Mathematics, nature and cryptography: Insights from philosophy of information

Sundar Sarukkai

One influential image that is popular among scientists is the view that mathematics is the language of nature. The present article discusses another possible way to approach the relation between mathematics and nature, which is by using the idea of information and the conceptual vocabulary of cryptography. This approach allows us to understand the possibility that secrets of nature need not be written in mathematics and yet mathematics is necessary as a cryptographic key to unlock these secrets. Various advantages of such a view are described in this article.

Keywords: Cryptography, mathematics, nature, philosophy.

IT seems to be the case that we all know what information really is. We collect information, pass on information, make judgements about such information and so on. But what exactly constitutes 'information'? Is information data? Is it a particular proposition? Is it a fact? In using words like data and fact, it is quite possible that we are only using synonymous terms for information, without adding more meaning to it. Is information a concept like others such as knowledge, truth and so on? If so, what are its characteristics? In other words, how do we judge whether something is information or not? Although we are immersed in the world of information, there is some difficulty in finding a unified meaning for it, a difficulty which has been noted by a range of writers, including Shannon who was instrumental in initiating the study of information.

However, it is possible that these questions are ill-posed. Given the wide diversity of contexts where we engage with the idea of information, it is reasonable to expect, as Floridi does, that the idea of information 'can be fruitfully analysed only in relation to well-specified contexts of application'[1]. Rather than search for a unified meaning transcending contexts, it may be more useful to search for the meaning within each context in which the information appears.

Although epistemology, in its most fundamental preoccupations, deals with the notion of information, detailed analyses of this idea arose primarily through its association with the idea of computation and development of the field of computer science and communication technology. Although information arises in all fields, particularly in the sciences, the 'philosophy of information' is, in the words of Adriaans, still a 'young discipline with unclear boundaries'[2]. The relation between information and science is further reinforced by Adriaans' observation that in his view the 'central motivation' for a philosophy of information allows us to address two old philosophical problems, namely 'a unified mathematical description of reality' as well as 'a unified scientific language'.

There are many different ways of defining information, definitions which reflect their disciplinary origins. For example, Shannon's well-known definition is given in terms of bits as the units of information. There are other possible ways of defining information such as quantum information, Fisher information and so on[2]. In general, information is something that is involved in transmission and exchange, and thus is central to communication and representation. Such a view underlies not only some of the common definitions arising in information theory or computer science but, as Adriaans points out, also in science. He goes to the extent of claiming that the 'concept of a message sent from a sender to a receiver can be seen as a true paradigm of modern science in the Kuhnian sense'[2]. He then points out three elements that constitute this idea of information: (i) there is a flow of information from the sender to the receiver concomitant with the observation that the information possessed by the receiver increases as a result of such transmission; (ii) messages and information can be 'coded in terms of systems of arbitrary signs', and (iii) it is possible to have a 'mathematical measure of information content of the message'[2]. This article focuses on some specific issues, particularly those that relate information, science and mathematics. In particular, I would like to explore the relation between mathematics and information with reference to the capacity of mathematics to reveal the information present in nature. This will involve a critique of an established tradition which views nature as an open book written in the language of mathematics. I also suggest the contours of another model, namely nature as a cryptographic machine and

Sundar Sarukkai is in the National Institute of Advanced Studies, Indian Institute of Science Campus, Bangalore 560 012, India.
e-mail: sarukkai@nias.iisc.ernet.in

mathematics as a key to open the secrets of nature, a view which will help us rethink the relation between mathematics and nature along the lines of a philosophy of information.

Mathematics and the philosophy of information

Adriaans notes that the origin of the modern idea of information can be traced back to France in the 15th century, after which it began to be used in Europe with various meanings. He also points out that interestingly, this idea went out of circulation for over two centuries in the works of various philosophers, including Kant. The revival of this term (with the specific connotations that we now associate it with) was related to the development of new communication technologies as well the need for transmitting coded information by militaries.

