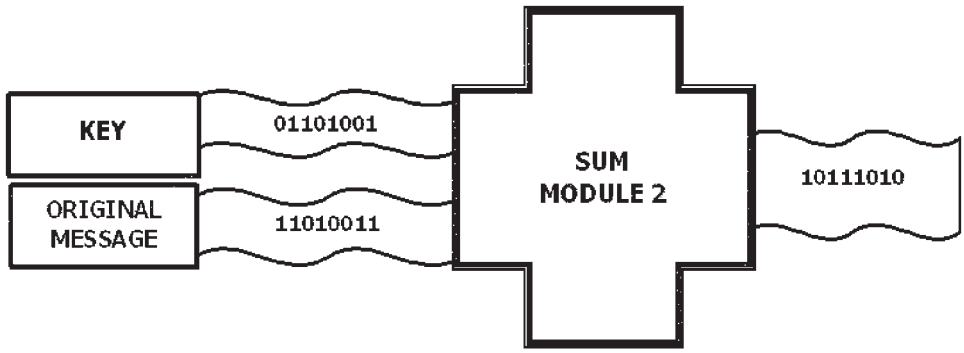

Fig. 4. One-time pad.

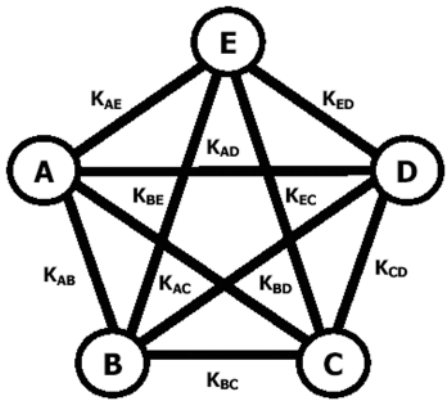

Fig. 5. Secret key management.

Example of Hill cipher:

In order to discover the key for the case $b = 0$ and with 2×2 matrices, once a corresponding pair of ciphered and original message is known, the student computes the inverse and multiplications of matrices:

Ciphered message: P = 15, Q = 16, C = 2, F = 5, K = 10, U = 20

Original message: F = 5, R = 17, I = 8, D = 3, A = 0, Y = 24

$$a = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 8 & 3 \end{pmatrix}$$

Solutions: $a = 19 \times 15 - 1 = 19 \times 7 = 133 = 3$ (*mod* 26) and $b = 16\text{-}12 = 4$

Finally, substitutions are part of composed ciphers extensively used in commercial cryptography such as block ciphers Data Encryption Standard (DES) and Rijndael, which may be used to define the composition of functions. In order to close the theme of classical cryptography, it is advisable to remark that its major disadvantage is key management because the number of secret shared keys increases with the number of users (Fig. 5). This problem becomes more evident

when considering a large network where any two users wish to communicate. So, this subject may be introduced in order to practice with combinatorics and also for mentioning the issue of communications complexity and security.

3. Primes, vectors and curves through public-key

The concept of public-key ciphers may be introduced in a mathematics lesson by means of a real-life analogy one-way streets, where it is easy to go from a point P to another point Q, and is practically impossible to go from Q to P (Fig. 6) (8). So, the public-key cipher may be viewed as the direction from P to Q because, although you are able to go in this direction, this does not enable you to go in the opposite direction, i.e. to decipher. This is a good example of the idea of one-way function, which forms the basis of public-key cryptography. In order to make it possible, in any public-key environment each user i should have a public encryption key e_i and the corresponding private decryption key d_i (Fig. 7).

After explaining that no good algorithm exists for solving a concrete difficult problem like factorization, one can show that there is, however, a simple algorithm for 'going backwards', i.e. starting with a solution and constructing a difficult instance of the problem around it. Such a one-way function constitutes the foundation of the best-known public-key cipher, the RSA (the letters stand for the names of the inventors: Rivest, Shamir and Adleman). This cipher can be easily introduced after having taught how to reduce numbers modulo a positive integer in substitution lessons. RSA may be described as follows. Each user Alice has a public key (n_A, e_A) consisting of a composite number $n_A = p_A q_A$ (where p_A and q_A are primes) and an encryption exponent e_A. The security of the system is based on the secret factorization of n_A. The corresponding decipher key d_A should satisfy the modular equation $e_A d_A = 1 \ (mod \ (p_A - 1)(q_A - 1))$, which is easily computed with the Euclidean algorithm. To cipher a message M, a user Alice should raise it to the power e_B, reduce modulo n_B and send the result to Bob, who should decipher it by raising it to the power d_B and reducing modulo n_B (Fig. 8). So, the RSA cipher is an excellent opportunity for students to discover the usefulness of primes.

