

3837890 SCCS/M : MAJOR : Computer Science : M.Sc. (Computer Science)
KEY WORDS : SECURE E-MAIL/ INFORMATION THEORY
PEERAWIT WANNAWITTAYAPA: TRUSTED ELECTRONIC MAIL
SYSTEM ON INTERNET. THESIS ADVISOR: DAMRAS WONGSAWANG Ph.D.,
SUPACHAI TANGWONGSAN Ph.D. 94 P. ISBN 974-662-552-7

Normally, sending E-mail via Internet system uses Simple Mail Transfer Protocol (SMTP) to manage transferring data. This protocol has been designed for general application and it is not adequate for use in applications requiring high level security. Thus, problems often occurred regarding security issues, for example, reading, imitating, modifying E-mails by unauthorized people. These are serious problems causing decrease in E-mail usage. Presently, new systems of sending E-mail have been developed and implemented for higher security, such as S/MIME, PEM, and PGP. However, these systems lack management, inspection, and verification.

This thesis proposed the secure E-mail system, called S-mail, having very high level security. S-mail focus on security of transferring E-mail via Internet. It used the concept of central security control, which provides better security than the distributed one. Namely, a server will manage security of the system, including communication services to users. Then, it encodes data by symmetric and asymmetric cryptosystems. This approach helps improve the management, inspection, and verification of security in the emailing system. This will increase confidence of sending importance messages. S-mail provides many security services such as self-destruct E-mail, anonymous E-mail, etc. These services are not provided in other systems. Experimentally, S-mail is one of the highest security E-mail systems. This system can be used for practical application. This thesis presents the model and structure of S-mail in detail. The implementation and experimentation are also presented. The results are discussed and evaluated and the improvements are suggested.