International Journal of Pure and Applied Mathematics
Volume 83 No. 5 2013, 631-633
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v83i5.3
ijpam.eu

CRYPTOGRAPHY AND STEGANOGRAPHY IN INFORMATION SECURITY

P.K. Saxena
Director SAG, DRDO, Delhi

Invited Talk
NCRTMSA – 2012

*

The history of development of civilization in different parts of the world is quite old. They grew mainly near natural surroundings, where water and natural vegetation was available in abundance. Most of developments at these localized pockets took place in isolation, but they had many commonalties as communicating with each was also emerged a requirement..

The natural process of evolution took place over long period of time and the early man learned how to live in groups and communicate among themselves. They used smoke, fire, beating drums and pipes etc. to alarm their fellows from possible threats and for some other such purposes. But when they failed to have written records, the man developed some symbols in the form of line, scratches and figure associating meanings to them according to their need and perception. Thus came the cuneiform and hieroglyphic writings of ancient time. Many proofs have been found during excavations in the form of clay tablets or inscriptions in stones. This was around 4000 - 5000 years BC, which could be treated an era of beginning of scripts in an organized manner.

As the civilization grew, man became a part of bigger society and they started making laws for them to follow. The concept of leader or ruler or king and their subjects came into existence and their came a need for hiding information from undesired persons. The skill on spying, sending messages of secret, executing plan to consolidate their holds on kingdoms or to overthrow kings and ruler started developing. Thus came the art of secret communication in existence.

There were primarily two ways of securing a message: (i) hiding the text written in script available and send it to the receiver secretly hiding it through some means and (ii) converting the text itself to a form making it unintelligible for unauthorized interceptor where as enabling the intended receiver to recover the original text using 'key' or 'method' used there in. The first of these arts is known as 'Steganography' where as the second is known as 'cryptography'.

During old days, Steganography existed in many forms such as hiding messages on shaven heads of the slaves or engraving messages under the skins of the killed rabbits and thus delivering messages to intended persons, deceiving the soldiers etc. There are evidences where Germans used newspapers for hiding their messages through micro dots printed under the letters which constituted the secret messages for their comrades. Use of Grills, where windows were cut in rectangular plates to read messages hidden in some other message written on the plate of the same dimensions was also a part of this art.

However, with development of mathematics and other ingenious thinking, Cryptography took over since it came handy in the form of electro-mechanical devices that could be interfaced with tele-printers and later with telegraphs directly for sending secret messages. Today, Cryptography is not just an art but a well developed science based on highly complex mathematical principles for providing confidentiality to the contents to be communicated. Both the world wars witnessed a large-scale use of cryptographic equipments along with state of art weapons [1].

With the development in electronics and microprocessor technology, computers became smaller in size, more powerful and suitable for general-purpose applications. Different features for handling images, audio and multimedia were incorporated in computers to make them friendly and simpler to use. Today using a personal computer, browsing the internet and sending voice mails have become easy and do not require any professional assistance.

In the present digital era where enormous amount of information flows in bits and bytes with global connectivity, the horizon of security has broadened and is not limited to securing just the contents but also addressing issues such as authentication, data integrity, availability [2]. With the increasing bandwidth and data rates, it has become very easy to send images/pictures across, both of which have a very large redundancy. It has been found recently that such redundancy could be used very scientifically for hiding information without being easily detected. And thus the art of steganography has emerged as a new science for secret communication, which plays a major role in achieving information security goals, like cryptography [3]. Increase in voice traffic over conventional and packet switched networks has generated a golden opportunity for the audio steganography community [4].

In this talk we discuss developments that have taken place in Cryptography as well as Steganography and describe broad principles that are prevalent in present day systems.

References

[1] D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.*

[2] W. Stallings, *Cryptography and Network Security.*

[3] Fabien A.P. Petitcolas, Ross J. Anderson, Markus G. Kuhn, Information hiding – A survey, In: *Proceedings of the IEEE*, Special Issue on *Protection of Multimedia Content*, **87**, No. 7 (1999), 1062-1078.

[4] W. Mazurczyk, K. Szczypiorski, Steganography of VoIP Streams, *OTM 2008* (Ed-s: R. Meersman, Z. Tari), Part II, LNCS 5332 (2008), 1001-1018.