As a side excursion, it is possible to explain digital signatures based on the RSA cipher, which gives the chance to recall the commutative property through a widely used real application because such a property guarantees that the decryption of the encryption coincides with the encryption of the decryption. Digital signatures also allow the introduction of a specific kind of one-way function called hash. A hash function is a map h from a very long input M to a much shorter output $h(M)$ such that it is not feasible to find two different inputs M and M' such that

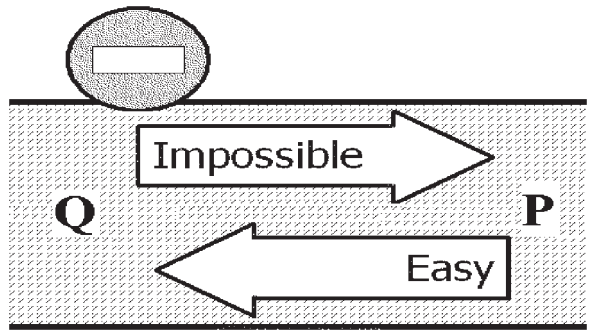

Fig. 6. One-way function.

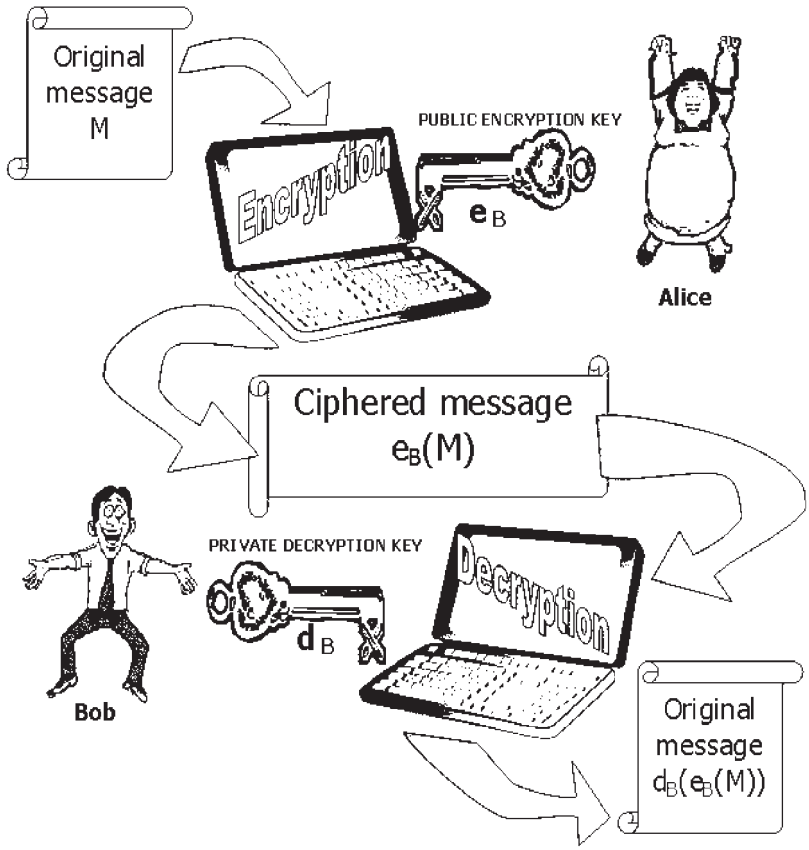

Fig. 7. Public-key cryptography.

