Arithmetic and Cryptography

Michel Waldschmidt

Michel Waldschmidt is a specialist of transcendental number theory. He has been President of the French Mathematical Society (SMF: Société Mathématique de France) and is now vice-president of the International Center of Pure and Applied Mathematics (CIMPA: Centre International de Mathématiques Pures et Appliquées), an international organization helping to promote the mathematical sciences in developing countries supported by the UNESCO.

Keywords
Number theory, arithmetic, cryptography, RSA, public key cryptosystem, prime numbers, factorization, algorithms, residue class ring, theoretical computer science, internet security, information theory, trapdoor oneway function.

Among the unexpected features of recent developments in technology are the connections between classical arithmetic on the one hand, and new methods for reaching a better security of data transmission on the other. We will illustrate this aspect of the subject by showing how modern cryptography is related to our knowledge of some properties of natural numbers. As an example, we explain how prime numbers play a key role in the process which enables you to withdraw safely your money from your bank account using ATM (Automated Teller Machines) with your secret PIN (Personal Identification Number) code.

1. Short History

Old cryptography methods relied on elementary operations on the symbols of the initial text, a simple example being to replace each letter by another one following a given rule which was supposed to be known only by the sender and the receiver. Julius Caesar is often quoted as using the code which consists in shifting each letter of the alphabet by a given number of places. Many variants have been introduced, but now it is known that none of them is really reliable: it is easy to decipher such messages without knowing the key, and one can even recover the key from an encoded message.

To break such a code, one efficient process is to perform a statistical study of occurrences of the different letters. This idea was used as early as IX-th century by Abu Youssouf Ya qub Ishaq Al Kindi who checked the authenticity of sacred Islamic texts.

During the XIII-th century, in his *Letter concerning the Marvelous Power of Art and Nature and the Nullity of Magic*, Roger Bacon described seven methods to encrypt messages.

In the XVI-th century, the French diplomat Blaise de Vigenère was also a cryptographer.

C Babbage (1791-1871)[1], who invented the computer, pointed out the usefulness of statistics for deciphering encrypted messages. At the same period a remarkable breakthrough was achieved by J-F Champollion who pioneered decipherment of the previously unreadable ancient scripts of Egypt involving hieroglyphs.

[1] Please see issue on Charles Babbage, *Resonance*, Vol.7, No.6, 200.

After the war in 1870 between France and Germany, the French Government realized that one strong point of the German army was communication; it was decided to create military centres for the study of carrier-pigeons. At the same time, James C Maxwell was developing electromagnetism theory which, thanks to the works of H H Herz and Acharya J C Bose, was going to give rise to radio and modern means of transmitting data.

In a visionary paper on *the military cryptography* published in the *Journal of Military Sciences* in 1883, A Kerckhoffs proposed a number of principles which are still valid. One of the most important principles emphasises that it should be assumed that any cryptographic method is known to the enemy; and thus, the security of the system must rely only on the choice of the keys, which should be renewed on a regular basis.

It should be assumed that any cryptographic method is known to the enemy; and thus, the security of the system must rely only on the choice of the keys, which should be renewed on a regular basis.

The *red phone* (which was a fax) between White House and Kremlin during the cold war used the disposable mask technique which had been invented by G Vernam in 1917.

During World War II, most German communications were enciphered on the Enigma cipher machine. It was

based on rotors whose movement produced ever-changing alphabetic substitutions. The mathematician A Turing[2] invented a codebreaking machine, the Bomb, which gave birth to the first electronic programable computer by Max Newman. The work done by him and his colleagues at Bletchley Park brought cryptology into the modern world. It required ingenious logic, statistical theory, the beginnings of information theory, advanced technology, and superb organisation.

[2] Please see issue on A M Turing, *Resonance*, Vol.2, No.7, 1997.

C Shannon[3], an American electrical engineer and mathematician, has been called 'the father of information theory': he pioneered the modern mathematical theory of data transmission.

[3] Please see issue on C Shannon, *Resonance*, Vol.7, No.2, 2002.

