PP/018/V/R2

LABORATORIUM
TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS AHMAD DAHLAN

PETUNJUK PRAKTIKUM

EDISI KURIKULUM OBE

KEAMANAN KOMPUTER

Penyusun:
Nur Rochmah Dyah P.A., ST.,M.Kom
Eko Aribowo ST.,M.Kom
Nuril Anwar ST., M.Kom
Faisal Fajri Rahani, S.Si., M.Cs.

2021

HAK CIPTA

PETUNJUK PRAKTIKUM NAMA PRAKTIKUM

Diterbitkan oleh:
Program Studi Teknik Informatika
Fakultas Teknologi Industri
Universitas Ahmad Dahlan
Jalan Ring Road Selatan, Tamanan, Banguntapan, Bantul Yogyakarta 55166

Penulis	: Nur Rochmah Dyah P.A., ST.,M.Kom Eko Aribowo ST.,M.Kom Nuril Anwar ST., M.Kom Faisal Fajri Rahani, S.Si., M.Cs.
Editor	: Laboratorium Teknik Informatika, Universitas Ahmad Dahlan
Desain sampul	: Laboratorium Teknik Informatika, Universitas Ahmad Dahlan
Tata letak	: Laboratorium Teknik Informatika, Universitas Ahmad Dahlan
Ukuran/Halaman	: 21 x 29,7 cm / 83 halaman

Didistribusikan oleh:

Laboratorium Teknik Informatika
Universitas Ahmad Dahlan
Jalan Ring Road Selatan, Tamanan, Banguntapan, Bantul Yogyakarta 55166
Indonesia

KATA PENGANTAR

Alhamdulilllah, segala puji dan syukur kehhadirat Allah SWT, hanya atas rahmat dan hidayah-Nya lah akhirnya buku petunjuk praktikum kuliah Keamanan Komputer telah terselesaikan. Cakupan Keamanan Komputer membahas tentang metode-metode yang dapat digunakan dalam pengamanan data digital dan jaringan internet antara lain : penggunaan autentikasi, kriptografi, steganografi, firewall, wireless security, digital signature, dll.

Petunjuk praktikum mahasiswa berisi langkah-langkah pada kegiatan praktikum untuk mahasiswa semester IV di program studi Teknik Informatika Universitas Ahmad Dahlan. Capaian kompetensi setelah mahasiswa mengikuti kegiatan praktikum dalam mata kuliah keamanan komputer adalah mahasiswa mampu mengimplemtasikan konsep dasar kriptogri dan fungsi dalam kaitannya dengan keamanan komputer. Mampu menganaalisa dan mengimplementasikan sistem pengamanan data dan jaringan dengan metode firewall, steganografi. Mampu memberikan analisa atas perkembangan teknik pengamanan dan serangan yang ada pada sistem jaringan.

Penulis mengucapkan terima kasih kepada Dimas chaerul mahasisiwa Teknik Informatika yang telah membatu dalam penulisnapetunjuk praktikum ini. Dan juga semua pihak yang tentunya tidak bisa penulis sebutkan satu persatu yang telah membantu dalam penyusunan. Tentu saja buku ini masih jauh dari memuaskan, namun penulis berharap buku ini dapat bermanfaat bagi mahasiswa. Saran dan kritik sangatlah penulis harapkan, untuk perkembangan selanjutnya.

Yogyakarta, 1 Agustus 2021

Penyusun

DAFTAR PENYUSUN

Nur Rochmah Dyah P.A., ST.,M.Kom
Eko Aribowo ST.,M.Kom
Nuril Anwar ST., M.Kom
Faisal Fajri Rahani, S.Si., M.Cs.

