4037887 SCCS/M: MAJOR: COMPUTER SCIENCE: M.Sc. (COMPUTER SCIENCE).
KEY WORDS : FACTORIAL/POWER-DECIMAL SYSTEM/REASONABLY LARGE NUMBER.

NGUYEN BA HUNG: DESIGN AND ANALYSIS OF THE ALGORITHM FOR SOLVING FACTORIAL PROBLEM OF ANY REASONABLY LARGE NUMBER USING THE POWER-DECIMAL SYSTEM. THESIS ADVISORS: DAMRAS WONGSAWANG, Ph.D., SUPACHAI TANGWONGSAN, Ph.D., 68 p., ISBN 974-662-349-4.

The computation of factorial of any small number is relatively simple, straightforward and easy to implement. However, in practical applications, factorial of very large numbers is needed, e.g., the using of factorial to the compute very large prime numbers will be used in RSA, one of the most popular public-key cryptosystems currently in use. For such a case, the straightforward algorithm of factorial computation can not be applied due to the overflow problem.

This thesis is intended to study the factorial problem of reasonably large numbers. The factorial computation technique and algorithm called Fast Factorial Algorithm (FFA), was proposed, analyzed and devised. The FFA introduced the use of Power-Decimal System as its main representation of very large numbers that allows arithmetic operations to be done on a normal computer such as PC without the overflow problem. The complexity of FFA was analyzed and its performance was tested. The experimental results were presented and recommendation for practical use was also suggested.