

# Daftar Isi

Kata Pengantar .....	iii
Daftar Isi .....	v
<b>1 Pengantar Kriptografi .....</b>	<b>1</b>
1.1 Definisi dan Terminologi .....	1
1.2 Tujuan Kriptografi .....	9
1.3 Sejarah Kriptografi .....	10
1.4 Kriptanalisis .....	12
1.5 Kriptografi Kunci-Simetri dan Nirsimetri .....	13
<b>2 Serangan Terhadap Kriptografi .....</b>	<b>17</b>
2.1 Kriptanalisis .....	17
2.2 Keamanan Algoritma Kriptografi .....	18
2.3 Kompleksitas Serangan .....	19
2.4 Jenis-jenis Serangan .....	19
<b>3 Landasan Matematika .....</b>	<b>27</b>
3.1 Fungsi .....	27
3.2 Permutasi dan Kombinasi .....	32
3.3 Teori Peluang .....	32
3.4 Teori Informasi .....	34
3.5 Teori Bilangan .....	36
3.6 Aljabar Abstrak .....	48
<b>4 Algoritma Kriptografi Klasik .....</b>	<b>55</b>
4.1 <i>Cipher</i> Substitusi .....	56
4.2 Jenis-jenis <i>Cipher</i> Substitusi .....	61
4.3 <i>Cipher</i> Transposisi .....	69
4.4 Super Enkripsi .....	70
4.5 Teknik Analisis Frekuensi .....	71
4.6 <i>Affine Cipher</i> .....	77
4.7 <i>Vigènere Cipher</i> .....	79
4.8 <i>Playfair Cipher</i> .....	86
4.9 <i>Enigma Cipher</i> .....	89
4.10 <i>One-Time Pad</i> .....	93

# 5

## Algoritma Kriptografi Modern ..... 97

5.1	Rangkaian Bit dan Operasinya .....	98
5.2	Algoritma Enkripsi dengan <i>XOR</i> Sederhana .....	100
5.3	Kategori <i>Cipher</i> Kunci-Simetri .....	102
5.4	<i>Cipher</i> Aliran .....	103
5.5	Pembangkit Aliran-Kunci .....	105
5.6	Jenis-jenis <i>Cipher</i> Aliran .....	107
5.7	<i>Linear Feedback Shift Register</i> (LFSR) .....	109
5.8	Serangan Terhadap <i>Cipher</i> Aliran .....	110
5.9	<i>RC4</i> .....	113
5.10	<i>A5</i> .....	115
5.11	<i>Cipher</i> Blok ( <i>Block Cipher</i> ) .....	116
5.13	<i>Cipher Block Chaining</i> (CBC) .....	123
5.14	<i>Cipher-Feedback</i> (CFB) .....	126
5.16	<i>Output-Feedback</i> (OFB) .....	129
5.17	Prinsip-prinsip Perancangan <i>Cipher</i> Blok .....	130

# 6

## Beberapa Algoritma *Cipher* Blok ..... 135

6.1	<i>DES</i> .....	136
6.2	Double <i>DES</i> dan Triple <i>DES</i> .....	148
6.3	<i>GOST</i> .....	151
6.4	<i>RC5</i> .....	154
6.5	<i>Advanced Encryption Standard</i> ( <i>AES</i> ) .....	157

# 7

## Kriptografi Kunci-Publik ..... 171

7.1	Konsep Kriptografi Kunci-Publik .....	172
7.2	Sejarah Kriptografi Kunci-Publik .....	176
7.3	Perbandingan Kriptografi Kunci-Simetri dengan Kriptografi Kunci-Publik .....	177
7.4	Aplikasi Kriptografi Kunci-Publik .....	178
7.5	<i>RSA</i> .....	179
7.6	<i>ElGamal</i> .....	184
7.7	Algoritma Pertukaran Kunci <i>Diffie-Hellman</i> .....	186
7.8	Algoritma <i>Knapsack</i> .....	188
7.9	Algoritma untuk Perpangkatan-Modulo .....	193
7.10	Tipe Data Bilangan Bulat yang Besar .....	197
7.11	Pembangkitan Bilangan Prima .....	197