The principles of using public keys for enciphering messages was suggested by W Diffie and M E Hellman in 1976; its first realization in 1978 by R L Rivest, A Shamir and L M Adleman produced the RSA system which is nowadays the most efficient. We shall outline below the basic ideas behind the RSA crypto-system.

2. The Exchange of Suitcases Protocol

An elementary example of secured data transmission is the following one. Alice wishes to send a suitcase to Bob. She does not want Charlie, who is going to carry the suitcase, to know what is inside. Alice has a lock and the key of the lock. Bob also has a lock and the corresponding key, but they are not compatible with the ones of Alice (otherwise it would be straightforward). How can they proceed? Given the minimal amount of information, it is not difficult to find the following solution. Alice wants to send the suitcase whose content is confidential, so she needs to close it with her lock. Then she asks Charlie to carry it. When Bob receives it, he is not able to open it. Now he remembers he also owns a lock: so he uses it and gives back to Charlie the suitcase closed with two locks. When Alice receives the suitcase

The principles of using public keys for enciphering messages was suggested by W Diffie and M E Hellman in 1976; its first realization in 1978 by R L Rivest, A Shamir and L M Adleman produced the RSA system.

from Charlie, she is not able to open it (anyway she knows the content), what she can do is to remove her own lock since she has the key, and to give once more the suitcase to Charlie. Finally when Bob receives for the second time the suitcase, there is only one lock, of which he has the key, so he is able to open it.

We shall explain how to translate this protocol in arithmetic terms. Charlie will be replaced by electronic connections, and the substitute for the suitcase will be a digital message, hence a sequence of 0 and 1. This message will be split into pieces, all of the same length: hence the message to be sent will be a number given by its binary expansion, and this number will lie between 0 and a given bound. The lock and the key will also be replaced by numbers. To close the suitcase with the lock or to remove the lock with the key will be replaced by arithmetical operations, involving the corresponding numbers (those of the message and the lock or the key). Applying successively the lock and the key should give back the initial message. Moreover, someone who does not have the key should not be able to open the lock.

3. Checking the Identity

In many circumstances one needs to prove one's own identity, or at least to prove that one knows a secret code or password that is supposed to be known only to him. Take the example of someone who wishes to use an *Automated Teller Machine* (ATM) to withdraw money from his bank account using his plastic smartcard with a chip. He knows his *personal identification number* (PIN). In a secured transaction, the bank does not know the PIN: it would be too risky to store this information in a computer. How could the bank check that the user knows his PIN? One should assume that other people are able to listen to all messages which are sent during this transaction. So the user should prove to the bank that he knows his PIN without giving any

In many circumstances one needs to prove one's own identity, or at least to prove that one knows a secret code or password that is supposed to be known only to him.

information which would enable anyone to discover this PIN: at the end of the transaction the bank still does not know it, the bank only checks that the user knows his PIN.

No solution to this problem by means of classic enciphering methods is known. In order to solve this problem, one requires to use the recent developments of the subject.

We shall explain how it works in practice, but let us start by telling the first step: the bank will ask a question to the user, and each time the question will be different. Knowing the right answer to one such question will not give hints to guess the answer to another one. In other terms the first message sent by the bank will be selected randomly. Once more it will be a number (given by its digital representation) between 0 and a given bound. The chip will make some computation using this number (message) together with the PIN (which is another number), and the result will be sent to the bank. Hence one needs to find a process which enables to compute the outgoing message using the incoming message if one knows the PIN, and which enables to check that the users knows his PIN if one knows both the incoming and outgoing messages.

In the cryptosystems used before Diffie and Hellmann, there was a symmetry: Alice and Bob were exchanging information using each a secret key that they shared. These keys enabled each of them to write to the other and to decypher the messages they received. The basic feature of *public key cryptography*, introduced by Diffie and Hellmann in 1976, is that any user has two keys, a public one and a secret one. The public key is known by everybody, and everybody is able to send a message to any user, by means of its public key. Only the receiver having the private or secret key is able to understand the message. The public key is a substitute for the lock

In the cryptosystems used before Diffie and Hellmann, there was a symmetry.

and the private key for the key of the lock.

