

COMP6720 Initial Report

Computer Methods for Factorization and Cryptography

Client: Dr. Richard Brent

Supervisor: Mr. Pascal Vuylsteker

Dr. Alistair Rendell

Student: Shi Bai

College of Engineering and Computer Science



ANU

Outline

- **1. Introduction**
- **2. Background**
- **3. History**
- **4. Challenges**
- **5. Classification**
- **6. Timetable and Lit Review Plan**
- **7. References and Resources**

Introduction

■ Concepts

■ 1. Integer Factorization:

breaks down a composite number into smaller divisors(primes).

■ 2. Cryptography:

It is about communication in the presence of adversaries.

Background

- Cryptography is used in many applications that touch everyday life:
 - ATM Cards
 - Electronic commerce
 - Military communication

History

■ Classical Methods

- Ancient - substitution ciphers
- WWII electromechanical rotor machine - Enigma

■ Modern Techniques

- symmetric-key cryptography (DES, AES)
 - share a single private key
- public-key cryptography (RSA, ECC)
 - public-key
 - private-key

Challenges

- Presume to be intractable without proof
- Computational cost
- public-key interception

Classifications

- Mathematics

- integer factorization
- discrete logarithm

- Algorithms

- symmetric-key (private-key)
- asymmetric-key (public-key)

- Applications

- encryption
- digital signature - sender authentication

Initial Timetable and Plan

- week3 methods of factorization
- week4 public-key app: RSA, Rabin etc.
- week5 discrete logarithm
- week6 public-key app: elliptic curves
- week7 generation of pseudorandom numbers
- break First Draft of Report
- week8 comments by supervisor
- week9 Refine
- week10 Refine
- week11 2nd Draft of Report
- week12 comments and Finalize Report

Reference and Resources

- 1. Mathematical Books
 - Hans Riesel, Prime Numbers and Computer Methods for Factorization, second edition, Progress in Mathematics, Birkhauser 1994.
 - Kenneth Ireland, Michael Rosen, A classical Introduction to Modern Number Theory, second edition. Springer-Verlag, 1990.
- 2. Cryptography Books
 - Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, October 1996.
 - A. Mollin, An Introduction to Cryptography, 2001, CRC.
- 3. Journal & Conference papers
- 4. Google and Citeseer



Thank You !