HALAMAN REVISI

Yang bertanda tangan di bawah ini:

Nama : Nur Rochmah Dyah P.A., S.T., M.Kom

NIP : 1908762005012001

Jabatan : Koordinator Mata kuliah Keamanan Komputer

Dengan ini menyatakan pelaksanaan Revisi Petunjuk Praktikum Keamanan Komputer untuk Program Studi Teknik Informatika telah dilaksanakan dengan penjelasan sebagai berikut:

No	Keterangan Detail Revisi (Per Pertemuan)	Tanggal Revisi	Nomor Modul
1	Menambahkan teori dan petunjuk kegiatan materi Management password, pada Praktikum 1	25 Agustus 2019	PP/018/V/R1
2	Menambahkan teori dan petunjuk kegiatan materi MD 5 dan Fungsi Hash, pada Praktikum 3.	25 Agustus 2019	PP/018/V/R1
3	Merevisi petunjuk praktikum ke template yang baru.	25 Agustus 2019	PP/018/V/R1
4	Melengkapi halaman cover dari petunjuk praktikum.	25 Agustus 2019	PP/018/V/R1
5	Merevisi petunjuk praktikum ke template OBE.	1 Agustus 2021	PP/018/V/R2

Yogyakarta, 1 Agustus 2021

Penyusun

Nur Rochmah Dyah P.A., S.T., M.Kom

NIP. 197608192005012001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Lisna Zahrotun, S.T., M.Cs.

NIK/NIY : 60150773

Jabatan : Kepala Laboratorium Teknik Informatika

Menerangkan dengan sesungguhnya bahwa Petunjuk Praktikum ini telah direview dan akan digunakan untuk pelaksanaan praktikum di Semester Gasal Tahun Akademik 2021/2022 di Laboratorium Praktikum Teknik Informatika, Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan.

Yogyakarta, 1 Agustus 2021

Mengetahui, Ketua Kelompok Keilmuan Relata	Kepala Laboratorium Teknik Informatika
Guntur Maulana Zamroni, B.Sc. M. Kom	**Lisna Zahrotun, S.T., M.Cs.**
NIY. 60181172	NIY. 60150773

VISI DAN MISI PRODI TEKNIK INFORMATIKA

VISI

Menjadi Program Studi Informatika yang diakui secara internasional dan unggul dalam bidang Informatika serta berbasis nilai-nilai Islam.

MISI

1. Menjalankan pendidikan sesuai dengan kompetensi bidang Informatika yang diakui nasional dan internasional
2. Meningkatkan penelitian dosen dan mahasiswa dalam bidang Informatika yang kreatif, inovatif dan tepat guna.
3. Meningkatkan kuantitas dan kualitas publikasi ilmiah tingkat nasional dan internasional
4. Melaksanakan dan meningkatkan kegiatan pengabdian masyarakat oleh dosen dan mahasiswa dalam bidang Informatika.
5. Menyelenggarakan aktivitas yang mendukung pengembangan program studi dengan melibatkan dosen dan mahasiswa.
6. Menyelenggarakan kerja sama dengan lembaga tingkat nasional dan internasional.
7. Menciptakan kehidupan Islami di lingkungan program studi.

TATA TERTIB LABORATORIUM TEKNIK INFORMATIKA

DOSEN/KOORDINATOR PRAKTIKUM

1. Dosen harus hadir saat praktikum minimal 15 menit di awal kegiatan praktikum untuk mengisi materi dan menandatangani presensi kehadiran praktikum.
2. Dosen membuat modul praktikum, soal seleksi asisten, pre-test, post-test, dan responsi dengan berkoordinasi dengan asisten dan pengampu mata praktikum.
3. Dosen berkoordinasi dengan koordinator asisten praktikum untuk evaluasi praktikum setiap minggu.
4. Dosen menandatangani surat kontrak asisten praktikum dan koordinator asisten praktikum.
5. Dosen yang tidak hadir pada slot praktikum tertentu tanpa pemberitahuan selama 2 minggu berturut-turut mendapat teguran dari Kepala Laboratorium, apabila masih berlanjut 2 minggu berikutnya maka Kepala Laboratorium berhak mengganti koordinator praktikum pada slot tersebut.

