

1.5 Keamanan Algoritma	10
1.6 Kriptologi	12
1.7 Sejarah Kriptografi	14
1.7.1 Mesin Purple Jepang	16
1.7.2 Mesin Enigma Jerman	17
1.8 Klasifikasi Algoritma Kriptografi	19
1.9 Sejarah Perjalanan Kriptografi	20
BAB 2 KRIPTOGRAFI KLASIK	31
2.1 Teknik Enkripsi Klasik	31
2.2 Teknik Substitusi	31
2.3 Jenis-Jenis Sandi Substitusi	32
2.3.1 Monoalphabetic Cipher atau Simple Substitution Cipher	32
2.3.2 Caesar Cipher	32
2.3.3 Atbash Cipher	37
2.3.4 Pigpen Cipher	38
2.3.5 Polybius Square	39
2.4 Homophonic Substitution Cipher	40
2.5 Polyalphabetic Substitution Cipher	40
2.5.1 Vigenère Cipher	42
2.5.2 Beaufort Cipher	48
2.5.3 Autokey Cipher	49

2.5.4 Running Key Cipher.....	50
2.5.5 Alberti Cipher	50
2.6 Polygram Substitution Cipher.....	54
2.6.1 Playfair Cipher.....	54
2.6.2 Bifid Cipher	57
2.6.3 Trifid Cipher	58
2.6.4 CM Bifid (Conjugated Matrix Bifid).....	59
2.6.5 Foursquare Cipher	60
2.6.6 Digraph Cipher	61
2.7 Transposition Cipher.....	62
2.7.1 Railfence Cipher	62
2.7.2 Redefence Cipher	63
2.7.3 Reverse Cipher	63
2.7.4 Menghasilkan Abjad Campuran	64
2.7.5 Double Transposition Cipher	66
2.7.6 Myszowski	68
2.7.7 Nihilist Substitution Cipher	69
2.7.9 Nihilist Transposition Cipher	70
2.7.10 Bazeries Cipher	70
2.7.11 Gronsfeld Cipher.....	71
2.7.12 Hill Cipher	72

2.7.13 Chinese Remainder Theorem.....	79
2.7.14 Bilangan Prima	80
BAB 3 STREAM DAN BLOCK CIPHER.....	83
3.1 Stream Cipher	83
3.1.1 Synchronous Stream Cipher	86
3.1.2 Self-Synchronous Stream Ciphers.....	89
3.2 Pembangkit Aliran-Bit-Kunci (<i>Keystream Generator</i>)	91
3.3 Aplikasi Stream Cipher.....	94
3.4 Sandi Blok (<i>Block Cipher</i>)	95
3.4.1 Teknik Kriptografi Klasik yang Digunakan pada Block Cipher ..	96
3.4.2 Prinsip Penyandian Shannon	97
3.4.3 Mode Operasi Block Cipher	98
BAB 4 DATA ENCRYPTION STANDARD (DES).....	113
4.1 Pengantar Algoritma DES.....	113
4.2 Sejarah DES	115
4.3 Algoritma Sebagai Standar	116
4.4 Keamanan dan Kriptanalisis	118
4.4.1 Serangan Brute Force	118
4.4.2 Serangan yang Lebih Cepat dari Brute Force	120
4.5 Algoritma Triple DES.....	122
4.5.1 Algoritma Enkripsi	122

4.5.2 Algoritma Dekripsi	126
4.5.3 Fungsi Cipher f	127
4.5.4 Penjadwalan Kunci	131
4.5.5 Contoh Enkripsi DES	137
4.6 Triple DES	141
BAB 5 INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA)	145
5.1 Pendahuluan IDEA	145
5.2 Penugasan dan Pembentukan Subkunci (Subkey)	146
5.3 Enkripsi IDEA	147
5.4 Dekripsi IDEA	152
5.5 Triple Data Encryption Algorithm (TDEA)	171
5.5.1 Dasar TDEA Forward dan Inverse Cipher Operation	171
5.5.2 Pilihan Kunci TDEA	172
5.5.3 Mode Operasi TDEA	172
5.5.4 Contoh dari Operasi TDEA Forward dan Inverse Cipher	174
BAB 6 ADVANCED ENCRYPTION STANDARD (AES)	179
6.1 Pendahuluan AES	179
6.2 Notasi dan Konvensi	180
6.2.1 Input dan Output	180
6.2.2 Byte	180
6.2.3 Array Byte	181