# 8

## Pembangkit Bilangan Acak Semu ..... 199

8.1	<i>Linear Congruential Generator</i> ( <i>LCG</i> ) .....	199
8.2	Pembangkit Bilangan Acak yang Aman untuk Kriptografi .....	202
8.3	<i>Blum Blum Shut</i> .....	203
8.4	<i>CSPRNG</i> Berbasis <i>RSA</i> .....	204

8.5	CSPRNG Berbasis Chaos .....	205
<b>9</b>	<b>Fungsi <i>Hash</i> Satu-Arah dan <i>MAC</i> .....</b>	<b>217</b>
9.1	Fungsi <i>Hash</i> Satu-Arah .....	218
9.2	Algoritma <i>MD5</i> .....	202
9.3	<i>Secure Hash Algorithm</i> (SHA) .....	231
9.4	<i>MAC</i> dan Aplikasinya .....	237
9.5	Algoritma <i>MAC</i> .....	238
<b>10</b>	<b>Tandatangan Digital .....</b>	<b>239</b>
10.1	Konsep Tanda-tangan Digital .....	241
10.2	Penandatangan dengan Cara Mengenkripsi Pesan .....	241
10.3	Tanda-tangan dengan Menggunakan Fungsi Hash .....	243
10.4	<i>Digital Standard Algorithm</i> (DSA) .....	247
<b>11</b>	<b>Protokol Kriptografi .....</b>	<b>251</b>
11.1	Protokol Komunikasi dengan Sistem Kriptografi Simetri .....	252
11.2	Protokol Komunikasi dengan Sistem Kriptografi Kunci-Publik .....	252
11.3	Protokol untuk Tanda-tangan Digital .....	253
11.4	Protokol untuk Tanda-tangan Digital dengan Enkripsi .....	255
11.5	Pertukaran Kunci .....	257
11.6	Otentikasi .....	259
<b>12</b>	<b>Infrastruktur Kunci Publik .....</b>	<b>261</b>
12.1	Sertifikat Digital .....	261
12.2	<i>X.509</i> .....	265
12.3	Infrastruktur Kunci Publik .....	267
12.4	<i>Microsoft Authenticode</i> .....	271
<b>13</b>	<b>Manajemen Kunci .....</b>	<b>273</b>
13.1	Pembangkitan Kunci .....	272
13.2	Penyebaran Kunci .....	274
13.3	Penyimpanan Kunci ( <i>Key Storage</i> ) .....	274
13.4	Penggunaan Kunci .....	275
13.5	Perubahan Kunci .....	275
13.6	Penghancuran Kunci ( <i>Key Destruction</i> ) .....	276

<b>14</b>	<b>Kriptografi dalam Kehidupan Sehari-hari</b>	<b>277</b>
14.1	Kartu Cerdas	277
14.2	Transaksi lewat Anjungan Tunai mandiri (ATM)	279
14.3	<i>Pay TV</i>	281
14.4	Komunikasi dengan Telepon Seluler	281
14.5	<i>E-commerce</i> di Internet dan <i>SSL</i>	283
14.6	Pengamanan <i>E-mail</i> dengan <i>PGP (Pretty Good Privacy)</i>	291
<b>15</b>	<b>Steganografi dan <i>Watermarking</i></b>	<b>301</b>
15.1	Sejarah Steganografi	302
15.2	Persoalan Tahanan Penjara	302
15.3	Konsep dan Terminologi	304
15.4	Teknik Penyembunyian Data	308
15.5	<i>Watermarking</i>	309
15.6	Jenis-jenis <i>Image Watermarking</i>	315
15.7	Aplikasi <i>Image Watermarking</i>	316
15.8	Metode <i>Image Watermarking</i>	317
15.9	<i>Watermarking</i> pada Media Digital Lain	318
15.10	<i>Watermarking</i> pada Program Komersil	318
	Daftar Pustaka	319