Title: A STUDY ON HYBRID CRYPTOSYSTEM: PRETTY GOOD PRIVACY (PGP)

By

HILMI BINTI HJ HARUN

A project paper submitted to
FACULTY OF INFORMATION TECHNOLOGY AND QUANTITATIVE SCIENCES
UNIVERSITI TEKNOLOGI MARA

In partial fulfillment of requirement for the
BACHELOR OF SCIENCE (Hons) IN DATA COMMUNICATION AND NETWORKING

Major Area : Network Security

UNIVERSITI TEKNOLOGI MARA
SHAH ALAM, SELANGOR
OCTOBER 2003

ACKNOWLEDGEMENT

In the name of Allah, who is the Gracious, Most Merciful, Praise to Allah, the one and only, for giving strength and inspiration necessary to accomplish the impossible.

The study presented in this dissertation could not be conducted without the support, encouragement and cooperation of many people. First and foremost, I would like to express my deepest gratitude to my supervisor, Pn Rosanita Adnan, who has always given me valuable advice, comments, ideas and encouragement for my thesis project. I am so grateful to have this opportunity to be under her supervision. Secondly, a special appreciation also to my lecturer for Research Project Course (ITT580), Assoc. Prof. Dr Saadiah Bt Yahya, for her guidance, encouragement, comments and ideas.

Thirdly, I am grateful to individuals that participated in my thesis project. I would like to dedicate my deepest appreciation to En Shukrey, who I met in Bincang.net and provided me with a basic knowledge of network security, also to Mr John (also known as august_1883), who I met in Yahoo! Chat (Hacker's Channel) and guided me through a simple chatting session and also keep giving me some information inside my e-mail boxes

My gratitude also extends to my friends, En and her fiancee, who helped checking the grammar in this report with their valuable suggestions for improvement. I also would like to thanks my family especially to my mother, who always motivate me and support me throughout this project. For my father, hopefully you will get well soon.

Last but not least, millions of thanks to all my friends who helped me along the way, due to complete this project. I wish them best of luck and thank you for everything. To all mentioned here, may Allah bless you all.

Hilmi Bt Hj Harun

TABLE OF CONTENT

ABSTRACT

Recent advances in computing power and recent interest in this privacy issue have led to the development of techniques to store sensitive information by using mathematics to encrypt and decrypt data. This technique enables us to store sensitive information or transmit it across insecure networks like the Internet so that it cannot be read by anyone except the intended recipient. This is what we called as cryptography.

With the combination of some cryptosystem such as conventional cryptography and public key cryptography, it produced a hybrid cryptosystem that we called a Pretty Good Privacy (PGP).

In this dissertation, we will only provide basic knowledge of PGP with simple explanation based on research done by security experts around the world. Throughout this thesis, we will look into the history of cryptography and the basic concept of how PGP works and its key components. We also will look into the possible attack available for key components used in PGP. At the end of this paper, we will discuss on possible attack of PGP in general without specifying on any key component used in PGP.