6.2.4 State.....	182
6.2.5 State Sebagai Array Kolom.....	183
6.3 Konsep Dasar Matematika.....	183
6.3.1 Penambahan.....	184
6.3.2 Perkalian.....	184
6.4 Spesifikasi Algoritma.....	185
6.5 Cipher.....	188
6.5.2 Transformasi ShiftRows()	194
6.5.3 Transformasi MixColumns()	195
6.5.4 Transformasi AddRoundKey()	197
6.6 Key Expansion	198
6.6.1 Contoh Key Expansion	199
6.7 Inverse Cipher.....	205
6.7.1 Transformasi InvShiftRows()	206
6.7.2 Transformasi InvSubBytes()	206
BAB 7 ALGORITMA MESSAGE DIGESTION	209
7.1 Message Digest 2 (MD 2)	209
7.1.1 Kelemahan pada MD2.....	210
7.2 Message Digest 4 (MD 4)	210
7.3 Message Digest 5 (MD 5)	213
7.3.1 Pengujian Integritas.....	214
7.3.2 Algoritma MD5	214

7.3.3 Kerusakan pada MD5.....	216
7.3.4 Pseudocode	219
BAB 8 SECURE HASH STANDARD	221
8.1 Pendahuluan Secure Hash Standard	221
8.2 Bit String dan Integer	222
8.3 Fungsi.....	223
8.3.1 Fungsi SHA-1	224
8.3.2 Fungsi SHA-256.....	224
8.4 Konstan	224
8.4.1 Konstan SHA-1	224
8.4.2 Konstan SHA-256	225
8.5 Padding Message.....	225
8.5.1 SHA-1 dan SHA-256.....	225
8.6 Memparsing Padded Message	226
8.6.1 SHA-1 dan SHA-256.....	226
8.7 Pengaturan Initial Hash Value (H(0))	226
8.7.1 SHA-1	226
8.7.2 SHA-256	227
8.8 Secure Hash Algorithms	227
8.8.1 SHA-1	227
8.8.2 Contoh SHA-1 (One-Block Message).....	228
8.8.3 Contoh SHA-1 (Multi-Block Message)	232

8.8.4 Contoh SHA-1 (Long Message)	241
8.9 Hashing Variable Length	241
BAB 9 HASH MESSAGE AUTHENTICATION CODE (HMAC)	249
9.1 Definisi HMAC	250
9.2 Algoritma HMAC	251
9.3 Cara Kerja HMAC	253
9.4. Implementasi	254
9.4.1 SHA-1 dengan Kunci 64-Byte	255
9.4.2 SHA-1 dengan Kunci 20-Byte	256
9.4.3 SHA-1 dengan Kunci 100-Byte	257
9.4.4 SHA-1 dengan Kunci 49-Byte, Dipotong Sampai 12-Byte HMAC	259
BAB 10 KRIPTOSISTEM KUNCI PUBLIK RIVEST SHAMIR ADLEMAN (RSA).....	261
10.1 Sejarah RSA	261
10.2 RSA	262
10.3 Algoritma Enkripsi/Dekripsi	264
10.4 Algoritma RSA	265
10.5 Kekuatan dan Keamanan RSA	267
10.6 Aplikasi RSA dalam Kehidupan Sehari-Hari	268
10.7 Keuntungan dan Kerugian Menggunakan RSA	271

10.8 RSA Sebagai Standar Resmi	273
10.9 RSA Sebagai Standar De Facto	274
BAB 11 KRIPTOSISTEM KUNCI PUBLIK ELGAMAL.....	277
11.1 Pengantar ElGamal	277
11.2 Kriptosistem ElGamal	278
11.3 Enkripsi ElGamal	278
11.4 Tanda Tangan ElGamal	281
11.5 Skema Autentikasi ElGamal	283
BAB 12 ALGORITMA KNAPSACK	287
12.1 Pengantar Algoritma Knapsack.....	287
12.2 Knapsack Superincreasing.....	288
12.3 Algoritma Cryptosystem Knapsack	290
12.4 Membuat Private Key dari Public Key	291
12.5 Enkripsi.....	292
12.6 Dekripsi	292
12.7 Implementasi Secara Praktis	293
12.8 Keamanan Knapsack	293
12.9 Varian Knapsack.....	294
BAB 13 PRETTY GOOD PRIVACY (PGP).....	295
13.1 Pendahuluan PGP	295
13.2 Alasan Kenapa Menggunakan PGP	297

