ISO/IEC 18032:2005-01 (E)

Information technology - Security techniques - Prime number generation

Contents

Page

Foreword iv

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Symbols 2

5 Trial division 3

6 Probabilistic primality tests 4
6.1 Miller-Rabin primality test 4
6.2 Frobenius-Grantham primality test 5
6.3 Lehmann primality test 5

7 Deterministic primality verification methods 6
7.1 Elliptic curve primality certificate 6
7.2 Primality certificate based on Maurer's algorithm 7

8 Prime number generation 8
8.1 Requirements 8
8.2 Using probabilistic tests 9
8.3 Using deterministic methods 10

9 Candidate prime testing 11

Annex A (informative) Error probabilities 13

Annex B (informative) Generating primes with side conditions 16

Bibliography 18