Although Adriaans locates the specificity of the modern idea of information in the shift in the meaning of information from merely an act of informing to the belief that 'something' in a message is 'used to inform', it has always been the case that any communication presupposes the belief in something which is being transmitted. In the case of language, which could be seen as the original model of communication, the question of what is being transmitted in a word/sentence or in an utterance has always been a central issue in various philosophies of language. For example, in the rich Indian philosophical tradition on language, this was an issue that was at the fore of their preoccupations about the nature of language[3]. The ideas of codes and signs were already available for those who subscribed to the view that language was conventional. A user of a language, who is not trained in that convention, cannot know what the words mean. Thus, natural language is already the first example of a system of codes. However, the necessity of going beyond this occurs when we need to transmit secret information between people who know the language. Nevertheless, the view of language as encoding information, as carrying information and transmitting it, already lies at the root of many philosophical theories of language.

Instead of a structured system like language with its all encompassing reach which allows us to use it for a wide range of human activities, codes in general have specific uses, important ones being transmission of information and efficient storage. Thus, we can view codes as being a subset of linguistic activity, if we understand language as going much beyond a role of only transmitting information. For example, the expressive capacity of language is one of its dominant roles. Although this capacity might have encoded information that is being transmitted, there seems to be a qualitative difference in this act and the information communicative act.

Typical notions associated with codes are that of secrecy, efficiency and non-redundancy. Ordinary use of language exhibits various forms of redundancy; looked at in terms of information transfer, ordinary language is an inefficient carrier since it carries along with the information various overlapping information, or auxiliary information which may not be needed. As far as communication of information is concerned, ordinary language overkills and codes underkill in general. Codes are essentially concerned with efficiency and minimizing the effort of transference, although they are also used to increase redundancy as in error correlation. The richness of language arises because of its lack of concern with efficiency. For the modern view of information, language must do something contrary to this instinct. There is a long historical trajectory in many world civilizations which worried about the profligate character of natural language. The shift to arbitrary symbols as modes of representation, the creation of symbolic technical languages, the importance of 'characteristica universalis' of Leibniz, the development of a technical vocabulary in Sanskrit for Indian philosophy and so on, point to ways of dealing with what is seen as an intrinsic problem of languages[4].

Floridi notes two approaches to the philosophy of information: metaphysical and analytical. He makes the interesting point that from 'Descartes to Kant, epistemology can be seen as a branch of communication theory'[5]. The belief that knowledge about the world is indeed accessible to us and communicable is based on the influential belief that we can indeed decipher the secrets of the world. The burden of this decipherment is placed on the human subject, an autonomous subject who has to carry the burden of 'correctly' reading the message. Floridi points out that the linguistic turn overturns a naïve belief in accessing the information of the world without distorting it, for example, through language. The constructionist view, in general, would claim that all that is there are great amount of data and the semantic synthesis of these occurs within the subject. This challenges the position that the message is given (by gods or nature or…) and the human subject merely deciphers that message. The informational model acknowledges the subject as the site of meaning-creation, as the agency who understands the world.

Whatever philosophical worldview we might choose, there is one constant theme: the privileging of mathematics in the modern theories of information. Furthermore, the relation between this view of information and modern science is also strong, not only because of the common mathematical world which they draw from, but also because of the use of many conceptual ideas developed in modern science. Adriaans points to the idea of entropy and the theory of thermodynamics as being influential in the field of information. However, what seems to be commonly accepted is the fast that mathematics and/or technical languages are needed to encode/decode and transmit information.

As mentioned earlier, Adriaans posits that the philosophy of information resolves two old philosophical problems

of finding a 'unified scientific language' as well as to generate 'a unified mathematical description of reality'. The belief in the creation of a unified mathematical description of reality is an essential component of the scientific worldview and is also based on a particular understanding of the relation between mathematics and nature. In what follows, I will describe this worldview and the possible objections to it. In so doing, we not only get an insight into the nature of information, but also an insight into the nature of mathematics. After all, if mathematics is so essential to modern information theory, then presumably awareness of the nature of mathematics can also help us more clearly understand this link between mathematics and the idea of information.