$h(M) = h(M')$. Having introduced hash functions, the teacher may describe practical RSA digital signatures. After sending to Bob the message M, Alice signs it in the following way: first she hashes it using the public hash function h, then she raises $h(M)$ to the power d_A, reduces modulo n_A and sends the result $DS(M)$ to Bob. After receiving the messages M and $DS(M)$, Bob computes $h(M)$, raises $DS(M)$ to the power e_A and reduces modulo n_A. If this last result agrees with $h(M)$, then he knows that Alice must in fact have sent him the message M because nobody else could have generated a suitable M and $DS(M)$.

A simple public-key cipher based on the knapsack problem may be used with students to practice with volume estimations and vector multiplications. Intuitively, the knapsack problem consists in filling completely a knapsack of a concrete volume with some items from a set with different volumes. Such a problem is another fine example of a one-way function because it is easy to choose several concrete items to define a knapsack, but on the other hand, from this knapsack value, in general, it is difficult to recover the concrete volumes of the original used items. In spite of its general difficulty, there exists a very easy instance of the knapsack problem, the so-called superincreasing knapsack, consisting of an ordered vector of item volumes such that each volume exceeds the sum of the preceding volumes. Such a knapsack may be easily solved by the principle of 'the biggest item first'. In the knapsack cipher, Alice should choose as her private key $d_A = (w_A, K_A)$, where w_A is an integer and K_A is a superincreasing knapsack vector.

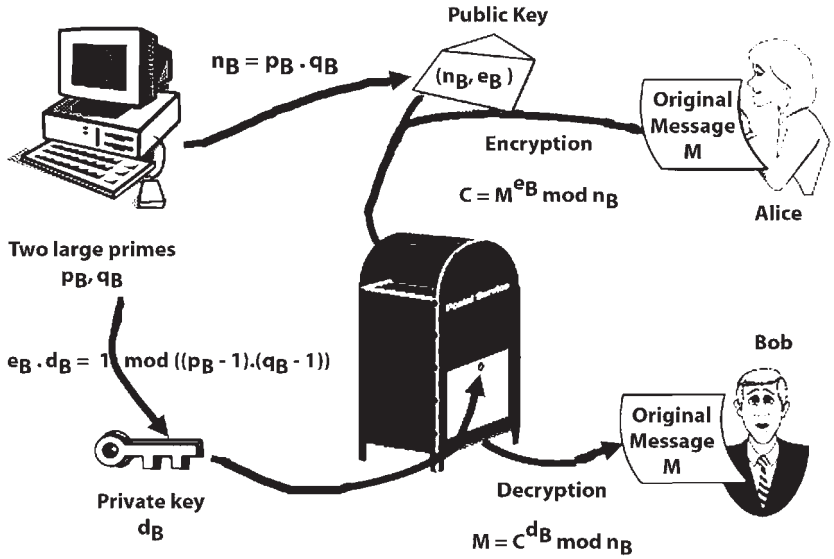

Fig. 8. RSA.

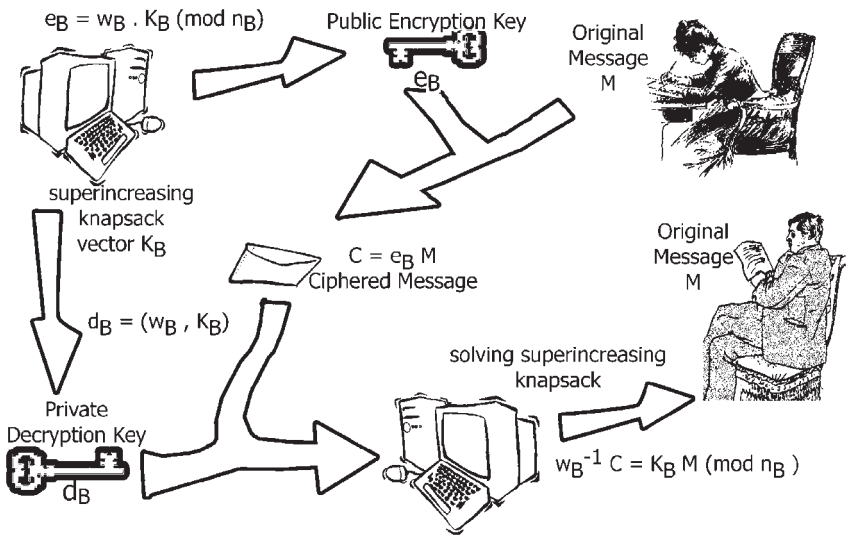

Fig. 9. Knapsack cipher.