One may notice that in the question of exchange of suitcases, if the lock of Bob is replaced by a public key, then a single trip from Charlie is sufficient: Alice uses the public key (lock) of Bob, and Bob can open the suitcase with his secret key.

Modern cryptographic methods rely on mathematical questions for which no efficient solution is known.

4. A Trapdoor Oneway Function

To find the right path in a maze may be very complicated. However, if someone gives you the solution, it is much easier to check whether it works or not. A similar situation occurs in arithmetics: if I give you two numbers and ask for their product, it is not a too difficult task, provided that the numbers are not too large. On the other side if I give you their product only, it may be harder to find the two numbers. For instance if I tell you that the product I get is 2 047, it takes more time to find that the two numbers I multiplied are 23 and 89 than to check the result.

Modern cryptographic methods rely on mathematical questions for which no efficient solution is known. The *factorisation problem*, which is the problem of decomposing an integer into a product of primes, like we did for 2 047, can be solved by modern computers for numbers with no more than 150 or 200 decimal digits. For larger numbers the required computing time is prohibitive.

In cryptography, a *trapdoor oneway function* is a function that is easy to compute in one direction, yet believed to be difficult to compute in the opposite direction; however, given some extra information (called the trapdoor information), it becomes feasible to compute the inverse function. We shall give a simplified example using the ideas which are involved in RSA.

In cryptography, a *trapdoor oneway function* is a function that is easy to compute in one direction, yet believed to be difficult to compute in the opposite direction.

We are going to work with numbers of three decimal digits only, which means that one considers the integers

between 000 and 999. We shall perform some computations, when the result exceeds 1 000, one keeps only the last three digits. This amounts to divide by 1 000 and to keep the remainder, if you prefer.

We shall take *powers* of numbers. The *square* of a number (second power) is the product of this number with itself. For instance, the square of 471 is 471×471, namely 221 841. The *cube*, or third power, is the product of the square with the initial number: so the cube of 471 is the product of 221 841 with 471, the result being $471 \times 471 \times 471 = 104\,487\,111$. If we continue and multiply this last number by 471 we get the fourth power, and so on.

It will be convenient to introduce the *exponential* notation with an upper exponent: the successive powers of 2 will be denoted by $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64\ldots$.

The secret key will be 3, and the operation will be to raise to the third power and keep only the last three digits. For instance starting with 471 we consider the last three digits of its cube $471^3 = 471 \times 471 \times 471 = 104\,487\,111$ and we get 111. Notice that it is more clever to keep only the last three digits after each step, for instance after computing the square 471×471 we keep only the last three digits, namely 841, which we multiply with 471 and get 396 111. The last three digits are obviously the same, but this way leads us to work only with numbers having no more than 6 decimal digits.

If I tell you that the operation which I just describe (raise to the cube and keep the last three digits) produces 631, will you be able to tell me which is the three digits number I started with?

The brute force solution is to try one after the other all 999 possibilities: for each of them you perform the operation and you compare with 631. Of course you

will find the solution, which is 111, but this so-called *greedy method* is a bit long to implement, and in practice it will not be possible to perform it in a reasonable time because the numbers to be considered will involve hundreds of digits, not just 3. So, let us forget it for a while.

Now I give you the secret key (which is the trapdoor information here): it is 67. This means that if you compute the last three digits of the 67-th power of 631, you find the initial number 111. It is much faster to compute a 67-th power than to perform the above mentioned exhaustive search. To compute a square requires one multiplication. For a cube you need one more. You might expect that a 67-th power requires altogether 66 multiplications, but one may improve the process by means of the *square-and-multiply algorithm*. Indeed, if you multiply the square of a number by itself, you find the 4-th power, with only two multiplications. The product of the 4-th power by itself yields the 8-th power, with only 3 multiplications altogether. So to compute the last three digits of 631^{67}, first write $67 = 64 + 2 + 1$, and then take successive squares (keeping only the last three digits): 631^2, 631^4, 631^8, 631^{16}, 631^{32}, 631^{64}. Now you multiply the values of 631^{64}, 631^2, and 631 (keeping always the last three digits only, the others are useless here). The final result is 111, as we announced. This is how 3 plays the role of the lock and 67 of the key: if you put the lock 3, you remove it with the key 67. Here is the scheme:

$$\boxed{111} \xrightarrow{3} \boxed{631} \xrightarrow{67} \boxed{111}$$

More generally the lock and the key interact as follows:

$$\boxed{\text{original message}} \xrightarrow{\text{lock}} \boxed{\text{encoded message}} \xrightarrow{\text{key}} \boxed{\text{decoded message}}$$

Of course the decoded message should be identical with the initial one!

Here, it turns out that we could permute the process: if you take 67 as a lock, then 3 is a key: the last digits of 111^{67} are 471 while the last digits of 471^3 are 111

$$\boxed{111} \xrightarrow{67} \boxed{471} \xrightarrow{3} \boxed{111}$$

You will check that for the lock 7 one may use the key 43. For instance the last three digits of 111^7 are 871, and the last three digits of 871^{43} are 111:

$$\boxed{111} \xrightarrow{7} \boxed{871} \xrightarrow{43} \boxed{111}$$

We always selected the same initial message, 111. Any number between 0 and 999 could be selected, provided that its last digit is 1, 3, 7 or 9 (see Section 5).

Now we are able to produce the analogue of the protocol of exchanges of suitcases. We replace the suitcase by 111, Alice's lock by 7, the key of her lock by 43, the lock of Bob by 3, the key of his lock by 67, and of course each time we consider the last three digits of the corresponding power.

So Alice first puts her lock 7 on the suitcase 111: this means that she sends to Bob the last three digits of 111^7, wich are 871.

Hence Bob receives 871, which corresponds to the suitcase closed with Alice's lock. He puts his own lock 3, which means that he sends back to Alice the last three digits of 871^3, which are 311.

Now Alice uses her key 43 to remove her lock: she sends the last three digits of 311^{43}, namely 631. Therefore 631 corresponds to the suitcase closed only with Bob's lock.

And now Bob is able to open the suitcase thanks to his key 67: the last three digits of 631^{67} are indeed 111, as we already saw.

$$\boxed{111} \xrightarrow{7} \boxed{871} \xrightarrow{3} \boxed{311} \xrightarrow{43} \boxed{631} \xrightarrow{67} \boxed{111}$$

Hence 7 closes the suitcase while 43 removes this lock, while 3 puts another lock and 67 opens it.

Next let us go to the bank. Assume that the key 3 of Bob is public, but that he is the only one to know the secret key 67. When he goes to an ATM to withdraw cash, the bank will send him (or rather send to the chip of his credit card) a random message; say that this message is 111. Using his secret key 67 he computes the last three digits of 111^{67}, he finds 471, and this is what he replies to the bank. Now the bank checks that the last three digits of the cube of 471 are the initial message 111 (the cube, since the public key is 3).

$$\boxed{111} \xrightarrow{67} \boxed{471} \xrightarrow{3} \boxed{111}$$

5. Arithmetic

We should insist that we have given only an outline of the method: a number of questions arise, some of them are well understood, while others are being investigated now.

Let us explain why $(3, 67)$ and $(7, 43)$ are admissible pairs of $(key, lock)$. The point is that the last two digits of both products 3×67 and 7×43 are 01, while all numbers corresponding to messages have for last digit 1, 3, 7 or 9. We need some more arithmetic to explain what is going on.

For an integer m, the following statements are equivalent:
- the last decimal digit of m is 1, 3, 7 or 9,
- m is neither divisible by 2 nor by 5,
- m is relatively prime to 10,
- m is relatively prime to $10^3 = 1\,000$,
- the residue class of m modulo 10^3 is a unit (invertible element) in the quotient ring $\mathbf{Z}/\mathbf{10^3Z}$.