Nature and mathematics

The belief that mathematics is the language of nature, a view held over the centuries by many prominent scientists, entails that the language of science must necessarily be mathematical. There has been much written about this link and on the influential view that nature is an open book written in the language of mathematics[6]. In the context of a philosophy of information, I would like to reconsider this particular view and discuss another possible approach towards understanding the link between science and mathematics.

The view that nature is an open book written in the language of mathematics does many jobs. One, it explains why mathematics is necessary for science – it is so because if the language of nature is mathematics, then the task of science is first to learn this language and secondly to read-off what is written in nature. Two, it explains, although not satisfactorily, the mysteriousness of mathematical applicability in the sciences, a mystery that has worried scientists over time. Three, it offers an important insight into the nature of scientific activity, namely that it is nothing more than reading an already written book. The activity of reading that is invoked here is passive in character, meaning thereby that a book is already available for reading and the scientist only reads what is opened before her. At a fundamental level, this is what scientific objectivity amounts to since the scientist has no part in the writing of the text, but is only seen as an unobtrusive reader. This does not mean that the scientist does not intervene in nature, but only that the laws of nature are independent of human interests. Natural laws order natural processes and the scientist can only be an observer and discoverer of what is already present in nature. But scientific discovery is also not as simple as merely reading. The process of reading is a process of writing and a process of discovery in itself[6]. To invoke another image, we could say that the book is indecipherable at the first instance and doing science is to make legible this indecipherability.

But looking at the activity of science through the philosophy of information allows us to formulate another model to explain scientific activity. This has to do with the information that is encoded in nature, transmitted to the human mind and decoded by a community of scientists. In this view, doing science is to discover the information hidden inside nature. The three most important elements therefore become: How does nature hide its information or how is information encoded within nature? How is the information transmitted to the scientist? How does a scientist decode this information? What I am suggesting is that understanding the methodology of science along the image of information encoding, transmission and decoding actually gives us a fruitful alternate picture to the nature-as-book view.

Note that the belief that nature is written in mathematics is actually a view about information and its relation to language. We can understand this image of nature in the following way. Information about nature is accessible through language; information is encoded within nature in mathematical terms and for immediate access to this information, without any loss in this access as it were, the scientist too has to be a mathematician. The (miraculous!) fact is that the medium in which nature's information is encoded – mathematics – is also the same mathematics available to the scientist and hence not only is this information accessible, but there is also minimal loss in accessing such information. So, even in the view of mathematics as a universal language, the language of nature, an information theoretic element is implicitly present. Without loss of anything significant, we could as well say that the secrets of nature are encoded in mathematics and that science uses mathematics only because it allows us to decode these secrets.

The philosophical problem in this view has to do with the presupposition about the relation between nature and mathematics as the language of information, or the language in which information is stored. The underlying belief is that language is needed to store information and if the same language is available, then the original information is liable to be available without distortion. We can question both these assumptions. We can critique the belief that language, including the complete language of mathematics, encodes information about the world. Furthermore, we can question the belief that merely possessing mathematics necessarily enables us to correctly discover this information.

There are various problems with this perspective of the relation between mathematics and nature. If mathematics is the language of nature, then what is the role of a large domain of mathematics which is not used to describe nature? Physics, for example, only uses a small percentage of the total mathematics that is available to us. Secondly, we can use the same mathematics to construct physical worlds which are contradictory to ours. Thus, there must be something in our physical world that matches with a small set of mathematical entities and processes, thereby

challenging the primacy of mathematics as the language of nature. Thirdly, we have reasons to believe that mathematics, at least significant parts of it, arises from our response to the physical world and thus functions at least at this level as natural languages. The conventionality of mathematics and its indebtedness to the human imagination must also make us wary of accepting at face value, the view that mathematics is the language of nature and doing science is only to read the book of nature.

Approaching this problem of mathematics and its relation to nature through the rubric of information and decoding such information gives us a different insight about the nature of mathematics in these processes. First, what is it about nature that makes it hide its information? Why is information not available as an open book which we can read off without either knowing mathematics or decoding? Asking the question as why a question sounds extremely metaphysical, as if nature has an agency. We can rephrase this as follows: How is information encoded in nature? How do we, as receivers, decode this information? What is the key needed to enable such decoding?

