This essay was mainly written to motivate the students of mathematics and computer science into research in cryptology. It was published in *Point: Journal of Mathematics, Department of Mathematics, Sree Chaitanya College, Habra, India* (Sanatan Paul et al., eds.), Sept. 2005.

**Cryptology:**

**A Mathematician’s Quest for Making and Breaking the Code**

Souradyuti Paul

Katholieke Universiteit Leuven, Dept. ESAT/COSIC, Kasteelpark Arenberg 10, B-3001, Leuven-Heverlee, Belgium

Souradyuti.Paul@esat.kuleuven.be

One of the most delicate mathematical thinkers of the past century G. H. Hardy once lamented in his book *A Mathematician’s Apology*, written in 1940, that pure mathematics had no utilitarian value and would never benefit the society. The book is, in fact, a profoundly poignant tale of a Cambridge number theorist who, because of his old age, was unable to practice the art whose beauty had captivated his entire self since his boyhood days. Hardy, who dedicated his whole life to the development and promotion of pure mathematics, died in 1947. Thirty one years later, in 1978, three computer scientists from the Massachusetts Institute of Technology (MIT) - Ronald Rivest, Adi Shamir and Leonard Adleman - used the so called hardness of a number theoretic problem - *the factorization problem* (about which I will talk later) - to design a method to exchange confidential information over the Internet. Nowadays, as *Internet banking*, *Electronic money transfer* (e.g. payment through credit cards), *Internet Shopping* (e.g. ordering books on the amazon.com) are being widely used all over the world, the science of secure communication on the digital networks has evoked unprecedented interest and enthusiasm in both industry and academia. Imagine the dreadful scenario where you purchased a fashionable footwear at one of the shoe-stores at Shyambazar using your credit/debit card but even before you reached home at Salt Lake, to your greatest shock, you found that your bank account had been emptied by a hacker who, taking advantage of the lack of security of the system, successfully deciphered the secret code of the card. In certain applications, the only indispensable way of ensuring secure information transfer on the Internet is to use the famous RSA Cryptosystem, the security of which is solely based on the age old hardness of factoring large integers into its prime factors. RSA is named after its
discoverers Rivest, Shamir and Adleman. Apart from revolutionizing the science of secure
Internet communication, the RSA Cryptosystem has secretly created a historical landmark;
it has liberated pure mathematics, particularly number theory and other related branches
such as algebraic geometry, combinatorics, from the curse of being dubbed useless in human
welfare, despite remaining the darling of many of the fertile brains of all time. There are
no other engineering or technological applications in the history of human civilization where
number theory is used to such an advantage without any alternatives. What’s more, in
recognition of the cryptosystem’s natural mathematical elegance and its huge contribution in
secure data transfer on the Internet, the trio Rivest, Shamir and Adleman have been jointly
honored with the Turing Award (also known as the Nobel Prize for computer science) in
2002, as long as twenty four years after their discovery. Had Hardy lived till today, surely he
would have considered reorganizing his book including the title too.

The main purpose of this article is to bring to the notice of the students of pure mathe-
matics a branch of computer science, known as Cryptology, which, in the last two decades has
generated enormous interest among the number theorists, algebraic geometers, statisticians
and computer scientists alike. As I will restrict myself to a minimum of technicalities that
are barely necessary to expound the basic ideas of the subject, the essay may not be of much
interest to the serious researchers of this area.

Cryptology, in a word, is the science of hiding information from the unauthorized users,
but making them available to the legitimate ones. The word cryptology is derived from two
Greek words: kryptós which means ‘hidden’ and logos meaning ‘system’. Historically, the
art of secret writing is as old as the time of Pharaohs of ancient Egypt. Julius Caesar (100
BC – 44 BC) is known to have had used some specific techniques, known as Caesar cipher,
to protect messages of high military worth. In fact, the emergence of classical cryptology as
a well structured scientific discipline from a mere black art of Middle Ages has been greatly
influenced by the growing military needs of modern times to disguise sensitive information
from the enemy. It is still now debated whether the breaking of the German secrecy system
Enigma by the Allied cryptologists (one of them was the famous British mathematician Alan
Turing who is deemed the father of modern computer science) had shortened the duration of
the World War II by at least a couple of years. Interested readers are highly recommended
to look at the classical book The Codebreakers by David Kahn that traces the evolution of
cryptology since the dawn of civilization till the age of the modern computer science.

At the heart of cryptology, there are two mathematical functions \( E \) and \( D \) which are used
for encryption and decryption respectively. Another component, known as the secret key \( k \),
also plays an important role in cryptologic applications. The functions \( E \) and \( D \) are publicly
known but the secret key is known only to the sender and the receiver of the message. Let
us take an example. Suppose Alice wants to send a confidential email to Bob through an
unprotected path which can be accessed by all. In other words, the email sent by Alice to Bob
can be captured midway by a third party whose name is, say Oscar. What Alice (the sender)
essentially does is encrypt the email (technically called message) using the function \( E \) and a
secret key $k$. Thus, if the message is $x$ then Alice generates the encrypted code $E(k, x)$. The encrypted code $E(k, x)$ is then sent out on an insecure channel. At the receiving end Bob gets $E(k, x)$ and decrypts it to recover the original message using the function $D$ and the shared secret key $k$, i.e., by performing the operation $D(k, E(k, x)) = x$. When Oscar captures the encrypted message on the way, he tries to recover $x$ from $E(k, x)$ without the knowledge of the secret key $k$. The system fails if Oscar succeeds. The system is considered secure if the recovery of the original message from the encrypted message is ‘impossible’ without the knowledge of the secret key.