13.3 Layanan PGP	300
13.4 Manajemen Kunci dalam PGP	304
13.5 PGP Dikomersialkan	307
BAB 14 TANDA TANGAN DIGITAL	317
14.1 Pengantar Tanda Tangan Digital	317
14.2 Tanda Tangan Digital Menggunakan <i>Public Key Cryptosystem</i>	322
14.3 Algoritma Tanda Tangan Digital	325
14.3.1 Digital Signatures Generation	326
14.3.2 Digital Signature Verification dan Validation	328
14.4 Algoritma Tanda Tangan Digital RSA	329
14.4.1 Pembentukan Pasangan Kunci RSA	329
14.5 Elliptic Curve Digital Signature Algorithm (ECDSA)	331
14.5.2 Domain Parameter Generation	332
14.6 Schnorr Authentication dan Digital Signature Scheme	333
14.6.1 Pembentukan Kunci	333
14.6.2 Protokol Autentikasi	334
14.6.3 Protokol dan Tanda Tangan Digital	336
14.7 Bagaimana Teknologi Tanda Tangan Digital Bekerja?	338
BAB 15 STEGANOGRAFI	341
15.1 Definisi Steganografi	341
15.2 Sejarah Steganografi	343

15.3 Kriteria Steganografi yang Baik	343
15.4 Jenis-Jenis Steganografi.....	344
15.5 Perlindungan Terhadap Steganografi	345
DAFTAR PUSTAKA	349
DAFTAR ISTILAH	353
LAMPIRAN.....	359
Lampiran 1 Program Monoalfabetik.....	359
Lampiran 2 Program Vigenère	365
Lampiran 3 Program Playfair	371
Lampiran 4 Program Hill Cipher	381
Lampiran 5 Program ElGamal	386
TENTANG PENULIS	391

Daftar Isi

KATA PENGANTAR	III
DAFTAR ISI	V
BAB 1 PENGANTAR KRIPTOGRAFI.....	1
1.1 Pengertian dan Istilah	1
1.1.1 Pengirim dan Penerima.....	1
1.1.2 Pesan dan Enkripsi	1
1.2 Tujuan Kriptografi	2
1.3 Algoritma dan Kunci	4
1.3.1 Algoritma Simetris.....	5
1.3.2 Algoritma <i>Public-Key</i>	6
1.4 Kriptanalisis	7

1.5 Keamanan Algoritma	10
1.6 Kriptologi	12
1.7 Sejarah Kriptografi	14
1.7.1 Mesin Purple Jepang	16
1.7.2 Mesin Enigma Jerman	17
1.8 Klasifikasi Algoritma Kriptografi	19
1.9 Sejarah Perjalanan Kriptografi	20
BAB 2 KRIPTOGRAFI KLASIK	31
2.1 Teknik Enkripsi Klasik	31
2.2 Teknik Substitusi	31
2.3 Jenis-Jenis Sandi Substitusi	32
2.3.1 Monoalphabetic Cipher atau Simple Substitution Cipher	32
2.3.2 Caesar Cipher	32
2.3.3 Atbash Cipher	37
2.3.4 Pigpen Cipher	38
2.3.5 Polybius Square	39
2.4 Homophonic Substitution Cipher	40
2.5 Polyalphabetic Substitution Cipher	40
2.5.1 Vigenère Cipher	42
2.5.2 Beaufort Cipher	48
2.5.3 Autokey Cipher	49

2.5.4 Running Key Cipher.....	50
2.5.5 Alberti Cipher	50
2.6 Polygram Substitution Cipher.....	54
2.6.1 Playfair Cipher.....	54
2.6.2 Bifid Cipher	57
2.6.3 Trifid Cipher	58
2.6.4 CM Bifid (Conjugated Matrix Bifid).....	59
2.6.5 Foursquare Cipher	60
2.6.6 Digraph Cipher	61
2.7 Transposition Cipher.....	62
2.7.1 Railfence Cipher	62
2.7.2 Redefence Cipher	63
2.7.3 Reverse Cipher	63
2.7.4 Menghasilkan Abjad Campuran	64
2.7.5 Double Transposition Cipher	66
2.7.6 Myszowski	68
2.7.7 Nihilist Substitution Cipher	69
2.7.9 Nihilist Transposition Cipher	70
2.7.10 Bazeries Cipher	70
2.7.11 Gronsfeld Cipher.....	71
2.7.12 Hill Cipher	72