The first observation that should strike us is that information for nature cannot be linguistic. There is nothing linguistic about this world, including nothing mathematical about it. Information about nature is not stored in bits or as some datapoints, although such bits/points might be correlative with some physical processes. So the process of doing science is first of all to add a language to information bits correlated with processes in nature. Now, we must believe that adding language or representing information in terms of language does not distort that information.

However, there is another way of understanding the relation between mathematics and nature. It is based on the observation that accessing this information in/about nature is not to read the mathematics in which this information is coded, but rather to use mathematics as a key. The analogy for this model comes from cryptography. The standard problem in cryptography is this: there is a message which needs to be sent from a sender to a receiver. Only the receiver is expected to have the key to access this message. To get the message, the receiver has to unlock the code. In the cryptography model of science, the key is as important as the message and equally importantly, it is a different category compared to the message – the key is at a meta-level.

Drawing upon this image, we immediately see another way of understanding the relation of mathematics with nature. Instead of looking at nature as written in mathematics, we can consider mathematics as a key that will help us decode the information present in nature. The significant difference is that in this view we do not claim that the message or information is itself written in mathematics but only that mathematics does the job of unlocking the encryption.

It may be useful to draw upon another image here – the image of scientists as eavesdroppers. Early literature in cryptography alludes to codebreakers, those who try to break codes without knowing the original encryption algorithm or not knowing the key even when the algorithm was known. Scientists are eavesdroppers in this sense, who try to break codes and discover the secrets of nature without knowing the key or the original encryption algorithm which nature might have used. In this case, scientists are not really receivers who already have the key, but are only eavesdroppers. However, it is also the case that once a particular key is found, then the same is used in various other contexts and thus in this case they do function as receivers who already possess the key. This view of scientists-as-eavesdroppers instead of scientists-as-readers (of the book of nature) does the added job of explaining scientific activity and the ideas of creativity and excitement associated with it. Codebreaking is a much more exciting activity in comparison to merely being the receiver who uses the key to unlock the original secrets. Furthermore, real creativity in this field occurs in the act of codebreaking, since the codebreaker has to be far more creative than the sender and receiver, and he/she has little information to initially work from. Thus, one can understand the paradigm jumps in scientific practice as also exemplifying the discovery of a new key and normal science as continuing to use this key (and modifications to it) to decipher more secrets of nature. (I thank Nithin Nagaraj for emphasizing this nature of scientists as eavesdroppers and its consequence to scientific creativity.)

Nature and cryptography

Cryptography deals with encryption and decryption. In the most general sense, encryption is conversion of information or message into a code which is then decrypted to render the original message. There are many ways by which the original message can be encrypted. The task of cryptography would involve not only finding methods to encrypt the original information and transmitting it, but also to decrypt the message at the end-point. Encryption and decryption use keys and the real challenge is to find appropriate keys for both encryption/decryption and also for safe transmission.

Cryptography is essentially about information security. One definition of cryptography captures many of the issues related to it: 'Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication'[7]. If we look at the various terms that arise in the study of cryptography, we can see some immediate parallels between the activity of science and cryptography. One important pointer to this lies in the belief that information is not lost nor modified in this process of encryption/decryption (data integrity) with the further stipulation that if there has been some modification, it must be detectable. Authentication also involves authen-

tication of information, which includes some means of validating the origin of information and other particulars associated with this original process of information.

