شبكة المعلومات الجامعية

بسم الله الرحمن الرحيم

شبكة المعلومات الجامعية

التوثيق الالكتروني والميكروفيلم

شبكة المعلومات الجامعية

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

SPEEDING UP EXPONENTIATION ALGORITHMS FOR PUBLIC-KEY CRYPTOSYSTEMS

Presented By
Khaled AbdElrafea AbdElbari
B.Sc. in Computer Science, Ain Shams university

Supervised By
Assoc. Prof. Sameh Samy Daoud
Assoc. Prof. Hatem Mohamed Bahig

A THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS
FOR THE MASTER OF SCIENCE DEGREE
IN COMPUTER SCIENCE
TO
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
AIN SHAMS UNIVERSITY
CAIRO, EGYPT
2021

AIN SHAMS UNIVERSITY

Author:	**Khaled AbdElrafea AbdElbari** **B.Sc. in Computer Science, Ain Shams university**
Title:	**Speeding Up Exponentiation Algorithms for Public-Key Cryptosystems**
Division:	**Computer Science**
Department:	**Department of Mathematics**
Faculty:	**Faculty of Science**
Degree: **M.Sc.**	Year: **2021**

Contents

List of Tables

List of Figures

List of Algorithms

List of Abbreviations

We use the following standard notations with a short explanation.

Notation	**Explanation**
$AC(e)$	Addition chain of an integer e
B&B	Branch and Bound
BFS	Breadth First Search
CUDA	Compute Unified Device Architecture
DFS	Depth First Search
GPUs	Graphics Processing Units
Z_m	Set of integers {0,1,...,m-1} modulo a positive integer m