



littlekay

# KRIPTO GRAFI

Teknik Keamanan Data & Informasi

Janner Simarmata | Sriadhi | Robbi Rahim

KRIPTOGRAFI

Teknik Keamanan Data & Informasi

www.littlekay.com



## PAGE MENU

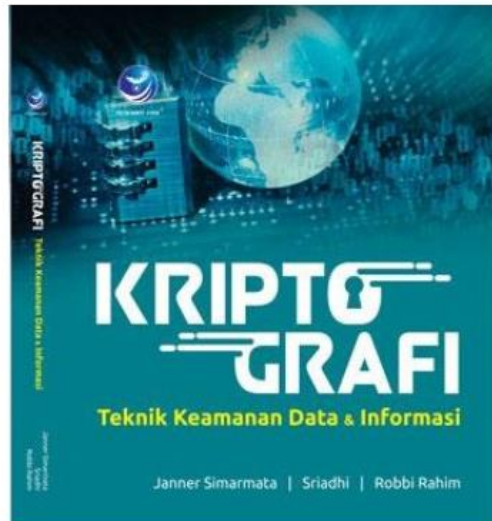
- Home
- Contact Us
- Jadi Penulis?
- Info-info
- Download
- Shipping
- Karier Penerbit Andi



## KATEGORI BUKU

**NEWS ANNIVERSARY PENERBIT ANDI KE-40 Tahun. Ikuti terus berbagai Program Menarik ANDIPUBLISHER**

ANNIVERSARY PENERBIT ANDI KE-40 Tahun. Ikuti terus berbagai Program Menarik ANDIPUBLISHER

**Kriptografi, Teknik Keamanan Data Dan Informasi**

<b>Kategori(Sub)</b>	: Komputer (Ilmu Komputer)
<b>ISBN</b>	: <a href="#">978-623-01-0288-2</a>
<b>Penulis</b>	: Janner Simarmata, Sriadhi Dan Robbi Rahim
<b>Ukuran/Halaman</b>	: 19x23 cm <sup>2</sup> / xvi+392 halaman
<b>Edisi/Cetakan</b>	: I, 1st Published
<b>Tahun Terbit</b>	: 2020
<b>Berat</b>	: 612 gram
<b>Harga</b>	: Rp 132.000,- Diskon 20%
<b>Harga Diskon</b>	: Rp <b>105.600,-</b>

[Review me](#)[Show Review \(0\)](#)[Add to Cart](#)**Sinopsis**



PENERBIT ANDI

# KRIPTO GRAFI

**Teknik Keamanan Data & Informasi**

Janner Simarmata | Sriadhi | Robbi Rahim

## KRIPTOGRAFI

Teknik Keamanan Data dan Informasi

Oleh: Janner Simarmata, Sriadhi, dan Robbi Rahim

Hak Cipta ©2019 pada Penulis.

Editor : Marcella Kika

Setting : yulius basuki

Desain Cover : Dany Nofianto

Korektor : Yulia Fransisca A.

Hak Cipta dilindungi undang-undang.

Dilarang memperbanyak atau memindahkan sebagian atau seluruh isi buku ini dalam bentuk apa pun, baik secara elektronik maupun mekanis, termasuk memfotokopi, merekam atau dengan sistem penyimpanan lainnya, tanpa izin tertulis dari penulis.

Penerbit CV. ANDI OFFSET (Penerbit ANDI, Anggota IKAPI) Jl. Beo 38-40,  
telp (0274) 561881, Fax (0274) 588282 Yogyakarta 55281

Percetakan CV. ANDI OFFSET (Penerbit ANDI, Anggota IKAPI) Jl. Beo 38-40,  
telp (0274) 561881, Fax (0274) 588282 Yogyakarta 55281

*Simarmata, Janner*

**KRIPTOGRAFI; TEKNIK KEAMANAN DATA DAN INFORMASI/ Janner  
Simarmata, Sriadhi, dan Robbi Rahim**

**- Ed. I. - Yogyakarta: ANDI;**

28 - 27 - 26 - 25 - 24 - 23 - 22 - 21 - 20 - 19

xvi + 392 hlm ; 19x23 Cm.

