

Table of Contents

I Introduction and Background	1
II Integrity Concepts	9
III Recommended Integrity Primitives	23
1 Introduction to Part III	25
2 MDC-4	31
3 RIPEMD	69
4 RIPE-MAC	113
5 IBC-Hash	145
6 SKID	169
7 RSA	179
8 COMSET	199
9 RSA Key Generation	213
10 Implementation Guidelines for Arithmetic Computation	233