Another integer n_A with no common factors with w_A should then be chosen by Alice. Then Alice states her public key c_A by means of the reduction modulo n_A of the vector produced by the multiplication $w_A K_A$. Such a public key constitutes a difficult instance of the knapsack problem, so nobody but Alice could obtain the secret key from the public key. In order to cipher a message, Alice should first encode it into bits and divide the result into binary vectors M whose lengths coincide with that of e_B. Once done, the cipher of every vector M is the vector multiplication $e_B M$, and its decipher is only possible for Alice, who can obtain w_B^{-1} modulo n_B and consequently solve the superincreasing knapsack resulting from the multiplication $w_B^{-1} e_B^M$ (Fig. 9).

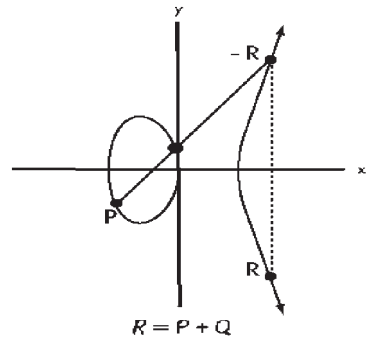

Fig. 10. Elliptic curve.

Although knapsack ciphers offer an opportunity to practice with vector multiplication, note that they have been already broken and so have no usefulness in real-life cryptography.

Example of knapsack cipher:

$K_B = (1, 2, 5, 9)$, $w_B = 7$, $e_B = 7(1, 2, 5, 9) = (7, 14, 15, 3)$ (*mod* 20)

Original message: $\mathrm{M} = 13 = 8 + 4 + 1 = (1101)$

Ciphered message: $\mathrm{C} = (7, 14, 15, 3)(1, 1, 0, 1) = 7 + 14 + 3 = 24$

Deciphered message: Solution of the superincreasing knapsack with K_B and $w_B^{-1}C = 3 \times 24 = 12$ (*mod* 20) obtaining $1 + 2 + 9 = (1101) = 13 = \mathrm{M}$

More reliable public-key ciphers are those based on elliptic curves over finite fields. The simplest elliptic curve E: $y^2 = x^3 - x$, whose graph is easily represented, can be used to introduce the basic notions of elliptic ciphers. So, after having taught curves representation, a brief definition of the addition of two points (Fig. 10) is necessary to introduce an elliptic cipher, whose description is as follows. Alice's public key is the point $d_A S$, where S is a public point of the curve E and d_A is a secret random integer, and each message is encoded into a point M of E. In order to cipher M, Alice should choose a random integer k_A and send to Bob the point $(k_A S, M + k_A(d_B S))$. So, in order to decipher, Bob should multiply the first coordinate of the received point by her private key d_B and subtract the result to the second coordinate. Note that in this case the teaching procedure should be different from the previous proposals because the educator should begin with the mathematical subject of curve representation before introducing one of the most promising ciphers through the previous simple example.

4. Randomness, proofs and equations through protocols

As mentioned before, a major problem in secret-key cryptography is key management. In order to solve it, two users may exchange public information to agree upon a random binary sequence that can be used as a shared secret key. One nice way of doing it is based on simple coin flipping, and bit commitment protocols based on the idea of bets on 'heads' or 'tails' may be introduced, which furthermore gives the opportunity to discuss topics like randomness. Coin-flipping protocols are used by two users to generate a common random binary sequence where A winning may be interpreted as '0', and B winning as '1'. On the other hand, a bit commitment protocol is a procedure that allows a user like Alice to put a secret inside an envelope in such a way that she cannot modify the secret after closing it and nobody can read the secret until she opens it.

