A Diophantine Equations Based Cipher for Internet EDI Security in Macau

by

Fei Chun, Ma

A thesis submitted for the degree of
Master of Science in Electrical & Electronics Engineering
at The Faculty of Science & Technology, University of Macau
in July 1997

Abstract

Driven by the fast-growing world-wise deployment of Electronic Commerce in recent years, a lot of ciphers have been developed in order to allow these electronic commerce transactions transferred securely in the open network like Internet. As more users adopt and the technology advances, electronic commerce via open network gain the global acceptance, in particular, special consideration of Internet EDI to be one of the future business basis is now changing the global business cycle.

In Macau, there are only two organizations/networks (University of Macau and Companhia de Telecomunicações de Macau S.A.R.L.) support local resident getting wired into the Internet. With this simplicity, this may induce a very interesting and promising result when dealing with the local internal trading electronic commerce in Macau. In fact, this simple local network users' characteristics of Macau facilitates the analysis of Internet EDI nature owning to an inter-connection between two organizations.

All open networks have the same disputes of high security, fast data transmission, optimal bandwidth utilization etc. and Internet is no exception. Specially, the affairs of security and data transmission are two utmost important factors for the success of

Internet EDI. With the advent of coupled development of security schemes and data transmission, Internet EDI security problem can be traditionally tackled by applying the symmetric and PGP type asymmetric encryption algorithms subject to the practical software/hardware consideration.

In this thesis, we proposed Macau Internet EDI security scheme having the basic methodology as mentioned above but with the replacement of PGP type asymmetric encryption by Diophantine equations based cipher. This scheme takes full advantage of the cipher's simplicity on key construction and the NP-complete property in order to speed up the encryption process and to secure the session key of the proposed scheme. On the other hand, thanks to the simple nature of Macau Internet, this allows the sufficient network traffic measurements done for the verification of the proposed scheme with ease. Indeed, the proposed scheme has the superior performance in encryption and maintains an acceptable security level. It should be emphasized that the combination of proposed security scheme and the simple nature of Macau Internet can contribute to the success of electronic commerce for Macau in future.

In order to clarify the theory, some experimental Internet EDI messages have been simulated within the Internet network domain of the University of Macau and that of the Companhia de Telecomunicações de Macau S.A.R.L.. This scheme reports not only the overall good security when compared with the traditional PGP based cipher but also obtains about 4 times faster encryption time. The good agreement with theory both in security and encryption process is reported and this shows the usefulness of the scheme in Macau Internet EDI.

Key words

Internet EDI, symmetric cipher, asymmetric cipher, session key, public key, private key, Diophantine Equations, NP-Complete