It will be convenient to work with the residue class ring $\mathbf{Z}/\mathbf{10^3Z}$. This amounts to keeping the last three decimal

digits, namely the remainder of the Euclidean division by 1 000.

By the Chinese Remainder Theorem, this ring $\mathbf{Z}/\mathbf{10^3Z}$ is isomorphic to the direct product of the ring $\mathbf{Z}/\mathbf{2^3Z}$ having $2^3 = 8$ elements with the ring $\mathbf{Z}/\mathbf{5^3Z}$ having $5^3 = 125$ elements.

The multiplicative group of the units in $\mathbf{Z}/\mathbf{10^3Z}$, which we denote by $(\mathbf{Z}/\mathbf{10^3Z})^\times$, is the direct product of the group $(\mathbf{Z}/\mathbf{2^3Z})^\times$ having $2^3 - 2^2 = 4$ elements with the group $(\mathbf{Z}/\mathbf{5^3Z})^\times$ having $5^3 - 5^2 = 100$ elements. Hence $(\mathbf{Z}/\mathbf{10^3Z})^\times$ has 400 elements; its *exponent* is the lcm (*least common multiple*) of 4 and 100, which is 100: this means that any element x in $(\mathbf{Z}/\mathbf{10^3Z})^\times$ satisfies $x^{100} = 1$. In other terms, if you take the 100-th power of an integer m with last digit 1, 3, 5 or 9, then the last three digits of the result m^{100} are 001. Obviously, any power of m^{100} has the same property, because any power of a number ending with 001 has also 001 as last three digits. This means that if b is a multiple of 100 and m is relatively prime to 10, then the last three digits of m^b are 001. As a consequence, if we multiply such a m^b with m, the last three digits of the product m^{b+1} are the same as the last three digits of m itself. And now, b is a multiple of 100 if and only if the last two digits of $b+1$ are 01.

So we have proved the following

Proposition. *Let m be a positive integer with last decimal digit* 1, 3, 7 *or* 9. *Let a be a positive integer with last two decimal digits* 01. *Then m^a and m have the same last three digits:*

$$\gcd(m, 10) = 1, \quad a \equiv 1 \pmod{100} \quad \Longrightarrow$$

$$m^a \equiv m \pmod{1\,000}.$$

Denote by $\lambda(m)$ the exponent of the multiplicative group $(\mathbf{Z}/\mathbf{mZ})^\times$. For instance $\lambda(1\,000) = 100$ and $\lambda(100) = 20$.

For $\ell \in \mathbf{Z}$ having $\gcd(\ell, 10) = 1$, we have $\ell^{20} \equiv 1 \pmod{100}$, so that the inverse k of ℓ modulo 100 is $\ell^{19} \pmod{100}$. This gives an algorithm to compute the secret key k when one knows the public key ℓ, provided that one knows also the number $\lambda(\lambda(N))$ for messages in $(\mathbf{Z}/\mathbf{NZ})^{\times}$. Examples with $N = 1\,000$ are $\ell = 3$, $k = 67$ and $\ell = 7$, $k = 43$:

$$3^{19} \equiv 67 \pmod{100} \quad \text{and} \quad 7^{19} \equiv 43 \pmod{100}.$$

Of course with such small numbers the cryptosystem is not secured! For actual implementation of the RSA cryptosystem one replaces $10^3 = 1\,000$ by the product of two distinct large prime numbers p and q. Each of them has some 150 decimal digits, so the product pq has about 300 decimal digits. Since $2^{10} = 1\,024$ is close to 10^3, a number with 300 decimal digits has about 1 000 binary digits. Exhaustive searches are not feasible with such large numbers, even with very powerful computers. One basic point is that the product $N = pq$ is public but p and q are kept secret. Nowadays, given a number with 300 decimal digits which is the product of two large prime numbers p and q, computers are not able to find the factors p and q within a reasonable time. The security of the RSA protocol relies heavily on this fact.