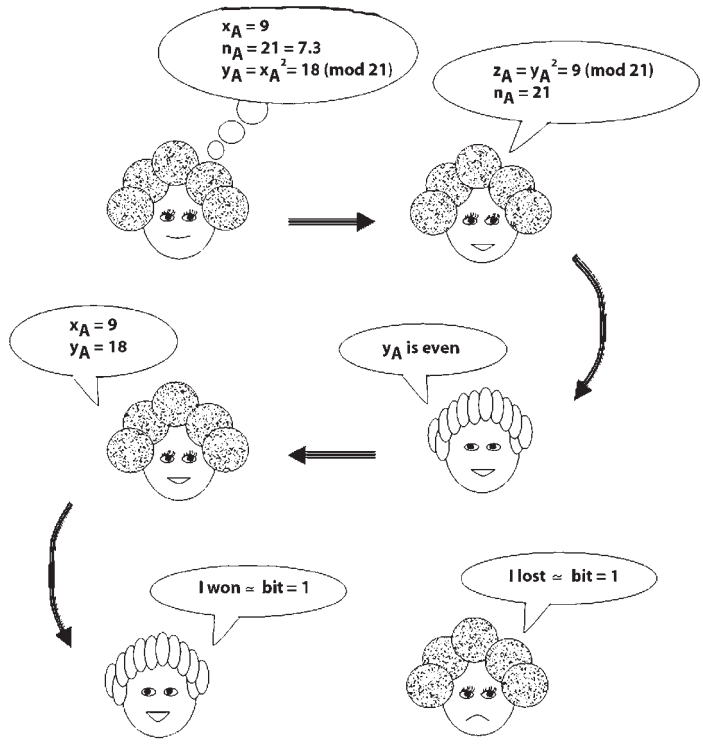

Fig. 11. Coin flipping.

It is possible to define through the following example a coin-flipping scheme based on one-way functions, that allow to experience with modular arithmetic and parity of numbers. In this proposal it is supposed that previously the users Alice and Bob agree on a one-way function f from X to Y, where X is a finite set of integers that contains the same quantity of odd and even numbers. So, the algorithm is defined as follows. First, Alice chooses a random element x in X, and sends $y = f(x)$ to Bob. Then, Bob bets publicly that x is even or odd, and Alice tells him whether his bet is correct or not, proving it to him by discovering x. Finally, Bob checks that $f(x) = y$. Note that if f is not adequately chosen, then it is possible that Alice cheats and knows two values x and x' of different parity, such that $f(x) = f(x')$. In a concrete version of this protocol, f might be a quadratic residual, and so Bob should have to decide whether its square root is even or odd (Fig. 11).

Various other cryptographic applications such as oblivious transfer and some multiparty protocols can be demonstrated by means of familiar physical objects such as playing cards because they have several convenient properties like randomness, uniqueness and indistinguishability. In an oblivious transfer, Alice wants to transfer a secret to Bob in such a way that it is transferred with a probability 1/2, and in the end Bob knows whether he got the secret but Alice does not. An example of this esoteric protocol, which may be introduced in order to work with the Euclidean algorithm, is the following one where the information to transfer is the factoring of a product of two primes. In such a protocol, first Alice chooses at random two primes p_A and q_A and sends to Bob the product $n_A = p_A q_A$. After that, Bob chooses a random number x with no common factors with n_A, reduces x^2 modulo n_A and sends the result to Alice, who can compute its

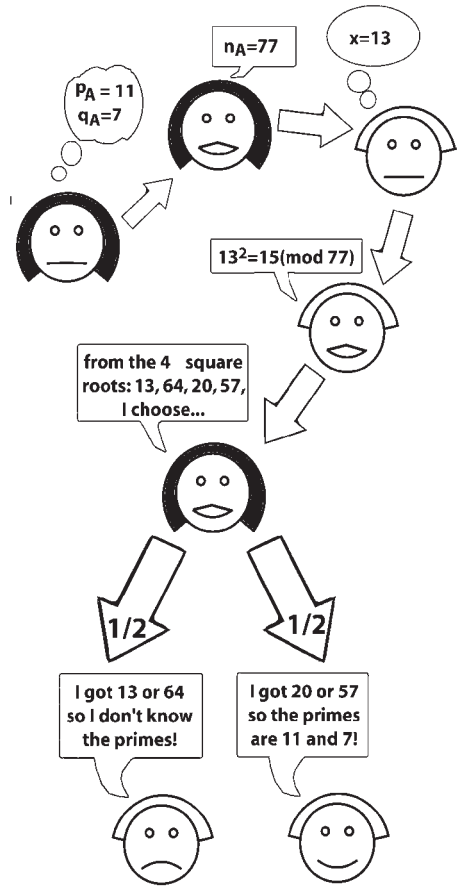

Fig. 12. Oblivious transfer.

