Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 03-05, DOI: 10.14429/dsj.62.1434

Guest Editorial

CRYPTOLOGY AND COMMUNICATION SECURITY

Cryptology is the scientific study and practice of making (cryptography) and breaking (cryptanalysis) of codes and ciphers. Code is a system of rephrasing parts of normal language meaningful with certain standard groups or symbols. Whereas cipher is a system of transforming fixed length group of language symbols at normally the single character of alphabet into code alphabet character. The science of making communications unintelligible to all except the intended recipient(s) is known as cryptography. Until recently cryptography has been of interest primarily to the defence and diplomatic personnel of governments, guarded over and directed by their national crypto logic services. But now a day's It has become the part of our daily life viz. providing electronic security to our house and offices, use of ATM, Credit Card, Smart Cards and RFID tags, etc. all of them needs cryptography in some form. Private business sectors, terrorist outfit and electronic communication agencies are using cryptographic methods to keep their data, valuable information and their developmental activities secret until they feel that it is important for their commercial interest, etc. Many cryptographic devices and algorithms are available for non-governmental application, such as M209, Hagelin machine, DES, AES, Public key cryptography (RSA system), and also varieties of crypto algorithms are available in the open literatures for any interested agency to implement their own system of encryptions.

The chronological development of the system of secret communication using symmetric key cryptography (where encryption and decryption keys are same, shared among the users securely by trusted means) can be broken into five stages.

1. Ancient hieroglyphic system of writing by Egyptians, shorthand invented by T. Shelton[1], steganography (microdot, invisible ink) and physically concealed messages such as inscribing the message on the shaven head of a slave then sending the slave to deliver the message after his hair had grown back again, etc. do not provide any practical security. Majority of such stories dealing with secret writing are concerned with the artfulness with which the message is concealed or conveyed and have no distant relation with cryptography. Physical security is something which go slow automatic degeneration and also there is slow communication. The speed with which communication is now possible makes such method inefficient, even though during the world war-I it was the practice to send spies across the enemy lines for communicating the messages using steganography.
2. Modern definition of cryptology states that communication is to be sent through open transmitting medium, which is accessible to all, but the communication should be unintelligible to unwanted or unauthorised persons. Information is to be intelligible only to the intended address. So the messages have to be intrinsically built-in made secure, which is achieved by certain mathematical transformation. Since the protection and security of communication play an important role particularly in military and political circles, the system of encryption should be such that it can be set right quickly and accurately. The basic principles involved in cryptography are transposition, substitution or both. In transposition, individual letter changes their relative position but not their identity. Scrambling of letters are done by using geometric patterns and route transcription, message is written along one route and its cipher version is obtained through another route, plain text is obtained by reversing the above procedure, To make it sufficiently secure in place of geometrical pattern, a high order column can be used (columnar transposition). Fixed segment transposition makes the system more secure, since for each segment, we use different permutation. The number of permutation depends on the segment size, i.e. key length which is kept secret. The units of the plain text retain their relative position in substitution ciphers but do not retain their identities. There are three methods of substitution encipherment namely, single alphabet substitution: every letter of plain text gets only one letter of cipher text, polyalphabetic substitution: every letter of plain text gets more than one cipher alphabet and polygraphic substitution: for digraphs or trigraphs of plain text cipher digraphs or trigraphs are made.
3. Transposition ciphers can be made more and more secure, but the complexity achieved in security is not commensurate with the efforts put in, although fixed segment transposition is used now a days to maintain the security of communication in speech secrecy system. Historically the advent of machine cipher favored substitution rather than transposition. The most widely used machine is M-209 and its derivatives. Such system can be solved if we have either sufficiently long cipher text or some portion of plain text as well as its cipher text. The Enigma and Typex which are world war-II vintage rotor based systems are still supposed to be the considerable secured cipher machine till today. These systems produce a very complicated set of polyalphabetic substitution generated with the help of randomised permutations through an electro-mechanical rotor system. Most of the mechanical/electro-mechanical machines are not solvable in real time because of its versatility and maneuverability.
4. C.E. Shannon[2,3] in his revolutionary paper has shown how cryptography could be put on a sound mathematical base. Shannon's ideas for introducing versatile cipher system have been realised with the advent of microelectronics