I want to argue here that cryptography and the general vocabulary of information offer us another image within which to situate the scientific activity. One major consequence of this image is a reconsideration of the role of mathematics in the sciences. The obvious point we can begin with is the observation that nature has secrets. Without imputing agency to nature, i.e. without necessarily implying that nature deliberately encrypts information, we can nevertheless understand the importance of the idea of secrecy of natural information (including natural laws) and the scientists' attempts to decrypt this secret. Nature has a storehouse of information which is encoded. Scientists decode this information. The problem then is to find the right codes in which nature's information is encoded and also to find the key that will allow the decipherment of this information. The methodology involved in cryptography, including data authenticity, validation of message in its origin, the belief that the secret information of nature is transmitted without modification and so on, parallel elements of scientific methodology. Two particular aspects in this relation stand out: the belief that the decoding of natural secrets is not influenced by or added upon by scientific interests. This means that there is a transparent access to nature's secret, once the decrypting is done. The other has to do with an essential aspect of scientific methodology, namely relating the empirical to the theoretical. We can understand observations of consequences of a theory as validation schemes in support of a particular message that has been successfully decoded.

The information-model of nature offers a different reading of mathematics. The traditional image of nature being written in the language of mathematics, implies that the secrets themselves are in mathematics. The problem with this view is the association of a particular language called mathematics with nature. But then how would we know that nature's mathematics is the same as the mathematics created by the humans? And also why is it that the language of nature is mathematics?

However, there is another possibility, which is that the secrets of nature, the informational content of nature, need not and are perhaps not 'written' in the language of mathematics. But then what is the language in which the original information has been written? There are two possibilities: one is that the language in which the information is originally written in could be mathematics. The other possibility is that the use of mathematics lies only in accessing this information, a view more in common with cryptography. Thus, the cryptographic view of nature gives prominence to mathematics as a means used to encode the information and also decode it later on. The key which is used to encode and decode can also be mathematical, as it often is in cryptography. However, the important point here is that the original information in itself is not mathematical. For example, we can take an ordinary sentence such as 'It is raining', encode it and choose a key. The content of the message is in English, whereas the encoding and decoding processes may use mathematics.

Thus, we do not have to accept that the secrets of nature are mathematical. However, the essential use of mathematics in the sciences should suggest that mathematics is the key to unlocking these secrets. And since the key is not the message, mathematics only allows us to 'read' the secrets of nature, which in their original form may not be mathematical at all. Thus, it is possible that nature is not an open book written in the language of mathematics, but a book which uses mathematics as a key that allows us to read its contents. Let me in what follows, explore the possibility of mathematics as being the key which opens the informational world of nature.

Mathematics as a cryptographic key

While ciphers or codes are necessary for encrypting a piece of information, the key is what allows us to decipher these codes. For example, it is desirable to have a general access to ciphers or codes and yet enable only certain people to decrypt the message. This is accomplished with the use of a key, a tool which really carries the burden of secrecy. Kerckhoff's law states that 'a cryptosystem should be secure even if everything about the system, except the key, is public knowledge'[8]. For example, if a key pair is exchanged between two parties, then every subsequent message can be encoded and decoded in a way that is only accessible to these two parties.

First of all, why are keys necessary? Here is one reason: 'Having transformations which are very similar but characterized by keys means that if some encryption/decryption is revealed then one does not have to redesign the entire scheme but simply change the key'[7]. This offers the advantage that if one has to change the key, one does not have to change the lock completely. The fact that there are many keys and many different types of keys has important consequences for our understanding of the role mathematics plays in unlocking the secrets of nature.

There are many kinds of keys possible. For example, we can have a symmetric key in which case the key codes for both sender and receiver are the same. There is also public-key, which has two different keys for the sender and the receiver. The development of cryptography has led to varieties of such keys. But since my main aim here is to explore the possibility of understanding mathematics as a key, I will not discuss these points here.

Consider information present in nature. This information is not accessible to us in any immediate sense. It has to be deciphered in some way. Mathematics is the key to this decryption of the secrets of nature. This means that independent of what language the secrets of nature are written in, mathematics is the key to unlock them. We can con-

sider an equivalent situation in cryptography. Imagine coming across a message which is encrypted and we have no key to break this encryption. How would we proceed to decipher the message? It is interesting to note that even in this case mathematics plays an essential role in finding ways to decrypt the message. But nature's secrets do not always reach us without any key. Mathematics itself is a key and thus most often by trail and error, we can completely or partially decrypt information about the world.