2.7.13 Chinese Remainder Theorem.....	79
2.7.14 Bilangan Prima	80
BAB 3 STREAM DAN BLOCK CIPHER.....	83
3.1 Stream Cipher	83
3.1.1 Synchronous Stream Cipher	86
3.1.2 Self-Synchronous Stream Ciphers.....	89
3.2 Pembangkit Aliran-Bit-Kunci (<i>Keystream Generator</i>)	91
3.3 Aplikasi Stream Cipher.....	94
3.4 Sandi Blok (<i>Block Cipher</i>)	95
3.4.1 Teknik Kriptografi Klasik yang Digunakan pada Block Cipher ..	96
3.4.2 Prinsip Penyandian Shannon	97
3.4.3 Mode Operasi Block Cipher	98
BAB 4 DATA ENCRYPTION STANDARD (DES).....	113
4.1 Pengantar Algoritma DES.....	113
4.2 Sejarah DES	115
4.3 Algoritma Sebagai Standar	116
4.4 Keamanan dan Kriptanalisis	118
4.4.1 Serangan Brute Force	118
4.4.2 Serangan yang Lebih Cepat dari Brute Force	120
4.5 Algoritma Triple DES.....	122
4.5.1 Algoritma Enkripsi	122

4.5.2 Algoritma Dekripsi	126
4.5.3 Fungsi Cipher f	127
4.5.4 Penjadwalan Kunci	131
4.5.5 Contoh Enkripsi DES	137
4.6 Triple DES	141
BAB 5 INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA)	145
5.1 Pendahuluan IDEA	145
5.2 Penugasan dan Pembentukan Subkunci (Subkey)	146
5.3 Enkripsi IDEA	147
5.4 Dekripsi IDEA	152
5.5 Triple Data Encryption Algorithm (TDEA)	171
5.5.1 Dasar TDEA Forward dan Inverse Cipher Operation	171
5.5.2 Pilihan Kunci TDEA	172
5.5.3 Mode Operasi TDEA	172
5.5.4 Contoh dari Operasi TDEA Forward dan Inverse Cipher	174
BAB 6 ADVANCED ENCRYPTION STANDARD (AES)	179
6.1 Pendahuluan AES	179
6.2 Notasi dan Konvensi	180
6.2.1 Input dan Output	180
6.2.2 Byte	180
6.2.3 Array Byte	181

6.2.4 State.....	182
6.2.5 State Sebagai Array Kolom.....	183
6.3 Konsep Dasar Matematika.....	183
6.3.1 Penambahan.....	184
6.3.2 Perkalian.....	184
6.4 Spesifikasi Algoritma.....	185
6.5 Cipher.....	188
6.5.2 Transformasi ShiftRows()	194
6.5.3 Transformasi MixColumns()	195
6.5.4 Transformasi AddRoundKey()	197
6.6 Key Expansion	198
6.6.1 Contoh Key Expansion	199
6.7 Inverse Cipher.....	205
6.7.1 Transformasi InvShiftRows()	206
6.7.2 Transformasi InvSubBytes()	206
BAB 7 ALGORITMA MESSAGE DIGESTION	209
7.1 Message Digest 2 (MD 2)	209
7.1.1 Kelemahan pada MD2.....	210
7.2 Message Digest 4 (MD 4)	210
7.3 Message Digest 5 (MD 5)	213
7.3.1 Pengujian Integritas.....	214
7.3.2 Algoritma MD5	214

7.3.3 Kerusakan pada MD5.....	216
7.3.4 Pseudocode	219
BAB 8 SECURE HASH STANDARD	221
8.1 Pendahuluan Secure Hash Standard	221
8.2 Bit String dan Integer	222
8.3 Fungsi.....	223
8.3.1 Fungsi SHA-1	224
8.3.2 Fungsi SHA-256.....	224
8.4 Konstan	224
8.4.1 Konstan SHA-1	224
8.4.2 Konstan SHA-256	225
8.5 Padding Message.....	225
8.5.1 SHA-1 dan SHA-256.....	225
8.6 Memparsing Padded Message	226
8.6.1 SHA-1 dan SHA-256.....	226
8.7 Pengaturan Initial Hash Value (H(0))	226
8.7.1 SHA-1	226
8.7.2 SHA-256	227
8.8 Secure Hash Algorithms	227
8.8.1 SHA-1	227
8.8.2 Contoh SHA-1 (One-Block Message).....	228
8.8.3 Contoh SHA-1 (Multi-Block Message)	232