in 1960s. It has been recognised that cryptography and cryptanalysis are essentially very highly mathematical and statistical disciplines and also embrace a number of scientific fields; notably computer science, electronics, communications, and very advanced modern mathematics. Present day cryptosystems are based upon modulo-2 addition of stream of binary digit sequences generated by mathematically designed crypto primitives. The generated sequence should be of very large period, highly complex in terms of predicting the forward or backward bits, not better than chance probability, with any amount of bit segment in hand. It should have sound statistical properties (proper distribution of ones and zeros, and good autocorrelation properties) and very large variability to make it impregnable. These new types of complex devices can provide a much higher level of security in comparison to all earlier systems and also satisfy all the military prerequisites for secret communication notably, simplicity, rapidity, practicability, accuracy and economy.

5. In 1950's, cryptography came in for open discussion and the first encryption standard, i.e. data encryption standard (DES) got universal acceptance by financial community. Single-key DES are vulnerable to attack but if double-length keys and unique keys per transaction is implemented it can resist real time attack. Triple DES is still in use but due to current computational power availability the DES can be attacked simply by brute force making it ineffective for real time use. And hence in the year 2000 new standard for data encryption namely advance encryption standard (AES) has been announced after rigorous analysis of many algorithms submitted by designers from all over the globe.

Symmetric key cryptography have some inherent weakness not in terms of security but in terms of uses like problem of key exchange through trusted courier, authentication, non repudiation, data integrity and digital signature, etc. To overcome all this in late 1950's Diffie, and Hellman introduced revolutionary idea of cryptography, where encryption method and part of the keys are made public and the remaining parts of the keys are kept secret. In this way public key cryptography was born, the first well known public-key cryptosystem is RSA. The security of the system depends upon the prime factorisation of the large integers (about 200 digits). The above encryption procedure has not been used by traditional military users because no definite proof of the computational infeasibility has been achieved and someone in future can develop an efficient algorithm for the factorisation of special type of large integers. There are several public key cryptographic schemes based on discrete log problem, elliptic curve and mathematical one way functions, which may not be solved in real time by available computing power in hand.

In the continuous fight for supremacy between the cryptographer and the cryptanalyst, it has been observed that cryptographer is always in a position to provide certain minimum security of systems. Present day technology favours the cryptographers, who have forced the cryptanalyst to adopt either of the following two approaches for analysis:

(i) System independent approach

(ii) System dependent approach.

In the first approach, the cryptanalyst works purely on his experience, heuristics, and knowledge gained during the process of analysis. Sometimes the availability of the following provides him more information to work under certain assumptions, viz. possession of several possible pairs of plain and cipher texts, availability of two messages on the same key or availability of same message on different portions of the same key.

In the second approach, the cryptoanalyst works under the assumptions that he possesses the knowledge of cryptosystems used by adversaries, the language of enemy's encipherment and the philosophy of encryption, decryption with knowledge of key space and there exists linear separability through the statistics of cipher text among them.

In the present special issue, some of these technologies have been presented in eight research papers out of which one is survey paper and another is short communication while remaining six are full length paper. A brief outlines of all these papers are given here.

Srinivasan and co-authors in their paper, 'Measuring Diffusion in Stream Ciphers using Statistical Testing Methods' have presented two modified statistical testing methods for testing strict avalanche criteria (SAC). They have experimented on the key stream of two eSTREAM candidates namely Trivium-80 and Grain-80. These candidate output key streams are not passing these tests and hence there is a need of further analysis of Trivium-80 and Grain-80.