The research in cryptology centers around designing the mathematical functions $E$ and $D$ such that the communication is secure in a manner argued in the previous paragraph. However, it is a pity that no cryptosystem has so far been proved to be secure!! Scores of cryptosystems are proposed at the conferences and in the journals every day and they are broken, often, more quickly than they are designed. This alternate making and breaking of secrecy systems, unlike any other scientific research, keep the practitioners of this subject always on adrenalin rush.

One of the most widely used cryptographic algorithms, known as the DES Cryptosystem (abbreviation for Data Encryption Standard) designed by a team of IBM and selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, was once thought to be unbreakable for a long time. However, new mathematical techniques were developed and the cipher was broken by the methods known as Differential and Linear Cryptanalysis in 1992-93 by Eli Biham, Adi Shamir (Israel) and Mitsuru Matsui (Japan). After its failure the DES Cryptosystem is being gradually replaced by a new standard called the AES Encryption Algorithm (Advanced Encryption Standard), also known as Rijndael named after its two Belgian designers Vincent Rijmen and Joan Daemen of the Katholieke Univeriteit Leuven. Till now, barring a few occasional rumors, AES-Rijndael has survived all attacks and is considered to be exceptionally strong. However, in cryptologic world, the borderline between the dead and the alive is so thin that one cannot really rest in peace, particularly when this cipher is being dissected day and night by the smartest of the mathematicians and engineers the world over. The greatest motivation for targeting AES-Rijndael is that, after a worldwide competition of four years it has been accepted as a standard to be used in most of the commercial and governmental applications and therefore, breaking this cipher will make a cryptographer world-famous instantly.

As explained before, one way of securing cryptographic systems is to make the sender and the receiver share the same secret key $k$. However, it is often difficult for the receiver and the sender, located wide apart on the globe, to share the same secret key because the transfer of the key over the Internet makes it prone to capture by a third party. Technically, how can one design the functions $E$ and $D$ (as explained before) securely without the shared component $k$? The problem, of designing a secure cryptosystem without the condition of sharing the key, became a hot pursuit by the mathematicians in the early 1970’s. Whitfield Diffie and Martin Hellman in 1976, initiated a new direction in cryptography by inventing Public-key
encryption algorithm where it was no more necessary to share a key in secret communication. Shortly afterwards that landmark invention three MIT scientists Ronald Rivest, Adi Shamir and Leonard Adleman, in 1978, stunned the world by first giving a practical algorithm – RSA Encryption Algorithm – for a Public-Key Cryptosystem which is based on the hardness of a well known number theoretic problem of factoring large integers. In the author’s opinion this is the most significant breakthrough in the history of cryptology. Discussion of how this type of cryptosystems works is out of the scope of this article, however, the underlying mathematical problem, which is the lifeblood of this type of secrecy system, can be described in a few words. If \( l = mn \) where \( m \) and \( n \) are large prime numbers then, given \( l \), it is hard to determine the prime factors \( m \) and \( n \) quickly. Countless mathematicians have spent their entire lives in developing fast methods to factor arbitrarily large composite numbers. If they ever succeed the RSA Cryptosystem will be sent to the grave in a moment. That is where cryptography is married to number theory, the queen of mathematics. Many similar proposals also came on the heels of RSA Algorithm. The other RSA-like encryption systems are the El Gamal cryptosystem and the Elliptic curve cryptosystem both of which are based on the hardness of the discrete logarithm problem. The discrete logarithm problem is: given two elements \( g \) and \( h \) in a finite group \( G \), find an integer \( x \) such that \( g^x = h \). For example, the solution to the problem \( 3^x \equiv 10 \pmod{17} \) is 3, because \( 3^3 = 27 \equiv 10 \pmod{17} \). This problem is known to be hard for large groups. Many other algebraic hard problems such as solving multivariate polynomial equations are, nowadays, being investigated for the purpose of information hiding.

Today the scope of cryptology is not limited to data encryption and decryption only. The ambit of the subject is in the continuous process of expansion and modification. Another interesting subarea of cryptology is the design of signature schemes where it is required to electronically sign a long message-text with a very short signature. Suppose, by sending an email to a bank you request for a transfer of money from your account to another. It is therefore, very important for the bank to make sure that the request come from a legitimate account holder. Cryptographic signature schemes address these security issues. There are many other application areas of cryptology such as data authentication (i.e., if the original message is distorted in transmission), secure communication among many users rather than only two, however it needs a separate occasion for elaborate discussion of them.

It is impossible to explain the subtleties and the sophistication of the entire gamut of Cryptology within a limited scope as this. The whole idea of this essay is to give to the interested pupils a flavor of a subject that combines many subareas of mathematics and statistics such as combinatorics, Boolean algebra, number theory, discrete mathematics, computational complexity theory, probability theory, algebraic geometry and many more, like no other applied science. The subject is inundated with loads of open problems and conjectures to excite the fancy of the theoreticians, on the other hand it gives immense pleasure to the engineers to engage their skills into practical applications. The readers who have come up to this point and are still eager to learn more about the rudimentary ideas of the subject are
kindly advised to obtain the book *Handbook of Applied Cryptography* by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. The entire book is freely available online at http://www.cacr.math.uwaterloo.ca/hac/. As a final message I would again like to remind that, if you are ever amazed by the beauty of mathematics you can no longer stay away from the challenges of making and breaking the codes – a quality that makes cryptology an evergreen subject.