10 9 8 7 6 5 4 3 2 1

ISBN: 978 - 623 - 01 - 0288 - 2

I. Judul

1. Cryptography

2. Sriadhi

3. Rahim, Robbi

DDC'23 :005.82

# Kata Pengantar

Puji syukur penulis ucapkan kepada Tuhan Yang Maha Esa, akhirnya ini dapat juga terselesaikan, walaupun banyak hambatan yang penulis alami selama penulisan buku ini. Penulis mengucapkan banyak terima kasih kepada sahabat-sahabat yang telah memberikan masukan.

Buku ini membahas tentang pengenalan kriptografi dan sejarah kriptografi klasik serta kriptografi modern yang banyak digunakan sampai saat ini. Buku ini sangat cocok digunakan oleh akademisi, tenaga guru dan dosen sebagai buku referensi dan menjadi buku pegangan mahasiswa.

Penulis minta maaf apabila terdapat kesalahan-kesalahan dalam penulisan buku ini. Penulis juga mengharapkan kritik dan saran untuk kemajuan ini di masa yang akan datang. Selain itu, penulis juga berharap semoga buku ini bermanfaat bagi Anda. Akhir kata, selamat membaca dan selamat menikmati. Terima kasih banyak kepada Penerbit ANDI yang telah menerbitkan buku ini.

Medan, November 2018

Penulis

# Daftar Isi

<b>KATA PENGANTAR</b> .....	<b>III</b>
<b>DAFTAR ISI</b> .....	<b>V</b>
<b>BAB 1 PENGANTAR KRIPTOGRAFI</b> .....	<b>1</b>
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
<b>KRIPTOGRAFI KLASIK .....</b>	<b>31</b>
2.1 Teknik Enkripsi Klasik .....	31
2.2 Teknik Substitusi .....	31
2.3 Jenis-Jenis Sandi Subsbtitusi .....	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

13 Chinese Remainder Theorem.....	79
14 Bilangan Prima.....	80
<b>DAN BLOCK CIPHER.....</b>	<b>83</b>
m Cipher.....	83
1 Synchronous Stream Cipher.....	86
2 Self-Synchronous Stream Ciphers.....	89
angkit Aliran-Bit-Kunci ( <i>Keystream Generator</i> ).....	91
asi Stream Cipher.....	94
i Blok ( <i>Block Cipher</i> ).....	95
1 Teknik Kriptografi Klasik yang Digunakan pada Block Cipher ..	96
2 Prinsip Penyandian Shannon.....	97
3 Mode Operasi Block Cipher.....	98
<b>ENCRYPTION STANDARD (DES).....</b>	<b>113</b>
gantar Algoritma DES.....	113
arah DES.....	115
ritma Sebagai Standar.....	116
amanan dan Kriptanalisis.....	118
4.1 Serangan Brute Force.....	118
4.2 Serangan yang Lebih Cepat dari Brute Force.....	120
ritma Triple DES.....	122
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
<b>BAB 5 INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA).....</b>	<b>145</b>
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
<b>BAB 6 ADVANCED ENCRYPTION STANDARD (AES).....</b>	<b>179</b>
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

e.....	182
e Sebagai Array Kolom.....	183
ar Matematika.....	183
ambahan.....	184
alian.....	184
Algoritma.....	185
.....	188
sformasi ShiftRows() .....	194
sformasi MixColumns() .....	195
sformasi AddRoundKey() .....	197
on.....	198
h Key Expansion .....	199
r.....	205
sformasi InvShiftRows().....	206
sformasi InvSubBytes() .....	206
<b>MESSAGE DIGESTION .....</b>	<b>209</b>
est 2 (MD 2) .....	209
ahan pada MD2.....	210
est 4 (MD 4) .....	210
est 5 (MD 5) .....	213
ujian Integritas.....	214
tma MD5 .....	214

7.3.3 Kerusakan pada MD5.....	216
7.3.4 Pseudocode .....	219
<b>BAB 8 SECURE HASH STANDARD .....</b>	<b>221</b>
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