Nowadays, given a number with 300 decimal digits which is the product of two large prime numbers *p* and *q*, computers are not able to find the factors *p* and *q* within a reasonable time. The security of the RSA protocol relies heavily on this fact.

The multiplicative group $(\mathbf{Z}/\mathbf{pqZ})^{\times}$ of the residue class ring $\mathbf{Z}/\mathbf{pqZ}$ modulo the product pq is a group of order n with $n = (p-1)(q-1)$. The condition in the previous example with 10^3 that the message m should not be divisible by 2 nor by 5 is replaced by the condition that m should not be divisible by p nor by q - now only a very tiny percentage of messages are excluded (while with 10^3 only 40% of the 1 000 possible messages were allowed). Next we consider the condition on the lock ℓ and the key k: in the case of 10^3 in place of pq the condition was that their product $a = \ell k$ had its last two decimal digits 01 (this means that the remainder of the division by 100 is 1). Now the condition is that the remainder

Box 1. Research in France and in India

Tuning up these ideas and implementing the process in a concrete way involves high level research activities in a number of laboratories all around the world, including France and India. Interaction between arithmetic and cryptology is a research subject in several places around the world. Among the laboratories where scientists pursue their investigations on this topic are the following French and Indian ones.

The *Computer Science Laboratory at X* in the École Polytechnique (Palaiseau, near Paris)
http://www.lix.polytechnique.fr/cryptologie/english- index.html,

The National Research Institute in Computer Science and Automatic *INRIA (Institut National de Recherche en Informatique et en Automatique)* in Rocquencourt, again near Paris, with the Project *CODES* dealing not only with coding theory but also with cryptography
http://www-rocq.inria.fr/codes/CODES/ENGLISH/index.html,

The Mathematics Department of the ENS (École Normale Supérieure) rue d'Ulm, Paris
http://www.di.ens.fr/CryptoRecherche.html,

In Caen the consortium *Cryptologie et Algorithmique En Normandie (CAEN)* including the *Groupe de Recherche en Informatique, Image, Automatique et Instrumentation de Caen* GREYC
http://www.greyc.unicaen.fr/,

The *Laboratoire de Mathématiques Nicolas Oresme* of the University Caen Basse Normandie
http://www.math.unicaen.fr/lmno/ and *France Telecom R& D Caen*,

In Grenoble the University Joseph Fourier
http://www-fourier.ujf-grenoble.fr/,

In Limoges the *Institut de Recherche XLim* of the University
http://www.xlim.fr/http://www.xlim.fr/,

In Toulon the *Groupe de Recherche en Informatique et Mathématiques GRIM* of the University Sud Toulon-Var
http://grim.univ-tln.fr,

In Toulouse the *Laboratoire d'Analyse et d'Architecture des Systèmes LAAS*
http://www.laas.fr/laas/,

with the team LILAC (Logic, Interaction, Language, and Computation)
http://www.irit.fr/recherches/LILAC/Pers/

Box 1. continued...

Box 1. continued...

and Toulouse Mathematical Institute
http://www.univ-tlse2.fr/grimm/algo.

Number Theory and Cryptography is also a research topic in a number of institutions all around India. We only quote a few of them:

In Kolkata *The Indian Statistical Institute*, with its *Statistics and Mathematics Unit* as well as its *Applied Statistic Division*
http://www.isical.ac.in/,

In Chennai the *Institute of Mathematical Sciences* studying both Mathematics and Theoretical Computer Science
http://www.imsc.res.in/,

In Kanpur the *Indian Institute of Technology* IIT
http://www.iitk.ac.in/

with the *Prabhu Goel Research Centre for Computer and Internet Security*
http://www.security.iitk.ac.in/,

In Bangalore the *Indian Institute of Science* where the section *Computer Science and Automation Cryptography* studies Computational Number Theory, Computational Combinatorics, Arithmetical, Algebraic and Geometric Algorithms
http://www.csa.iisc.ernet.in/,

Again in Chennai the *Society for Electronic Transactions and Security* S.E.T.S. which is specialized in Cryptography algorithms, Cryptology protocols, Secure Information Systems and Security Policy and Cryptanalysis
http://www.setsindia.org/.