8.8.4 Contoh SHA-1 (Long Message)	241
8.9 Hashing Variable Length	241
BAB 9 HASH MESSAGE AUTHENTICATION CODE (HMAC)	249
9.1 Definisi HMAC	250
9.2 Algoritma HMAC	251
9.3 Cara Kerja HMAC	253
9.4. Implementasi	254
9.4.1 SHA-1 dengan Kunci 64-Byte	255
9.4.2 SHA-1 dengan Kunci 20-Byte	256
9.4.3 SHA-1 dengan Kunci 100-Byte	257
9.4.4 SHA-1 dengan Kunci 49-Byte, Dipotong Sampai 12-Byte HMAC	259
BAB 10 KRIPTOSISTEM KUNCI PUBLIK RIVEST SHAMIR ADLEMAN (RSA).....	261
10.1 Sejarah RSA	261
10.2 RSA	262
10.3 Algoritma Enkripsi/Dekripsi	264
10.4 Algoritma RSA	265
10.5 Kekuatan dan Keamanan RSA	267
10.6 Aplikasi RSA dalam Kehidupan Sehari-Hari	268
10.7 Keuntungan dan Kerugian Menggunakan RSA	271

10.8 RSA Sebagai Standar Resmi	273
10.9 RSA Sebagai Standar De Facto	274
BAB 11 KRIPTOSISTEM KUNCI PUBLIK ELGAMAL.....	277
11.1 Pengantar ElGamal	277
11.2 Kriptosistem ElGamal	278
11.3 Enkripsi ElGamal	278
11.4 Tanda Tangan ElGamal	281
11.5 Skema Autentikasi ElGamal	283
BAB 12 ALGORITMA KNAPSACK	287
12.1 Pengantar Algoritma Knapsack.....	287
12.2 Knapsack Superincreasing.....	288
12.3 Algoritma Cryptosystem Knapsack	290
12.4 Membuat Private Key dari Public Key	291
12.5 Enkripsi.....	292
12.6 Dekripsi	292
12.7 Implementasi Secara Praktis	293
12.8 Keamanan Knapsack	293
12.9 Varian Knapsack.....	294
BAB 13 PRETTY GOOD PRIVACY (PGP).....	295
13.1 Pendahuluan PGP	295
13.2 Alasan Kenapa Menggunakan PGP	297

13.3 Layanan PGP	300
13.4 Manajemen Kunci dalam PGP	304
13.5 PGP Dikomersialkan	307
BAB 14 TANDA TANGAN DIGITAL	317
14.1 Pengantar Tanda Tangan Digital	317
14.2 Tanda Tangan Digital Menggunakan <i>Public Key Cryptosystem</i>	322
14.3 Algoritma Tanda Tangan Digital	325
14.3.1 Digital Signatures Generation	326
14.3.2 Digital Signature Verification dan Validation	328
14.4 Algoritma Tanda Tangan Digital RSA	329
14.4.1 Pembentukan Pasangan Kunci RSA	329
14.5 Elliptic Curve Digital Signature Algorithm (ECDSA)	331
14.5.2 Domain Parameter Generation	332
14.6 Schnorr Authentication dan Digital Signature Scheme	333
14.6.1 Pembentukan Kunci	333
14.6.2 Protokol Autentikasi	334
14.6.3 Protokol dan Tanda Tangan Digital	336
14.7 Bagaimana Teknologi Tanda Tangan Digital Bekerja?	338
BAB 15 STEGANOGRAFI	341
15.1 Definisi Steganografi	341
15.2 Sejarah Steganografi	343

15.3 Kriteria Steganografi yang Baik	343
15.4 Jenis-Jenis Steganografi.....	344
15.5 Perlindungan Terhadap Steganografi	345
DAFTAR PUSTAKA	349
DAFTAR ISTILAH	353
LAMPIRAN.....	359
Lampiran 1 Program Monoalfabetik.....	359
Lampiran 2 Program Vigenère	365
Lampiran 3 Program Playfair	371
Lampiran 4 Program Hill Cipher	381
Lampiran 5 Program ElGamal	386
TENTANG PENULIS	391

Daftar Isi

KATA PENGANTAR	III
DAFTAR ISI	V
BAB 1 PENGANTAR KRIPTOGRAFI.....	1
1.1 Pengertian dan Istilah	1
1.1.1 Pengirim dan Penerima.....	1
1.1.2 Pesan dan Enkripsi	1
1.2 Tujuan Kriptografi	2
1.3 Algoritma dan Kunci	4
1.3.1 Algoritma Simetris.....	5
1.3.2 Algoritma <i>Public-Key</i>	6
1.4 Kriptanalisis	7