SHA-1 (Long Message) .....	241
Variable Length .....	241
<b>HMAC AUTHENTICATION CODE (HMAC) .....</b>	<b>249</b>
C .....	250
MAC .....	251
MAC .....	253
si .....	254
1 dengan Kunci 64-Byte .....	255
1 dengan Kunci 20-Byte .....	256
1 dengan Kunci 100-Byte .....	257
1 dengan Kunci 49-Byte, Dipotong Sampai 12-Byte .....	259
<b>KUNCI PUBLIK RIVEST SHAMIR ADLEMAN (RSA).....</b>	<b>261</b>
.....	261
.....	262
enkripsi/Dekripsi .....	264
SA .....	265
n Keamanan RSA .....	267
a dalam Kehidupan Sehari-Hari .....	268
dan Kerugian Menggunakan RSA .....	271

10.8 RSA Sebagai Standar Resmi .....	273
10.9 RSA Sebagai Standar De Facto .....	274
<b>BAB 11 KRIPTOSISTEM KUNCI PUBLIK ELGAMAL.....</b>	<b>277</b>
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
<b>BAB 12 ALGORITMA KNAPSACK .....</b>	<b>287</b>
12.1 Pengantar Algoritma Knapsack .....	287
12.2 Knapsack Superincreasing .....	288
12.3 Algoritma Cryptosystem Knapsack .....	290
12.4 Membuat <i>Private Key</i> dari <i>Public Key</i> .....	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
<b>BAB 13 PRETTY GOOD PRIVACY (PGP).....</b>	<b>295</b>
13.1 Pendahuluan PGP .....	295
13.2 Alasan Kenapa Menggunakan PGP .....	297

in PGP .....300

emen Kunci dalam PGP .....304

ikomersialkan .....307

**TANDA TANGAN DIGITAL .....317**

ntar Tanda Tangan Digital.....317

Tanda Tangan Digital Menggunakan *Public Key Cryptosystem*.....322

ma Tanda Tangan Digital .....325

Digital Signatures Generation ..... 326

Digital Signature Verification dan Validation..... 328

ma Tanda Tangan Digital RSA.....329

Pembentukan Pasangan Kunci RSA ..... 329

Curve Digital Signature Algorithm (ECDSA).....331

Domain Parameter Generation..... 332

r Authentication dan Digital Signature Scheme.....333

Pembentukan Kunci..... 333

Protokol Autentikasi ..... 334

Protokol dan Tanda Tangan Digital ..... 336

mana Teknologi Tanda Tangan Digital Bekerja?.....338

**STEGANOGRAFI.....341**

i Steganografi.....341

n 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**

# Pengantar Kriptografi

## Bab 1

### 1.1 Pengertian dan Istilah

Berikut ini akan dibahas beberapa pengertian dan istilah-istilah yang sering digunakan pada kriptografi.

#### 1.1.1 Pengirim dan Penerima

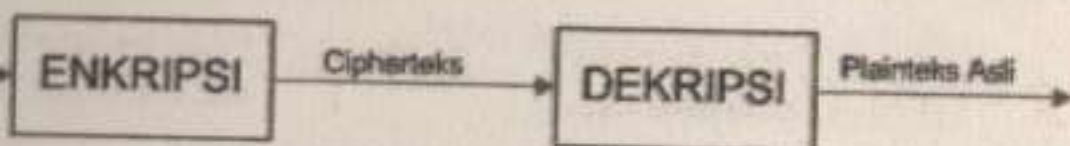
Misalkan seorang pengirim ingin mengirimkan suatu pesan kepada penerima, maka si pengirim ingin pesan yang akan dikirim dalam keadaan aman, si pengirim ingin meyakinkan bahwa penyusup tidak bisa membaca pesan tersebut.

