

目 次

①	暗号とは？	1
1.1	暗号の歴史	1
1.2	現代の暗号・認証技術の概要	9
1.3	本書の構成	12
②	共通鍵暗号	13
2.1	ワンタイムパッド	13
2.2	ブロック暗号	19
2.3	ブロック暗号のモード	24
③	公開鍵暗号	31
3.1	公開鍵暗号とは？	31
3.2	RSA 暗号	32
3.3	エルガマル暗号	37
3.4	楕円曲線暗号	42
④	ハッシュ関数とメッセージ認証	49
4.1	ハッシュ関数	49
4.2	メッセージ認証 MAC	53
⑤	デジタル署名	59
5.1	デジタル署名とは？	59
5.2	デジタル署名の安全性	60
5.3	RSA 署名	61
5.4	エルガマル署名	64
5.5	シュノア署名	67

⑥	インターネットへの応用	73
6.1	サーバ認証	73
6.2	公開鍵証明書	74
6.3	PKI	76
6.4	ハイブリッド暗号	78
6.5	SSL/TLS	80
6.6	暗号の危殆化	86
⑦	高機能暗号	89
7.1	双線型写像	90
7.2	ID ベース暗号	90
7.3	検索可能暗号	94
7.4	属性ベース暗号	98
7.5	放送型暗号	100
7.6	準同型暗号	103
7.7	グループ署名	104
⑧	暗号・認証技術の今後	107
	参考文献	111
	安全、安心なサイバー社会をつくる暗号のしくみを学ぼう (コーディネーター 井上克郎)	113
	索引	119