KRIPTOGRAFI

Teknik Keamanan Data & Informasi

Janner Simarmata | Sriadhi | Robbi Rahim

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

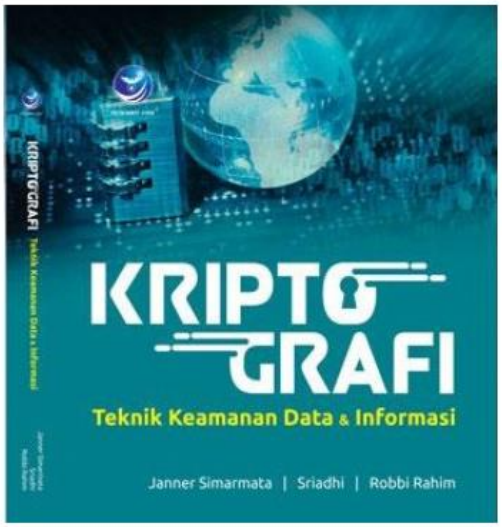
MOBILE VERSION
ANDROID VERSION

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



Kategori(Sub)	: Komputer (Ilmu Komputer)
ISBN	: 978-623-01-0288-2
Penulis	: Janner Simarmata, Sriadhi Dan Robbi Rahim
Ukuran/Halaman	: 19x23 cm² / xvi+392 halaman
Edisi/Cetakan	: I, 1st Published
Tahun Terbit	: 2020
Berat	: 612 gram
Harga	: Rp 132.000,- Diskon 20%
Harga Diskon	: Rp 105.600,-

Sinopsis

KRIPTOGRAFI

Teknik Keamanan Data & Informasi

Janner Simarmata | Sriadhi | Robbi Rahim

KRIPTOGRAFI
Teknik Keamanan Data dan Informasi
Oleh: Janner Simarmata, Sriadhi, dan Robbi Rahim

Editor : Marcella Kika
Setting : yulius basuki
Desain Cover : Dany Nofianto
Korektor : Yulia Fransisca A.

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 + 392hlm ; 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, akhirn
ini dapat juga terselesaikan, walaupun banyak hambatan yang penul
selama penulisan buku ini. Penulis mengucapkan banyak terim
kepada sahabat-sahabat yang telah memberikan masukan.

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

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

Medan, November 2018

Penulis

Daftar Isi

Bab 1

Pengantar Kriptografi

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

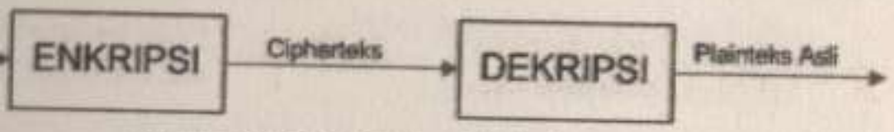
Misalkan seorang pengirim ingin mengirimkan suatu pesan kepada penerima, maka si pengirim ingin pesan yang akan dikirim dalam keadaan aman, si pengirim ingin meyakinkan bahwa penyusup tidak bisa membaca pesan tersebut.

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
er dan ***decipher*** atau istilah lain disebut juga ***encrypt*** dan ***decrypt***).

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



Gambar 1.1 Enkripsi dan dekripsi

dai dengan *M* untuk pesan, atau *P* untuk plainteks. Ini bisa merupakan
, file teks, bitmap, aliran suara digital, dan citra video digital, sedangkan
biner. Cipherteks ditandai dengan *C*. Ini juga data biner, kadang-kadang
a seperti *M*.

E, beroperasi pada *M* untuk menghasilkan *C*. Berikut adalah notasi
:

ses kebalikannya, yaitu fungsi dekripsi *D* beroperasi pada *C* untuk
M:

tografi

diakan, tingkat keamanan yang ditambahkan ke data selama
mpanan, dan komunikasi. Selama bertahun-tahun, matematikawan
uter mengembangkan serangkaian algoritma yang semakin kompleks,
ma 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
npi tidak berarti ke yang lainnya. Jargon codes meliputi simbol-simbol yang
unakan untuk menandakan kehadiran dan jenis sinyal jaringan wireless
archalking 2003).

vered* atau *concealment ciphers menyembunyikan pesan secara terbuka
la media pembawa sehingga dapat dikembalikan oleh orang yang
ngetahui rahasia walaupun telah dirahasiakan.

Daftar Pustaka

Aguirre, Jorge Ramió. 2005. *Electronic Book About Computer Security and Crypthography*.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 Scientarum*. 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.

epartment of Computer Science and Information Systems. The University of ong. http://www.csis.hku.hk/cisc/notes/english/index.html.

athan, Patrick Diskin, Samuel Lau, dan Robert Parlett. 2004. *Steganography*. of Computer Science. The University of Birmingham. http://www.cs.bham. mdr/teaching/modules03/security/students/SS5/Steganography.htm.

on. 1997. *Encyclopedia of Cryptology*. Instructional Horizons, Inc.

dan Kruh, L. 1985. *Machine Cryptographic and Modern Cryptanalysis*. Artech

Hellman, M. 1976. *New Directions in Cryptographic*. IEEE Transactions on tion 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 ds Publication 197.

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

e Keyed Hash Message Authentication Code (HMAC). FIPS PUB 198- Federal tion Processing Standards Publication.

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

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

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

004. *Computational Number Theory and Algebra*. http://cobweb.ecn.purdue. ak/coursesiteach/compsec/Lecture/Lecture_5.pdf.

eedings". 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.

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.I 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.
neier. B. 1996. *Applied Cryptography: Protocols, Algorthms, 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.
np, 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.
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.

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 numberic adalah ganjil
i numberic pada karakter pertama adalah sama atau lebih dari 10
gkonversi setiap 2 nomor yang berurutan untuk satu karakter


intext_length/2,;
laintext(z)-48)*10)+(num_plaintext(z+1)-48);
 $rcat(plaintext,char(q+'a'-1));


aintext

 plain text numberic adalah genap
lai numberic pada karakter pertama adalah sama atau kurang dari 10
versi nomor pertama untuk karakter pertama

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


_plaintext(z)-48)*10)+(num_plaintext(z+1)-48);
 = $rcat(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 perorangan, 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

Penerbit ANDI
Jl. Beo 38-40 Yogyakarta
Telp.(0274) 561881 Fax.(0274) 588282
andipenerbitan@gmail.com
www.andipublisher.com

Untuk Usia
0 5 10 15 25 40 65

COMPUTING & INTERNET
ISBN: 978-623-01-0288-2
Harga di Pulau Jawa: Rp132.000,00

KRIPTOGRAFI Teknik Keamanan Data & Informasi

Janner Simarmata
Sriadhi
Robbi Rahim