Steganography is an ancient method of concealing information from being intercepted during communication. Earlier methods like invisible ink, microdot etc. are no more being used. During 1990's, concealing information in images without changing the image quality were proposed and used intelligently. In the paper, 'Steganographic Techniques of Data Hiding using Digital Images' by Babloo Shaha, survey of existing steganographic algorithms is presented. This paper provides a good overview of the prevalent methods for steganography.

In the paper, 'Performance Evaluation of Exponential Discriminant Analysis with Feature Selection for Steganalysis' Rajput and co-authors have presented that how the recently proposed exponential discriminant analysis (EDA) in conjunction with feature selection techniques is found to be more effective for steganalysis. Steganalysis involves two steps first to discriminate between stego and non-stego images and then to exploit stego images for relevant information. Detection of steganographic algorithm used is another important step. The techniques described in the paper will be extremely suitable for steganalysis task.

Garga and co-authors in the paper, 'A Flexible Crypto-system Based upon the REDEFINE Polymorphic ASIC Architecture' have presented the REDEFINE architecture as a framework that can support various crypto algorithms to meet the requirement of more than one crypto algorithm to achieve the overall security. The presented architecture framework can also work as crypto accelerator capable of accelerating even 'run-time' defined crypto application. The framework is also capable of preventing side channel attacks by running a dummy program alongside the main program, so that the electromagnetic radiations from the device get obfuscated.

Data encryption standard (DES) has been the open domain cryptographic standard till late 1980's. The availability of fast computing power and high storage made DES insecure and hence a new cryptographic standard advanced encryption standard (AES) have been accepted after rigorous scrutiny. Algebraic construction of S-boxes used in AES has been studied and variations in the structure without affecting its security are proposed by Sinha and Arya in their paper, 'Algebraic Construction and Cryptographic Properties of Rijndael Substitution Box'.

Cryptanalysis is a herculean task in the absence of intelligence support and much needed side information like type of system and language of encryption used. Obtaining above mentioned information directly from cipher-text can be seen as system identification problem. Shri Kant in the paper, 'Classification Models for Symmetric Key Cryptosystem Identification' has selected and developed classification models, viz. statistical classification, support vector method, artificial neural network, and Hidden Markova's Model in a generic fashion, so that they can be tuned for any applications. Interesting results have been presented for symmetric key crypto system identification.

Suresh and Madhavan in the paper, 'Image Encryption with Space-filling Curves' have proposed an encryption techniques that uses fractal structures to encrypt salient components of images in such away that salient (encrypted) and non-salient (unencrypted) looks totally encrypted and do not allow the cryptanalyst to retrieve any meaningful information. This technique is extremely useful for multimedia encryption because conventional encryption algorithms are usually applicable for text data.

Being a challenging area and with very few institutes in the country working in the subject of cryptology, quite satisfactory number of papers have been received. After review only eight papers could be accepted. There is a fair representation of cryptographic and cryptanalytic techniques presented in this special issue on Cryptology and Communication Security. I am thankful to all the contributors for submitting their research work for this special issue of *Defence Science Journal.* I am also thankful to the researchers whose paper could not be accepted.

I am indeed grateful to the reviewers for their time and providing expert comments for the improvements and revisions of these papers by the authors. I am also grateful to Editor-in-chief for prompt approval of my proposal to bring out a special issue on subject like Cryptology and Communication Security. Finally, I would like to thank Director, DESIDOC and his team for their untiring effort in bringing out this special issue.

References

1. Shelton, T. Tachy-graphy. Ed 6th. 1620.
2. Shannon, C.E. A mathematical theory of communication (Pt I). *Bell Syst. Tech. J.*, 1948, **27**, 379-423.
3. Shannon, C.E. A mathematical theory of communication (Pt II). *Bell Syst. Tech. J.*, 1948, **27**, 623-56.

Dr Shri Kant
Sc 'G' & Coordinator
Joint Cipher Bureau
Deptt of Defence R&D
Metcalfe House,
Delhi -110054