PRAKTIKAN

1. Praktikan harus hadir 15 menit sebelum kegiatan praktikum dimulai, dan dispensasi terlambat 15 menit dengan alasan yang jelas (kecuali asisten menentukan lain dan patokan jam adalah jam yang ada di Laboratorium, terlambat lebih dari 15 menit tidak boleh masuk praktikum & dianggap Inhal).
2. Praktikan yang tidak mengikuti praktikum dengan alasan apapun, wajib mengikuti INHAL, maksimal 4 kali praktikum dan jika lebih dari 4 kali maka praktikum dianggap GAGAL.
3. Praktikan harus berpakaian rapi sesuai dengan ketentuan Universitas, sebagai berikut:
   - Tidak boleh memakai Kaos Oblong, termasuk bila ditutupi Jaket/Jas Almamater (Laki-laki / Perempuan) dan Topi harus Dilepas.
   - Tidak Boleh memakai Baju ketat, Jilbab Minim dan rambut harus tertutup jilbab secara sempurna, tidak boleh kelihatan di jidat maupun di punggung (khusus Perempuan).
   - Tidak boleh memakai baju minim, saat duduk pun pinggang harus tertutup rapat (Laki-laki / Perempuan).
   - Laki-laki tidak boleh memakai gelang, anting-anting ataupun aksesoris Perempuan.
4. Praktikan tidak boleh makan dan minum selama kegiatan praktikum berlangsung, harus menjaga kebersihan, keamanan dan ketertiban selama mengikuti kegiatan praktikum atau selama berada di dalam laboratorium (tidak boleh membuang sampah sembarangan baik kertas, potongan kertas, bungkus permen baik di lantai karpet maupun di dalam ruang CPU).
5. Praktikan dilarang meninggalkan kegiatan praktikum tanpa seizin Asisten atau Laboran.
6. Praktikan harus meletakkan sepatu dan tas pada rak/loker yang telah disediakan.
7. Selama praktikum dilarang NGENET/NGE-GAME, kecuali mata praktikum yang membutuhkan atau menggunakan fasilitas Internet.
8. Praktikan dilarang melepas kabel jaringan atau kabel power praktikum tanpa sepengetahuan laboran
9. Praktikan harus memiliki FILE Petunjuk praktikum dan digunakan pada saat praktikum dan harus siap sebelum praktikum berlangsung.
10. Praktikan dilarang melakukan kecurangan seperti mencontek atau menyalin pekerjaan praktikan yang lain saat praktikum berlangsung atau post-test yang menjadi tugas praktikum.

11. Praktikan dilarang mengubah setting software/hardware komputer baik menambah atau mengurangi tanpa permintaan asisten atau laboran dan melakukan sesuatu yang dapat merugikan laboratorium atau praktikum lain.
12. Asisten, Koordinator Praktikum, Kepala laboratorium dan Laboran mempunyai hak untuk menegur, memperingatkan bahkan meminta praktikan keluar ruang praktikum apabila dirasa anda mengganggu praktikan lain atau tidak melaksanakan kegiatan praktikum sebagaimana mestinya dan atau tidak mematuhi aturan lab yang berlaku.
13. Pelanggaran terhadap salah satu atau lebih dari aturan diatas maka Nilai praktikum pada pertemuan tersebut dianggap 0 (NOL) dengan status INHAL.

ASISTEN PRAKTIKUM

1. Asisten harus hadir 15 Menit sebelum praktikum dimulai (konfirmasi ke koordinator bila mengalami keterlambatan atau berhalangan hadir).
2. Asisten yang tidak bisa hadir WAJIB mencari pengganti, dan melaporkan kepada Koordinator Asisten.
3. Asisten harus berpakaian rapi sesuai dengan ketentuan Universitas, sebagai berikut:
   a. Tidak boleh memakai Kaos Oblong, termasuk bila ditutupi Jaket/Jas Almamater (Laki-laki / Perempuan) dan Topi harus Dilepas.
   b. Tidak Boleh memakai Baju ketat, Jilbab Minim dan rambut harus tertutup jilbab secara sempurna, tidak boleh kelihatan di jidat maupun di punggung (khusus Perempuan).
   c. Tidak boleh memakai baju minim, saat duduk pun pinggang harus tertutup rapat (Laki-laki / Perempuan).
   d. Laki-laki tidak boleh memakai gelang, anting-anting ataupun aksesoris Perempuan.
4. Asisten harus menjaga kebersihan, keamanan dan ketertiban selama mengikuti kegiatan praktikum atau selama berada di laboratorium, menegur atau mengingatkan jika ada praktikan yang tidak dapat menjaga kebersihan, ketertiban atau kesopanan.
5. Asisten harus dapat merapikan dan mengamankan presensi praktikum, Kartu Nilai serta tertib dalam memasukan/Input nilai secara Online/Offline.
6. Asisten harus dapat bertindak secara profesional sebagai seorang asisten praktikum dan dapat menjadi teladan bagi praktikan.
7. Asisten harus dapat memberikan penjelasan/pemahaman yang dibutuhkan oleh praktikan berkenaan dengan materi praktikum yang diasisteni sehingga praktikan dapat melaksanakan dan mengerjakan tugas praktikum dengan baik dan jelas.
8. Asisten tidak diperkenankan mengobrol sendiri apalagi sampai membuat gaduh.
9. Asisten dimohon mengkoordinasikan untuk meminta praktikan agar mematikan komputer untuk jadwal terakhir dan sudah dilakukan penilaian terhadap hasil kerja praktikan.
10. Asisten wajib untuk mematikan LCD Projector dan komputer asisten/praktikan apabila tidak digunakan.
11. Asisten tidak diperkenankan menggunakan akses internet selain untuk kegiatan praktikum, seperti Youtube/Game/Medsos/Streaming Film di komputer praktikan.