#### 1.1.2 Pesan dan Enkripsi

Suatu pesan adalah plainteks (plaintext) (kadang juga disebut **cleartext**). Proses menyembunyikan pesan disebut enkripsi (encryption). Pesan yang dienkripsi adalah cipherteks (ciphertext). Proses pengembalian cipherteks ke plainteks disebut dekripsi (*decryption*). Lebih jelasnya

ada Gambar 1.1 (Jika melihat standar ISO 7498-2, maka disebut dengan *encrypt* dan *decipher* atau istilah lain disebut juga *encrypt* dan *decrypt*).

menjaga keamanan pesan adalah kriptografi (*cryptography*) sedangkan penerapannya disebut sebagai *cryptographer*. Kriptanalis (*cryptanalysts*) adalah ahli dari kriptanalis, seni dan ilmu untuk memecahkan cipherteks yaitu dengan samaran. Cabang dari matematika yang mencakup kriptografi dan kriptanalisis (*cryptanalysis*) adalah kriptologi (*cryptology*) dan praktisi disebut kriptologis (*cryptologists*). Cryptologist modern biasanya dilatih dalam teori matematika.



Gambar 1.1 Enkripsi dan dekripsi

diawali dengan  $M$  untuk pesan, atau  $P$  untuk plaintext. Ini bisa merupakan file teks, bitmap, aliran suara digital, dan citra video digital, sedangkan ciphertexts biner. Cipherteks ditandai dengan  $C$ . Ini juga data biner, kadang-kadang disebut sebagai  $M$ .

Fungsi enkripsi  $E$ , beroperasi pada  $M$  untuk menghasilkan  $C$ . Berikut adalah notasi untuk enkripsi:

Proses kebalikannya, yaitu fungsi dekripsi  $D$  beroperasi pada  $C$  untuk menghasilkan  $M$ .

## Kriptografi

Keamanan, tingkat keamanan yang ditambahkan ke data selama transmisi, dan komunikasi. Selama bertahun-tahun, matematikawan terus mengembangkan serangkaian algoritma yang semakin kompleks, yang semuanya ini dirancang untuk memastikan kerahasiaan, integritas, autentikasi,

dan ketidaktahuan. Selama periode yang sama, hacker dan pemerintah sama-sama mencurahkan sumber daya yang signifikan untuk merusak algoritma kriptografi tersebut (Tittel dkk, 2003).

Sebagai tambahan terhadap menjaga kerahasiaan, kriptografi sering diminta untuk melakukan pekerjaan lain:

1. **Kerahasiaan** (*confidentiality*) adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berkepentingan. Di dalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi cipherteks. Misalnya diberikan pesan: "Harap datang pukul 8" maka pesan disandikan menjadi "TrxC#45motyptre!%". Istilah lain yang sama dengan kerahasiaan adalah **secrecy** dan **privacy**.
2. **Autentikasi** (*authentication*) adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*). Dua pihak yang saling berkomunikasi harus dapat mengautentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diautentikasi sumbernya. Dengan kata lain, aspek keamanan ini dapat diungkapkan seperti pertanyaan berikut: "Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?" Autentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan autentikasi sumber pesan. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda tangan digital (*digital signature*).
3. **Integritas data** (*data integrity*) adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima masih asli atau tidak mengalami perubahan?" Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan yang

**gon code** menggunakan bahasa yang dipahami oleh sekelompok orang tapi tidak berarti ke yang lainnya. Jargon codes meliputi simbol-simbol yang digunakan untuk menandakan kehadiran dan jenis sinyal jaringan wireless (Archalking 2003).

**ered** atau **concealment ciphers** menyembunyikan pesan secara terbuka pada media pembawa sehingga dapat dikembalikan oleh orang yang mengetahui rahasia walaupun telah dirahasiakan.

# Daftar Pustaka

- Aguirre, Jorge Ramió. 2005. *Electronic Book About Computer Security and Cryptography*. [http://www.criptored.upm.es/guiateoria/gt\\_m001a.htm](http://www.criptored.upm.es/guiateoria/gt_m001a.htm).
- Arnold, M., Schmucker, M., and Wolthusen, S. D. 2003. *Techniques and Applications of Digital Watermarking and Content Protection*. Norwood, Massachusetts: Artech House.
- Bacon, Sir Francis. 1889. *De Augmentis Scientiarum*. Book 6.
- Barker, William C. 2004. *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*. NIST Special Publication 800-67 Version 1.
- Bishop, Matt. 2004. *Introduction to Computer Security*. Prentice Hall PTR.
- Braingle. 2007. *Polybius Square*. <http://www.braingle.com/brainteasers/codes/index.php>.
- Burton, Sir Richard F. 1991. *The Kamasutra of Vatsayana*. Arkana/Penguin.