We complete this list with the *Cryptology Research Society of India*
http://www.crsind.com/ which organizes the annual International Conference on Cryptology in India *Indocrypt*:
http://www.crsind.com/indocrpt.asp

On each of these web pages one may find a number of further references and resources.

of the division by $\lambda(N)$ of this product is 1. Since $\lambda(N)$ divides n, it suffices to require

$$\ell k \equiv 1 \pmod{n} \quad \text{with} \quad n = (p-1)(q-1).$$

Given ℓ which is prime to n, there is a single k modulo n satisfying this condition, namely

$$k \equiv \ell^{\lambda(n)-1} \pmod{n}.$$

To compute k is easy, provided that one knows n: however, to know both pq and n amounts to knowing both p and q, since $n = pq + 1 - (p + q)$. For someone who knows p and q, it is easy to compute the key k associated with a given lock ℓ. For someone who knows ℓ and N but not the individual factors p and q of N, there is no efficient known way so far to deduce k.

Conclusion

Cryptography and coding theory, which use advanced number theory, teach us an important lesson: mathematical research (research on prime numbers, in particular), which seems to be completely unrelated to practical matters, may turn out to be crucial for some applications many years, or decades later, in a completely unpredictable way. In his book *A mathematician's apology*[1], the great British analyst G H Hardy (1877-1947), who was a fervent pacifist, took immense pride in working in number theory, an absolutely pure field, and at never having done anything which could be considered "useful":

"I have never done anything "useful". No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world. ... Judged by all practical standards, the value of my mathematical life is nil".

It was perhaps 'useless' at that time. It is no longer the case today.

[1] Full text of '*A Mathematician's Apology*' is in the public domain in Canada, courtesy of the University of Alberta Mathematical Science Society: http://www.math.ualberta.ca/~mss/misc/

Acknowledgment

This text is based on lectures given by the author in November 2006 and 2007 under the program *French Science Today* (http://www.frenchsciencetoday.org/) of the

French Embassy in India and the network of Alliances Françaises. The remarkably efficient coordination of this program was done by Bruno Rouot. Amartya Kumar Dutta suggested that this lecture be written down for *Resonance*. Himself as well as S C Bagchi, B Sury, Claude Levesque, Sudhir Ghorpade, and the editor of *Resonance* made very useful comments on a preliminary version. Also Chen Gong Liang sent me further relevant remarks on the security of cryptosystems. Many thanks to all of them.

Suggested Reading

[1] **Alfred J Menezes, Paul C van Oorschot and Scott A Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996. Fifth Printing (August 2001).**
Available online for free download on the web site
http://www.cacr.math.uwaterloo.ca/hac/

[2] **Palash Sarkar, *A Sketch of Modern Cryptology*, *Resonance*, Vol.5, No.9, pp.22–40, September 2000.**
http://www.ias.ac.in/resonance/Sept2000/pdf/Sept2000p22-40.pdf

[3] **R Thangadurai and A K Bhandari, *Classical Cryptosystems*,Bona Mathematica, Vol.12, Nos 1–2, pp.12–33, 2001.**

[4] **R Thangadurai, *Elliptic Curve Cryptosystems*, Bona Mathematica, Vol. 13, Nos 2–3, pp.27–59, June-September 2002,**

[5] ***Elliptic Curves, Modular Forms and Cryptography*, Fields Institute Communications, Vol.38, Hindustan Book Agency, New Delhi, 2003.**
http://www.hindbook.com/Home.asp?P=69

[6] **Gilles Lachaud, *Communicating without errors: error-correcting codes*, in: L'explosion des mathématiques, English version.**
http://smf.emath.fr/en/Publications/ExplosionDesMathematiques/index_en.html

Address for Correspondence
Michel Waldschmidt
Université Pierre et Marie Curie-Paris 6, UMR 7586 IMJ
175 rue du Chevaleret,
Paris, F-75013 France