LAIN-LAIN

1. Pada Saat Responsi Harus menggunakan Baju Kemeja untuk Laki-laki dan Perempuan untuk Praktikan dan Asisten.
2. Ketidakhadiran praktikum dengan alasan apapun dianggap INHAL.
3. Izin praktikum mengikuti aturan izin SIMERU/KULIAH.
4. Yang tidak berkepentingan dengan praktikum dilarang mengganggu praktikan atau membuat keributan/kegaduhan.

5. Penggunaan lab diluar jam praktikum maksimal sampai pukul 21.00 dengan menunjukkan surat ijin dari Kepala Laboratorium Prodi Teknik Informatika.

Yogyakarta, 1 Agustus 2021

Kepala Laboratorium Teknik Informatika

Lisna Zahrotun, S.T., M.Cs.
NIY. 60150773

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

SKENARIO PRAKTIKUM SECARA DARING

Nama Mata Praktikum : Keamanan Komputer
Jumlah Pertemuan : 11

TABEL SKENARIO PRAKTIKUM DARING

Pertemuan ke	Judul Materi	Waktu	Skenario Praktikum
1	Pengenalan Kriptografi	3 Hari	Google Classroom, video, whatsapp group.
2	Pengenalan Kriptografi Modern	3 Hari	Google Classroom, video, whatsapp group.
3	Information Hiding	3 Hari	Google Classroom, video, whatsapp group.
4	Authentication	3 Hari	Google Classroom, video, whatsapp group.
5	Password Management	3 Hari	Google Classroom, video, whatsapp group.
6	Digital Signature	3 Hari	Google Classroom, video, whatsapp group.
7	Sql Injection	3 Hari	Google Classroom, video, whatsapp group.
8	Firewall	3 Hari	Google Classroom, video, whatsapp group.
9	Dos Dan Ddos	3 Hari	Google Classroom, video, whatsapp group.
10	Wireless Network Security	3 Hari	Google Classroom, video, whatsapp group.
11	Analisa Paket Data	3 Hari	Google Classroom, video, whatsapp group.

PRAKTIKUM 1: PENGENALAN KRIPTOGRAFI

Pertemuan ke : 1

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 35 %
- Praktik : 40 %
- Post-Test : 25 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-02	Kemampuan memahami dan menerapkan konsep kriptografi, steganografi, digital signature dan manajemen key untuk meningkatkan kemanan.

1.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:
1 Menjelaskan konsep enkripsi.
2 Menerapkan penggunaan konsep.

1.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-02	Mahasisiwa memaham dan menerapkan kriptografi monoalphabetic, polyalphabetic, block cipher dan stream cipher.

1.3 TEORI PENDUKUNG

A. Caesar

Metode ini menggunakan pergeseran sederhana, sehingga metode ini tergolong dalam kelompok metode stream. Algoritma dasar dari metode ini sangat simple, setiap kunci diganti dengan huruf ketiga setelah kunci yang bersangkutan. Misalnya kita memiliki plaintext seperti berikut.