four different square roots that are $x, n_A - x, y$ and $n_A - y$, thanks to her knowledge of p_A and q_A. So, Alice chooses one of them at random and sends it to Bob. If he receives y or $n_A - y$, then he can compute p_A and q_A thanks to the greater common divisor of $x + y$ and n_A, i.e. p_A or q_A. If, on the contrary, he receives x or $n_A - x$, then he cannot calculate them (Fig. 12). In the end, Alice does not know whether Bob received her primes or not, a fact that is usually very intriguing for students.

The last two-party protocol that will be mentioned in this work is specially important to the concept of proofs, a subject that is usually recognized as one of the most difficult for students. There have recently been several interesting developments in mathematical practice in the area of proofs and verification that have provoked an active reconsideration of those basic issues related to mathematical proofs. So, cryptology offers a way of producing short proofs of theorems such that everybody can be convinced that the theorem is true, yet obtain no information about the proof itself. These so-called zero-knowledge proofs are a new type of proof that has little in common with its traditional form, and that has become one of the most intriguing and intensively studied concepts in cryptographic theory. A zero-knowledge proof can be defined as an interactive cryptographic protocol involving two parties, a prover Alice and a verifier Bob,

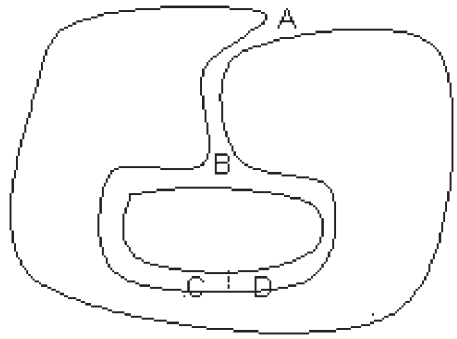

Fig. 13. Zero-knowledge cave.

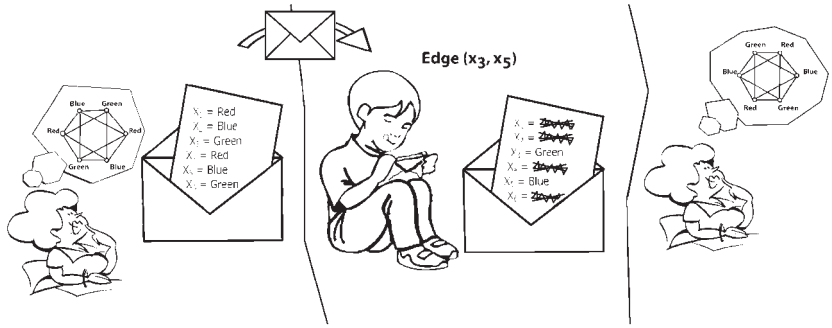

Fig. 14. 3-colouring zero-knowledge.

which enables her to provide him with convincing evidence that a traditional proof of a theorem exists without disclosing any information about the proof itself (9). While, as a result of such an interaction, Bob is convinced that the theorem in question is true, he has no knowledge of the proof and thus cannot convince others.

Zero-knowledge proofs may be carried out with or without a computer (10). In both cases there are several simple examples that may be used to introduce this interesting concept to the class, such as a game based on a cave, a graph three-colouring or a 'Where's Wally?' challenge. Firstly, in (11) the authors show how in the 'strange cave of Ali Baba' Bob could verify a claim of knowing the password to open the door without the secret being revealed. The cave had two passageways (Fig. 13), and only Alice, who knows the password, might enter one passageway, unlock the door and emerge from the other passageway. Bob would ask Alice to go down either of the passageways (he would not know which). Then Bob would ask Alice to emerge from one of the two passageways picked at random. He would know that, if she did not possess the password, then with a probability 1/2 she could not do this. So after a large number of repetitions, in all of which Alice passes the test, Bob can be certain with a small probability that she does in fact have the password.

The second example of zero-knowledge proof for demonstrating the knowledge of a graph three-colouring without revealing the coloring may be described as a sequence of independent iterations of the following stages (Fig. 14) (9). First, Alice switches the three colors at random (e.g. switching all red nodes to blue, all blue nodes to yellow and all yellow nodes to red).