Department of Computer Science and Information Systems. The University of Hong Kong. <http://www.csis.hku.hk/cisc/notes/english/index.html>.

Jonathan, Patrick Diskin, Samuel Lau, dan Robert Parlett. 2004. *Steganography*. Department of Computer Science. The University of Birmingham. <http://www.cs.bham.ac.uk/~jmr/teaching/modules03/security/students/SS5/Steganography.htm>.

Shannon, Claude. 1918. *Mathematical Foundations of Cryptography*. Instructional Horizons, Inc.

Shannon, Claude E. dan Kruh, L. 1985. *Machine Cryptographic and Modern Cryptanalysis*. Artech House, Inc.

Hellman, M. 1976. *New Directions in Cryptography*. IEEE Transactions on Information Theory.

Chapple, dan James Michael Stewart. 2003. *Certified Information Systems Professional*. SYBEX Inc.

*Cryptographic Coding for Data Bank Privacy*. IBM Research Report RC2827.

*Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication 197.

*Secure Hash Standard*. FIPS PUB 180-2 Federal Information Processing Standards Publication.

*The Keyed Hash Message Authentication Code (HMAC)*. FIPS PUB 198- Federal Information Processing Standards Publication.

*Digital Signature Standard (DSS)*. FIPS PUB 186-3 Federal Information Processing Standards Publication.

007. *Pigpen Cipher*. <http://freewebs.com/mcarter/personal/pigpen.pdf>.

008. 1995. *PGP: Pretty Good Privacy*. O'Reilly & Associates, Inc.

004. *Computational Number Theory and Algebra*. [http://cobweb.ecn.purdue.edu/~jacob/coursesiteach/compsec/Lecture/Lecture\\_5.pdf](http://cobweb.ecn.purdue.edu/~jacob/coursesiteach/compsec/Lecture/Lecture_5.pdf).

*Proceedings*. EUROCRYPT'90. Springer Verlag.

Iftene, Sorin. 2005. *Compartmented Secret Sharing Based on the Chinese Remainder Theorem*. <http://eprint.iacr.org/2005/408.pdf>.

Johnson, Neil F., and Sushil Jajodia. 1998. *Exploring Steganography: Seeing the Unseen*. IEEE Computer.

Kahn, David. 1967. *The Codebreakers*. Macmillan.

Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Penerbit Informatika.

Nichols, R. 1996. *Classical Cryptography Course*. Laguna Hills, CA: Aegean Park Press.

NIST. 2000. *Digital Signature Standard*. FIPS PUB 186-2, <http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf>.

Popa, R. 1998. *An Analysis of Steganographic Techniques*. The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering. [http://ad.informatik.uni-freiburg.de/mitarbeiter/will/dlib\\_bookmarks/digital-watermarking/popa/popa.pdf](http://ad.informatik.uni-freiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf).

Pretorius, Bertus. 2007. *Public Key Infrastructure Digital Certification*. <http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter5.htm>.

Price, Derek. J. 1995. *The Equatoric of the Planetis*. Edited from Peterhouse MS 75.1 Cambridge University Press.

Quadibloc. 2007. *Playfair and It's Relatives*. <http://www.quadibloc.com/crypto/pp1321.html>.

Rahayu, FS. 2005. *Proteksi dan Teknik Keamanan Sistem Informasi*. MTI-Fasilkom UI.

RFC2104. 1997. *HMAC: Keyed Hashing for Message Authentication*. <http://www.faqs.org/rfcs/rfc2104.html>.

Rhee, Man Young. 2003. *Internet Security: Cryptographic Principles, Algorithms, and Protocols*. John Wiley & Sons Ltd.

Rivest, Ronal L. 1994. *The RC5 Encryption Algorithm*.

Rolf Oppliger. 2005. *Contemporary Cryptography*. Artech House, Inc.

