# Contents

1 Introduction 1

1.1 Historical Remarks . . . . . . . . . . . . . . . . . . . . . 1

1.2 Who Has Contributed? . . . . . . . . . . . . . . . . . . . 3

1.3 Who Should Read this Report? . . . . . . . . . . . . . . 6

1.4 Notice . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

2 Scope of the Workshop 11

2.1 The Rôle of Public-Key Cryptography . . . . . . . . . . 11

3 List of Topics Chosen Through Self-Assessment 13

4 Short Classification and Description of the Most Prominent Public-Key Systems 15

4.1 One-Way Functions . . . . . . . . . . . . . . . . . . . . 16

4.1.1 General Knapsacks . . . . . . . . . . . . . . . . . . . . 17

4.1.2 Discrete Log Problems (Diffie-Hellman, etc.) . . . . . . . 17

4.2 Trapdoor One-Way Functions . . . . . . . . . . . . . . . 20

Bibliografische Informationen
http://d-nb.info/920261795

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

4.2.1 Trapdoor Systems Based on Transformed NP-Complete Problems . . . . . . . . . . . . . . . . . . . . . . 22

4.2.2 Trapdoor Systems Based on the Decomposition of Algebras (RSA, etc.) . . . . . . . . . . . . . . . . . 24

4.3 Hash Functions . . . . . . . . . . . . . . . . . . . . . 27

**5 Public-Key Cryptography Depending on Computational Number Theory 33**

5.1 Factorisation of Large Integers . . . . . . . . . . . . . . 34

5.1.1 The Elliptic Curve Method . . . . . . . . . . . . . . . 35

5.1.2 Double Large Prime Variation of the Multiple Polynomial Quadratic Sieve . . . . . . . . . . . . . . . 36

5.1.3 The Number Field Sieve (NFS) . . . . . . . . . . . . . 40

5.1.4 Exploiting the Power of Distributed Computing . . . . . 44

5.2 Discrete Logarithms . . . . . . . . . . . . . . . . . . 45

5.2.1 The Multiplicative Group of Finite Fields of Characteristic 2 . . . . . . . . . . . . . . . . . . . . . 47

5.2.2 The Multiplicative Group of Fields of Prime Order . . . 49

5.2.3 The Elliptic Curve Group over Finite Fields . . . . . . . 51

**6 Public-Key Systems: Mistakes and Problems 55**

6.1 Formal Approach to Design and Analysis . . . . . . . . . 55

6.2 Flow of Trust . . . . . . . . . . . . . . . . . . . . . . 60

**7 Projection of Needs and Requirements for Public-Key Systems 63**

7.1 Assessment and Prediction: Guide Public-Key Systems Implementations in the 1990s . . . . . . . . . . . . . . . 68

7.2 Some Remarks Concerning Exponentiation Schemes . . . 73

**References 83**