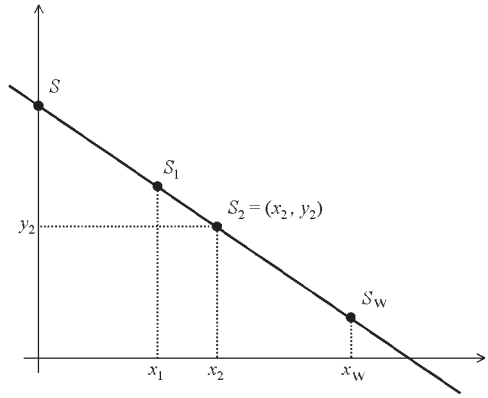

Fig. 15. Threshold scheme.

Then, Alice shows to Bob the new coloured graph with every vertex covered. Afterwards, Bob selects an edge of the graph at random, and Alice reveals the colours of the two nodes that are incident to this edge so that Bob can confirm that both endpoints of the edge are coloured with two different but legal colours. Finally, in the aforementioned 'Where's Wally?' example, the authors of (12) propose two solutions for Alice to prove she knows where Wally is without revealing his location.

A very practical multiparty protocol that allows teaching linear equations and determinants is secret sharing. It consists in splitting a secret into w pieces, which are distributed among users, so when some of them meet, the secret may be reconstructed. An interesting version of secret sharing, the so-called threshold schemes may be used to practice the resolution of systems of linear equations. In this case the secret S may be recovered from any t of the w pieces, and cannot be determined through any subset of $t-1$ or less pieces. One curious example of practical application of threshold schemes is the nuclear launch code, which is a threshold scheme where any two of the president, the minister of foreign affairs or the minister of defense can combine their pieces to recover the secret code. Another interesting example of application of threshold schemes is visual cryptography, consisting in the reconstruction of an image by means of the overlapping of some parts of it.

Polynomials have two properties that are very useful for defining threshold schemes. Firstly, it is always possible to find the coefficients of a curve of degree $t-1$, $f(x)$, if t points (x_i, y_i) with $y_i = f(x_i)$ are given. On the other hand, it is not feasible to figure out anything about $f(x)$ if only $t-1$ points on the polynomial are given. Both properties may be easily introduced to students through straight lines and planes. A threshold scheme based on polynomial interpolation to reconstruct a curve of degree $t-1$ from t points may be described as follows (Fig. 15). First, w values y_i, which will be the pieces to distribute, may be derived from any random $(t-1)$-degree polynomial $f(x) = (a_{t-1}x^{t-1} + \cdots + a_1x^1 + a_0)$, whose constant coefficient should be the secret, by evaluating $f(x)$ on w different values $x_1, \ldots, x_w$, $y_i = f(x_i)$, $i = 1, \ldots, w$. In this way, $f(x)$ and the secret can be easily reconstructed from any t pieces by solving the linear equation system.

Now we propose to practice with average computation through a curious multiparty version of an oblivious transfer, where several users learn some common information without letting anybody learn anything about individual secrets. A simple example that allows determining an average while concealing all individual values is now described (Fig. 16). First, students should sit in a circle and then a student Alice should secretly choose a random number, add it to her

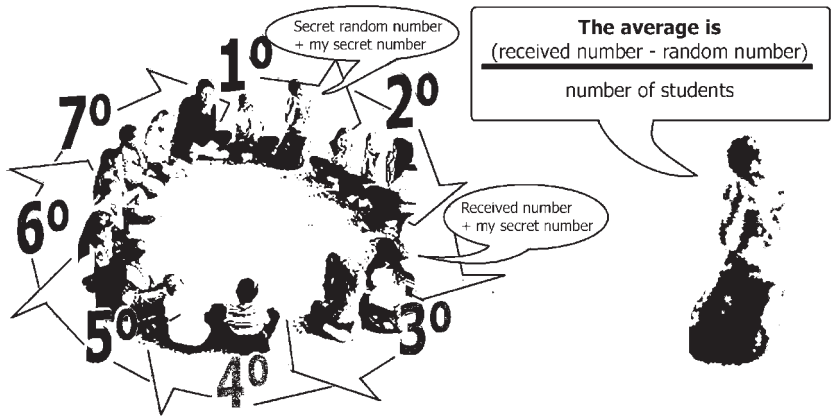

Fig. 16. Multiparty oblivious transfer.

secret number and communicate the result to her right neighbour Bob. Then Bob should add his secret number to the number he received from Alice and tell the sum to his right neighbour and so on. Finally, the sum returns to Alice, who should subtract the initial secret random number and divide the result by the number of students to find the average. So, no one has learned anyone else's individual secret, but everyone knows the average.

