EVALUATION AND ANALYSIS OF SYMMETRIC CRYPTOGRAPHIC ALGORITHMS FROM CRYPTANALYSIS PERSPECTIVE

ABSTRACT

of the Ph.D. Thesis

Submitted To
JAMIA MILLIA ISLAMIA
for the award of the
Degree of Doctor of Philosophy in

Submitted by

NEETA WADHWA

DR. S. Zeeshan Hussain
Supervisor
Jamia Millia Islamia
New Delhi

DR. S.A.M. Rizvi
Co-Supervisor
Jamia Millia Islamia
New Delhi

DEPARTMENT OF COMPUTER SCIENCE
Faculty of Natural Sciences
JAMIA MILLIA ISLAMIA, CENTRAL UNIVERSITY
NEW DELHI, INDIA
November 2013

ABSTRACT

Keywords : Symmetric Cryptography, AES, RC5, Peripheral Encryption, Keyboard, Thermal Printer

ABSTRACT

Information Security becomes the basic necessity of the digital world and has attracted the attention of the entire planet. Secure communication is an indispensable requirement in the present world of e-transactions and e-interactions. Cryptography is one of the most important techniques that help to meet this need.

Rapid innovations continuously generate new technologies with new vulnerabilities. The huge amount of information is daily travelled across the Computer Networks. Many techniques and measures are implemented for its security at every layer of the TCP/IP communication model. All the ongoing significant researches focus on the security of the information travelling across these insecure networks and its secure storage.

The substantial number of published researches and literatures has described the implication of Symmetric cryptographic algorithms to encrypt various kinds of data in different environments. The present study also tries to add some new significant results to the current research by analyzing various Symmetric Cryptographic Algorithms DES, AES, TwoFish, BlowFish, CAST from the Speed versus Security perspective in varying environments.

Information security threats can also come from an unlikely source like the most sensitive information as passwords, credit card numbers, bank account numbers etc. can be very easily tampered over while transmitting between the computer and its own peripherals, with the help of simple devices like Keyloggers. Keyloggers can be used as tools to steal confidential personal information of users in commercial, government, political espionage and financial sectors like banks.

Peripherals are the devices that transmit data to and from the computer without any processing. All the sensitive data entered through the keyboard and similarly printed through the printers. While this transmission, all kinds of data can be attacked by very simple means and without any technical expertise.

A above stated research gap still exists and there is a need to apply measures to secure the communication between Computer and its peripherals; to the best of our knowledge there has not been any study that specifically address and investigate the implication of various Symmetric encryption standards for encryption and decryption facilities in computer peripherals. The present research seeks to fill the said gap of incorporating encryption capabilities in the two peripherals of the computer: Keyboard and Thermal Printer.

A new protocol is proposed and implemented to secure the communication between computer and its peripherals. An encryption system called Peripheral Encryption System (PES) is developed in which encryption / decryption is done with two standard symmetric encryption algorithms AES and RC5. The system is designed to secure the communication between the computer and its serial peripherals (Keyboard and Thermal Printer). The performance of the AES and RC5 is analyzed on the basis of various parameters like encryption and decryption speed, memory requirement and number of machine cycles.

The present thesis seeks to address how the information can be secured that travels between the computer and its serial peripherals. The serial peripherals are usually limited memory devices. Thus a good encryption system should need less memory and also it should not affect the performance of peripherals. A new algorithm called Peripheral Encryption Algorithm (PEA) is proposed and implemented in PES. Simulations prove that PEA is better than AES and RC5 both in terms of speed and memory requirement.