13. Steve Bellovin and Marcus Ranum. 1995. *Individual Personal Communications*.
- . 2007. *RSA - Wikipedia, the Free Encyclopedia*. <http://en.wikipedia.org/wiki/RSA>.
- ard, John J. G. 2000. *Playfair Cipher*. [http://en.wikipedia.org/wiki/Playfair\\_cipher](http://en.wikipedia.org/wiki/Playfair_cipher).
- heier. B. 1996. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Second Edition. John Wiley & Sons, Inc.
- mir, A. 1995. *Myths and Realities*. Invited talk at CRYPTO'95. Santa Barbara, CA.
- ey, R. 2000. *Internet Security Glossary, Request for Comments 2828*.
- armata. J. 2006. *Pengamanan Sistem Komputer*. Yogyakarta: Penerbit Andi.
- mp, Mark. 2006. *Information Security: Principles and Practice*. JohnWiley & Sons.
- St Denis dan Simon Johnson. 2007. *Cryptography for Developers*. Syngress Publishing.
- chalking. 2003. *Warchalking: Collaboratively Creating a Hobo Language for Free Wireless Networking (Online)*. <http://www.warchalking.org/>.
- Ruizhong. 2003. *Introduction to Network Security: Lecture Notes*. Department of Computer Science Lakehead University.
- pedia. 2006. *Data Encryption Standard*. [http://en.wikipedia.org/wiki/Data\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Data_Encryption_Standard).
- yun Wang, D., Feng, X. Lai., dan H. Yu. 2004. *Collision for Hash Function MD4, MD5, HAVAL-128, and RIPEMD, Rump Session, CRYPTO*.
- yun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, dan Xiuyuan Yu. 2007. *Cryptanalysis of the Hash Functions MD4 and RIPEMD*. China: Shandong University, Jinan, 250100. [www.infosec.sdu.edu.cn/paper/md4-ripemd-attck.pdf](http://www.infosec.sdu.edu.cn/paper/md4-ripemd-attck.pdf).

# Daftar Istilah

**Algorithm (Algoritma)** – suatu proses untuk melengkapi suatu tugas. Suatu algoritma enkripsi merupakan suatu proses yang pada umumnya suatu proses matematika untuk enkripsi dan dekripsi pesan.

**Asymmetric Algorithm (Algoritma Asimetris)** – suatu algoritma yang mana kunci yang digunakan untuk enkripsi adalah berbeda untuk dekripsi. Juga dikenal sebagai kriptografi kunci publik (*public key cryptography*).

**Authentication (Autentikasi)** – proses membuktikan suatu file atau pesan yang belum di ubah ketika diterima oleh penerima.

**Block Cipher (Sandi Blok)** – suatu algoritma yaitu enkripsi data pada blok-blok, pada umumnya masing-masing 64-bit.

**Caesar Cipher atau ROT Cipher (Sandi Caesar atau ROT)** – proses menciptakan suatu kode dengan mempercepat huruf dari pesan dengan jumlah huruf spesifik.

lain text numeric adalah ganjil  
i numeric pada karakter pertama adalah sama atau lebih dari 10  
ngkonversi setiap 2 nomor yang berurutan untuk satu karakter

```
plaintext_length/2,;  
plaintext(z)-48)*10)+(num_plaintext(z+1)-48);  
t = strcat(plaintext, char(q+'a'-1));
```

plaintext

lain text numeric adalah genap  
i numeric pada karakter pertama adalah sama atau kurang dari 10  
konversi nomor pertama untuk karakter pertama

```
plaintext_length/2) + 1;  
text(1)-48;  
char(q+'a'-1);
```

```
n_plaintext(z)-48)*10)+(num_plaintext(z+1)-48);  
t = strcat(plaintext, char(q+'a'-1));
```

plaintext

# Tentang Penulis



**Dr. Janner Simarmata, S.T., M.Kom.**

Janner Simarmata saat ini bekerja di Universitas Negeri Medan sebagai Dosen. Penulis merupakan lulusan S-3 Pendidikan Teknologi Kejuruan dari Universitas Pendidikan Indonesia (UPI) dengan konsentrasi Pendidikan Informatika bidang kajian Blended Learning. Penulis aktif menulis buku sejak tahun 2006 dan saat ini menjabat sebagai Founder/CEO pada Yayasan Kita Menulis.





