

ABSTRAK

Keamanan informasi merupakan hal yang sangat penting dan salah satu unsur dari keamanan informasi adalah integritas data yang dimana data diterima sama dengan data yang dikirimkan.

MessageDigest 5 adalah salah satu teknik yang dapat menunjang tentang integritas data dengan menggunakan teori fungsi hash untuk algoritmanya. Apabila data diubah dalam proses pengiriman. MessageDigest 5 dapat mengetahui perubahan data dalam proses pengiriman.

MessageDigest 5 akan dibuat menggunakan bahasa JAVA. Bahasa JAVA adalah bahasa yang berbasis object oriented, bahasa yang multiplatform yang amat cocok untuk membuat program yang digunakan jaringan

Hasil program MessageDigest 5 yang menggunakan bahasaJAVA setelah dibandingkan dengan hasil dari memo yang dibuat oleh pencipta MD5 Ron Rivest dapat disimpulkan bahwa program telah berjalan sesuai dengan algoritmanya.

ABSTRACT

Information security is very important matter and one of element from information security is data integrity which is where data accepted equal to delivered data.

MessageDigest 5 one of technique which can support about data integrity by using theory of function hash for the algorithm of its. If data altered of delivery. MessageDigest 5 can know the data change course of delivery.

MessageDigest 5 will be made in JAVA language. JAVA language is being based on object oriented, which multiplatform very suited for making program used by network

Result of program MessageDigest 5 which JAVA after compared to by result from memo which made by creator of MessageDigest 5 Ron Rivest that program have walked as according to its algorithm.

DAFTAR ISI

ABSTRAK	i
<i>ABSTRACT</i>	ii
KATA PENGANTAR.....	iii
DAFTAR ISI.....	iv
DAFTAR GAMBAR.....	vii
DAFTAR TABEL	viii
BAB I PENDAHULUAN.....	1
I.1 Latar Belakang.....	1
I.2 Indentifikasi Masalah	3
I.3 Tujuan	3
I.4 Pembatasan Masalah.....	3
I.5 Sistematika Pembahasan.....	3
BAB II LANDASAN TEORI	5
II.1 Fungsi Hash.....	5
II.1.1 Algoritma Fungsi Hash	7
II.1.1.1 Snefru	7
II.1.1.2 N-Hash	7
II.1.1.3 MD2, MD4, RIPE-MD, Haval	7
II.1.1.4 Secure Hash Algoritma(SHA)	9
II.1.2 Penggunaan Fungsi Hash	9
II.1.2.1 Pseudo Random Functions	9
II.1.2.2 Keamanan Protocol Internet.....	10
II.1.2.3 Autentikasi pada HTTP	11

II.1.2.4 Biometrics	11
II.1.2.5 Challenge Handshake Authentictio Protocol	12
II.1.2.6 Jaringan LAN Nirkabel	13
II.1.2.7 DoS Attacks.....	13
II.1.2.8 Integritas Data	14
II.1.2.9 Pemblokiran URLs dan Mailicious Mobile Code	15
II.1.2.10 XML Signature.....	15
II.1.2.11 Personal Firewalls	15
II.2 Message Digest 5	16
II.2.1 Cara Kerja MD5	17
II.2.1.1 Proses HMD5	23
BAB III PERNCANGAN PROGRAM MD5	29
3.1 Inisialisasi Variable aBuf dan bBuf	30
3.2 Input String m dan Array m	31
3.3 Pengulangan While	31
3.4 Array aBuf[bBuf++]	32
3.5 Blok 512 bit.....	32
3.6 Padding	33
3.7 Penambahan Panjang	33
3.8 Proses Blok	34
3.9 Konversi Bilangan Heksa	35
BAB IV HASIL PERCOBAAN	36
IV.1 Pengujian Hasil Program	36
IV.1.1 Input Berbeda-beda.....	36
IV.1.2 Panjang Input Berbeda Karater Sama.....	37
IV.1.3 Panjang Input Sama Karakter Berbeda.....	39

IV.1.4 Percobaan Data Dalam Proses Pengiriman Dirubah	40
IV.1.5 Percobaan Perbandingan Dengan Ron Rivest	42
BAB V KESIMPULAN DAN SARAN	46
V.I Kesimpulan	47
V.II Saran	47
 DAFTAR PUSTAKA	
LAMPIRAN	

DAFTAR GAMBAR

Gambar 2.1 Operasi Fungsi Hash Sederhana dengan Operasi XOR.....	6
Gambar 2.2 Penggunaan HMAC dalam IPv6 dalam mode Authentiction Header	11
Gambar 2.3 Penggunaan Fungsi Hash pada CHAP	12
Gambar2.4 Message Digest MD5	16
Gambar 2.5 Proses Padding Bit	17
Gambar 2.6 Penambahan Panjang	18
Gambar 2.7 Proses dalam Satu Blok 512 bit	20
Gambar 2.8 Dasar Operasi MD5 dalam Satu Kali.....	24
Gambar 3.1 Diagram Alir MD5Hash.....	29
Gambar 4.1 Input Kesatu Memasukan Data Lady.....	41
Gambar 4.2 Input Kedua Memasukan Data Lady dan Dibandingkan	41
Gambar 4.3 Percobaan Ketika Data Dirubah Ditengah Jalan	45
Gambar 4.4 Perbandingan Dengan Ron Rivest Dengan Input a Dan abc.....	44
Gambar 4.5 Perbandingan Dengan Ron Rivest	45

DAFTAR TABEL

Tabel 2.1 Buffer A, B, C, D.....	19
Tabel 2.2a Tabel Kebenaran dari Fungsi Logika F, G, H, I.....	21
Tabel 2.2b Table T	22
Tabel 2.3 Fungsi g.....	24
Tabel 2.4 Rincian Operasi dalam Fungsi F(b, c, d)	25
Tabel 2.4 Rincian Operasi dalam Fungsi G(b, c, d).....	26
Tabel 2.4 Rincian Operasi dalam Fungsi H(b, c, d).....	27
Tabel 2.4 Rincian Operasi dalam Fungsi F(b, c, d)	28
Tabel 4.1 Hasil Percobaan Input Berbeda.....	36
Tabel 4.2a Percobaan Panjang Input Berbeda Karakter Sama.....	37
Tabel 4.2b Lanjutan	38
Tabel 4.3 Percobaan Panjang Input Sama Karakter Berbeda	39
Tabel 4.4 Perbandingan dengan Hasil dari Ron Rivest	43