PERFORMANCE ANALYSIS OF EXISTING PUBLIC KEY CRYPTOSYSTEMS

A PROJECT REPORT PRESENTED BY

CHAMPIKA SUDARSHANIE MEGASOORIYA

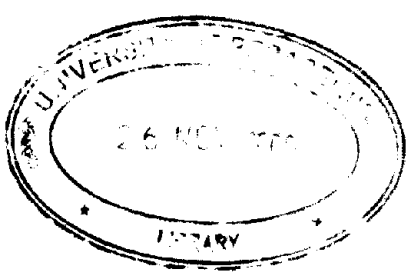
to the Board of Study in Statistics & Computer Science of the
POSTGRADUATE INSTITUTE OF SCIENCE

in partial fulfillment of the requirement
for the award of the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

of the

UNIVERSITY OF PERADENIYA
SRI LANKA
2008



PERFORMANCE ANALYSIS OF EXISTING PUBLIC KEY CRYPTOSYSTEMS

G.M.C.S. Megasooriya
Thalgamuwa
Dewanagala

Today, almost all people throughout the world use computers and computer networks to store bulk of their valuable data and to communicate with each other as a tool for commerce. Data traveling through insecure channels are always subjected to eavesdropping or injecting. This is the major security problem which is to be considered for privacy and authentication of the communication. Crypto systems are widely accepted solution for this problem.

In this research we investigated existing public key cryptosystems and analyzed their performances. Since public key cryptosystems are widely accepted and use, the work was limited to five public key cryptosystems. The performance of each system was analyzed by means of three factors: key size, computational overhead and computational complexity.

The result of the performance analysis was also presented. The results indicated that it is hard to conclude that one system is superior to others in all situations. However some systems are better than the other in certain situations.