Scientists misunderstand the fact that just because the laws of nature can be expressed in a mathematical form, necessarily implies that these laws are originally inscribed in a mathematical form. Consider a simple example. Suppose there is a particular message that is encrypted. After decrypting it, we can read the entire message. Suppose there is a sentence about the number of nuclear warheads that are transmitted secretly. After decoding the message, the original message is available to the receiver. Now, the receiver can express this original message in mathematical terms. This does not mean that the original message was also expressed in mathematics.

Decoding of nature's secrets must be differentiated from the mathematical expression of this secret after decoding. Just because our rewriting of the original message after decoding is done in mathematics, does not necessarily imply that the original message was also written in the same language. If we believe that the original message was also written in mathematics, then we are betraying our presuppositions about language and the nature of mathematics. First, we are presupposing that we are not re-expressing the decoded message. Secondly, we believe that such re-expression is not possible, since mathematics does not allow for faithful translation into other languages. Both these presuppositions are not completely correct. Understanding secrets of nature along the information model allows us to understand the possibility of re-expressing the original message in mathematics. And the question of translation of mathematics, which although needs to be established more rigorously, is one that is established empirically. Although mathematics resists translation and posits itself as a 'pure language' a la Walter Benajamin, there are enough reasons to believe in the translatability of mathematics, including the fact that there is an essential relation between mathematics and natural language[9].

Moreover, the belief that the laws of nature are mathematical can be critiqued on the following grounds. Given a law, say Newton's law of gravitation, we can immediately see that it is expressed in mathematical terms. This law essentially states that the force between two masses is proportional to the masses and inversely proportional to the square of the distance between them. This statement can be expressed mathematically, but it can also be expressed in English. Furthermore, the gravitation law is much more than its mathematical expression. For example, conceptual terms such as mass, distance, force, etc. play an integral role in the formulation of this mathematical expression. To reduce the law only to its mathematical expression overlooks this larger world of conceptual and linguistic terms that are already encoded within it. Thus, it is reasonable to believe that the laws of nature (as well as its other secrets) are not written in mathematics, but are writable in mathematics. The other major objection is that there is no reason to believe that every information sentence is expressed mathematically or can even be expressed so.

Then where does mathematics come in? Mathematics is a factor in the same way it is a factor in cryptography. Note that in encrypting messages, there is no claim that the messages are themselves originally expressed mathematically. In cryptography, encryption of the original messages (which could be in English, for example) transforms those messages in general into a symbolic one. The receiver can then decrypt this message if she knows the key to do so. In the process of encryption, decryption and transmission, various aspects of mathematics are used. But this in no way suggests that the original messages are themselves mathematical.

Consider therefore the possibility that this is so in the case of decrypting nature's secrets. The original secrets could in principle be in any language or at least capable of being expressed in any language. But the process of decrypting them or transmitting them without any deviation may be dependent on mathematics. We can further isolate another important characteristic of mathematics, namely its role as a key to decipher the messages. If mathematics functions as a key, and we can in principle define what kinds of keys this could be, then there is no need to believe that the original message is written in mathematics. By so doing, we are not jettisoning the integral relation between mathematics and the sciences. Mathematics is necessary for the sciences mainly because it is the key that unlocks nature's secrets and not because these secrets are themselves mathematical. Mathematics as the key and not as the information has immediate implications for understanding the relation between mathematics and nature.

This view also explains in part the problems with the nature-as-book view. I had earlier pointed out that there is much more available mathematics than is used in the sciences. In the view of mathematics-as-key we can understand this problem by noting that there are many more keys than are required at a particular moment. Various mathematical expressions can in principle be a key, but which key fits which lock depends on the nature of the lock. The possibilities of the natural world as well as its constraints are much more than those of the mathematical world, and hence the space of mathematical keys in much larger than the locks that, when opened, reveal nature's secrets.

The fact that the same mathematics can model, describe and explain contrary worlds to ours, a fact that runs counter to nature-as-book view, is also explained by viewing mathematics as a key. The mathematics used to

construct such contrary worlds is the key to open the secrets of such worlds if they exist. Since mathematics per se is not the language of our world, there is no problem in using the same mathematics to construct other worlds.

