PhD Thesis

Studies, Design and Development of Network Security Enhancement Services using Novel Cryptographic Algorithms

ABSTRACT

Internet today has become a vital part of day to day life, owing to the revolutionary changes it has brought about in various fields. Dependence on the Internet as an information highway and knowledge bank is exponentially increasing so that a going back is beyond imagination. Transfer of critical information is also being carried out through the Internet. This widespread use of the Internet coupled with the tremendous growth in e-commerce and m-commerce has created a vital need for information security.

Internet has also become an active field of crackers and intruders. The whole development in this area can become null and void if fool-proof security of the data is not ensured without a chance of being adulterated. It is, hence a challenge before the professional community to develop systems to ensure security of the data sent through the Internet.

Stream ciphers, hash functions and message authentication codes play vital roles in providing security services like confidentiality, integrity and authentication of the data sent through the Internet. There are several such popular and dependable techniques, which have been in use widely, for quite a long time. This long term exposure makes them vulnerable to successful or near successful attempts for attacks. Hence it is the need of the hour to develop new algorithms with better security.

Hence studies were conducted on various types of algorithms being used in this area. Focus was given to identify the properties imparting security at this stage. By making use of a perception derived from these studies, new algorithms were designed. Performances of these algorithms were then studied followed by necessary modifications to yield an improved system consisting of a new stream cipher algorithm MAJE4, a new hash code JERIM-320 and a new message authentication code MACJER-320. Detailed analysis and comparison with the existing popular schemes were also carried out to establish the security levels.

The Secure Socket Layer (SSL) / Transport Layer Security (TLS) protocol is one of the most widely used security protocols in Internet. The cryptographic algorithms RC4 and HMAC have been in use for achieving security services like confidentiality and authentication in the SSL / TLS. But recent attacks on RC4 and HMAC have raised questions about the reliability of these algorithms. Hence MAJE4 and MACJER-320 have been proposed as substitutes for them. Detailed studies on the performance of these new algorithms were carried out; it has been observed that they are dependable alternatives.

The results of the investigations carried out as well as the concepts in the algorithms developed were communicated and published in journals (six papers) and presented at international conferences (three papers).

PhD Thesis No: 6
Ms. Sheena Mathew