Finally, a point that deserves to be mentioned is that protocols described in this section are usually employed as ingredients of more practical and complex applications such as electronic elections, contract signing in networks, secure identification and digital cash.

5. Conclusions

The primary aim of this work is to propose cryptology as an invaluable source of tools for teaching mathematics in an entertaining way. In order to mention some of its possibilities, a trip through several important concepts of cryptology has been made while remarking on various mathematical subjects related to them.

The area of cryptology is increasingly becoming a vital part of our computational society (which is one of the reasons why it is mentioned in many recent movies). Our experiences using cryptology for mathematics teaching have shown us that curious students who are used to computers, passwords and the Internet have usually a more receptive attitude to cryptology.

The development of a complete collection of concrete activities intended to incorporate cryptology in an effective way into the mathematics standard curriculum is part of a work in progress.

Acknowledgements

The authors acknowledge the Spanish Ministry of Education and Science and the European FEDER Fund under Project SEG 2004-04352-C04-03 for partly supporting this work.

References

1. Schneier, B. (1994) *Applied Cryptography*. John Wiley and Sons.
2. Fellows, M. R. and Koblitz, N. (1993) Kid Krypto. Advances in Cryptology-Crypto92, *Lecture Notes in Computer Science* Vol. 740, Springer-Verlag, Berlin, pp. 371–389.
3. Sgarro, A. (1989) *Codici Segreti*. Mondadori.
4. Singh, S. (1999) *The Code Book*. Ed. Reviews.
5. Ruthven, K. and Hennessy, S. (2002) A Practitioner Model of the Use of Computer-based Tools and Resources to Support Mathematics Teaching and Learning. *Educational Studies in Mathematics*, **49**, 47–88.
6. Koblitz, N. (1999) *Algebraic Aspects of Cryptography*. Springer-Verlag, Berlin.
7. Dubinsky, E. (1985) The Use of Computers in Mathematical Education. *SIAM Newsletter*, June.
8. Salomaa, A. (1996) *Public-Key Cryptography*. 2nd edn. Springer-Verlag, Berlin.
9. Blum, M. (1986) How to Prove a Theorem So No One Else Can Claim It. *Proceedings of the International Congress of Mathematicians,* Berkeley, California, USA, Vol. 1.2, American Mathematical Society, 1444–1451.
10. Hanna, G. (2000) Proof, Explanation and Exploration: An Overview. *Educational Studies in Mathematics*, **44**, 5–23.
11. Berson, T., Guillou, L. and Guillou, J. J., (1990) How to Explain Zero-Knowledge Protocols to your Children. Advances in Cryptology-Crypto89, *Lecture Notes in Computer Science*, Vol. 435, Springer-Verlag, Berlin, pp. 628–631.
12. Naor, M., Naor, Y. and Reingold, O. (1999) Applied Kid Cryptography. *Journal of Craptology*, **1** www.wisdom.weizmann.ac.il/naor/PUZZLES/

Pino Caballero-Gil is professor of cryptography at the University of La Laguna, Canary Islands, Spain. Her research interests are in cryptography (design of cryptographic protocols and cryptanalysis of stream ciphers) and mathematics education (new resources for secondary education).

Carlos Bruno-Castañeda teaches Mathematics at a high school in Tenerife, Canary Islands, Spain. He is nowadays working on his PhD thesis dealing with cryptography used for mathematics education.

Address for correspondence: Pino Caballero-Gil, Department of Statistics, Operations Research and Computation, Faculty of Maths, University of La Laguna, 38271 La Laguna. Tenerife, Canary Islands, Spain. E-mail: pcaballe@ull.es