Finally, I believe that mathematics-as-key view also allows us a more refined understanding of the 'unreasonable effectiveness' of mathematics[10]. Keys are designed to open locks and after opening the locks it does not seem sensible to exclaim that the keys were unreasonably effective in opening the locks. The cryptographic view also explains why there is so much of mathematics that is irrelevant to the world, that one can use the same mathematics to construct a contrary physical world to ours and so on. These worries arise only if mathematics is seen as the language of nature, whereas they dissipate once we understand that mathematics is the key to unlock the information of nature. As keys, there are innumerable ones; the secret of scientific success lies in finding the right key for a particular message. There is not just one coding present in nature. Each one of its phenomena, in principle, encodes information in unique ways and to unlock them we need a unique mathematical key (as well as other linguistic keys). Thus, only special mathematical entities and structures are relevant. The process of discovery, the process of finding the 'right' mathematics, is actually the process of finding the right key. Finding the right mathematical term is nothing more than finding/constructing the correct key that fits the lock and opens the encrypted code in which nature's information is stored.

But why mathematics? What is so special about mathematics and its unique relationship with nature? The cryptographic view would suggest that mathematics is one particular key which allows access to the secrets of nature. Here, it is pertinent to note that even natural language functions as a key. There is much about the information of the world that is actually 'unlocked' by the use of natural languages. Having said that, we may need to acknowledge the fact that mathematics succeeds as a better key in some contexts but there are other contexts, for example, in certain scientific descriptions arising in biology or in the social sciences, which may not necessarily depend on it. Mathematics, therefore, is one key used by the scientists in their role as eavesdroppers. There are important consequences of this view for the use of mathematics in various disciplines such as social sciences. To understand this issue further, we need to analyse the role of mathematics in cryptography. Without doing this in detail here, let me only make one observation: cryptography uses mathematics without necessarily making any ontological or metaphysical claims about either mathematics or its special relationship with nature. This particular approach hides within it an alternate view about nature and its relationship to information and mathematics.

1. Floridi, L., Is semantic information meaningful data? *Philos. Phenomenol. Res.*, 2005, **LXX**, 351–370.
2. Adriaans, P., Philosophy of information, concepts and history (preliminary version): http://www.illc.uva.nl/HPI/
3. Matilal, B. K., *Logic, Language and Reality: Indian Philosophy and Contemporary Issues*, Motilal Banarsidass, Delhi, 1985 and Sarukkai, S., *Indian Philosophy and Philosophy of Science*, CSC/Motilal Banarsidass, Delhi, 2005.
4. *Ibid*, see also Sarukkai, S., The use of symbols in mathematics and logic. In *Essays on the Foundations of Mathematics and Logic* (ed. Sica, G.), Polimetrica, Monza, Italy, 2005, pp. 99–119.
5. Floridi, L., Two approaches to the philosophy of information. *Minds Machines*, 2003, **13**, 459–469.
6. Sarukkai, S., *Translating the World: Science and Language*, University Press of America, Lanham, 2002.
7. Menezes, A., van Oorschot, P. and Vanstone, S., *Handbook of Applied Cryptography*, CRC Press, 1996, Chapter 1; available online at http://www.cacr.math.uwaterloo.ca/hac/about/chap1.pdf
8. http://en.wikipedia.org/wiki/Kerckhoffs%27_law
9. Sarukkai, S., Mathematics, language and translation. *META*, 2001, **46**, 664–674 (the full text of the article is available at: http://www.erudit.org/revue/meta/2001/v46/n4/).
10. The phrase 'unreasonable effectiveness' is attributed to Wigner. For more on this topic, see Sarukkai, S., Revisiting the 'unreasonable effectiveness' of mathematics. *Curr. Sci.*, 2005, **88**, 414–423 (the full text of the article available at: http://www.ias.ac.in/currsci/feb102005/415.pdf).

ACKNOWLEDGEMENT. I am grateful to Nithin Nagaraj for many discussions on cryptography and for his critical comments on the manuscript.

Received 21 February 2007; accepted 8 March 2007