### **Robbi Rahim**

Robbi Rahim merupakan salah satu dosen di Sekolah Tinggi Ilmu Manajemen Sukma. Robbi Rahim menyelesaikan jenjang pendidikan S-1 dari STMIK Budi Darma, program Magister (S-2) dari Universitas Sumatera Utara, dan saat ini dalam tahap penyelesaian Program Doktor (S-3) dari Universitas Malaysia Perlis.

Robbi Rahim mengambil konsentrasi penelitian di bidang keamanan komputer terutama Kriptografi, Steganography, dan juga mengeksplorasi Sistem Pendukung Keputusan, Aplikasi Game dan Jaringan.



### **Drs. Sriadhi, S.T., M.Pd., M.Kom., Ph.D.,**

Drs. Sriadhi, S.T., M.Pd., M.Kom., Ph.D., lahir di Asahan Sumatra Utara pada tahun 1963. Menyelesaikan pendidikan S-1 di IKIP Medan dan UISU, program Magister Pendidikan di IKIP Bandung, dan Magister Komputer dari UPI YPTK Padang, serta Program Doktor dari Universitas Sains Malaysia dalam bidang Komputer Multimedia. Bertugas sebagai dosen tetap Universitas Negeri Medan pada program studi Pendidikan Teknik Informatika dan Komputer. Aktif dalam bidang penelitian dan publikasi, serta aktif sebagai narasumber bidang ICT. Penulis berpengalaman sebagai pemenang beberapa hibah nasional dan internasional serta aktif sebagai pengembang sistem informasi akademik dan e-learning.

Data dan informasi adalah sebuah aset yang paling berharga bagi perusahaan, organisasi, maupun perusahaan. Maka dari itu, data dan informasi tersebut perlu untuk dijaga. Di dalam buku ini, disajikan bagaimana cara untuk mengamankan data dan informasi tersebut yang dikenal dengan istilah Kriptografi. Kriptografi juga sering disebut "studi enkripsi" yang berasal dari bahasa Yunani. Kriptografi atau "kode rahasia" adalah alat keamanan informasi yang sangat mendasar. Kriptografi sendiri telah banyak digunakan, termasuk untuk melindungi kerahasiaan dan integritas data. Buku ini mengupas kriptografi klasik sampai modern, disertai beberapa contoh-contoh dan latihan-latihan, serta beberapa listing program (lampiran) untuk memperdalam ilmu kriptografi. Hal-hal yang akan dibahas di dalam buku ini sebagai berikut:

- Pengantar Kriptografi
- Kriptografi Klasik
- Stream dan Block Cipher
- Data Encryption Standard (DES)
- International Data Encryption Algorithm (IDEA)
- Advanced Encryption Standard (AES)
- Message Digest Algorithm
- Secure Hash Standard
- The Keyed Hash Message Authentication Code (HMAC)
- Kriptosistem Kunci Publik Rivest Shamir Adleman (RSA)
- Kriptosistem Kunci Publik ElGamal
- Algoritme Knapsack
- Pretty Good Privacy (PGP)
- Tanda Tangan Digital
- Steganografi

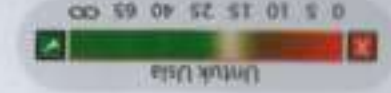
# KRIPTOGRAFI

Teknik Keamanan Data & Informasi

COMPUTING & INTERNET  
ISBN: 978-623-01-0286-2



Harga di Pulau Jawa: Rp132.000,00



Penerbit ANDI  
Jl. Buo 38-40 Yogyakarta  
Telp. (0274) 561881 Fax. (0274) 588282  
E-mail: andipenerbitan@gmail.com | www.andipublisher.com

Dapatkan Info Buku Baru, Kirim e-mail: info@andipublisher.com | andipublisher.com@yahoo.com

Janner Simarmata  
Sriadhi  
Robbi Rahim

KRIPTOGRAFI Teknik Keamanan Data & Informasi