I CAME I SAW I CONQUERED

Maka kalau kita enkripsikan dengan metode ini, didapatkan cipherteksnya adalah

L FDPH L VDZ L FRQTXHUHG

Atau secara umum substitusi tersebut dapat digambarkan seperti berikut :

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Plain :	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher :	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Secara umum proses Cipher dapat didefinisikan enkripsi dapat dikodekan dengan :
Enkripsi : **Ek : i → (i+k) mod 26**
Dekripsi : **Dk : i → (i-k) mod 26**

Keterangan :
i : huruf yang akan dienkripsi/dekripsi
k : kunci (pada Caesar cipher maka kunci adalah 3)

Modulus 26 digunakan untuk plaintext dengan basis 26 karakter. Untuk plainteks dengan basis ASCII maka digunakan modulus 256

B. Vigenere

Metode ini juga merupakan dasar dari polyalphabetic substitution cipher. Beberapa ketentuan dalam metode ini antara lain :

- Setiap kunci dapat disubstitusi dengan bermacam-macam kunci yang lain.
- Menggunakan kata kunci.
- Kata kunci digunakan secara berulang.
- Kata kunci digunakan untuk menetukan enkripsi setiap alphabet dalam plainteks.
- Huruf ke-i dalam plainteks dispesifikasikan oleh alphabet yang digunakan dalam kunci.
- Penggunaan alphabet bisa berluang.

Contoh, kita akan melakukan enkripsi pesan plainteks :

Pi : TO BE OR NOT TO BE THAT IS THE QUESTION

Dengan menggunakan kata kunci RELATIONS. Kita mulai dengan menuliskan kunci, berulang kali di bagian atas plaintext message.

Keyword :	R	E	L	A	T		I	O	N	S	R		E	L	A	T	I		O	N	S	R	E		L	A	T	I	O		N	S	R	E	L
Plaintext :	T	O	B	E	O		R	N	O	T	T		O	B	E	T	H		A	T	I	S	T		H	E	Q	U	E		S	T	I	O	N
Ciphertext:	K	S	M	E	H		Z	B	B	L	K		S	M	E	M	P		O	G	A	J	X		S	E	J	C	S		F	L	Z	S	Y

Secara umum proses enkripsi pada vigenere dapat dituliskan :

Ek : Ci → (Mi + (Kj – A)) mod 26

Untuk Dekripsi maka:

Pi = (Ci – Ki) mod 26

Keterangan :

Ci : nilai decimal karakter ciphertext ke-i

Pi : nilai decimal karakter plaintext ke-i

Ki : nilai decimal karakter kunci ke-i

1.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Dev C++
3. Tabel ASCII

1.5 PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-02	Jelaskan apa itu kriptografi !	25
2.	CPL-07	CPMK-02	Sebutkan dan Jelaskan Jenis - Jenis kriptografi !	25
3.	CPL-07	CPMK-02	Enkripsikan Plaintext Berikut kedalam Caesar Cipher Plaintext : Saya (Nama Lengkap) Mahasiswa Faktultas Teknologi Industri Teknik Informatika Universitas Ahmad Dahlan Kerjakan lengkap dengan langkah2nya !	50

1.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-02	Selesaikan langkah praktikum	Hasil praktikum langkah	100

Langkah-Langkah Praktikum:

1. Buka Dev C++
2. Membuat program C++ untuk proses enkripsi dan dekripsi kalimat (belum ada source code nya)
3. Jalankan.

1.7 POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-02	Lakukan Proses Enkripsi dan dekripsi dengan Metode vigenere secara manual pada plaintext: Plaintext : TEKNIK INFORMATIKA FTI UNIVERSITAS AHMAD DAHLAN YOGYAKARTA Key : GADALAWAN	30
2.	CPL-07	CPMK-02	Berdasarakan Proses Enkripsi dan deskripsi yang anda lakukan pada soal point 1 maka implementasikanlah kedalam program menggunakan C++.	70

1.8 HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-02	20%		
2.	Praktik	CPL-07	CPMK-02	30%		
3.	Post-Test	CPL-07	CPMK-02	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 2: PENGENALAN KRIPTOGRAFI MODERN

Pertemuan ke : 2

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 35 %
- Praktik : 40 %
- Post-Test : 25 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah
CPMK-02	Kemampuan memahami dan menerapkan konsep kriptografi, steganografi, digital signature dan manajemen key untuk meningkatkan kemanan.

2.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

1 Memahami konsep dan peneranapan Kriptografi Asimetrik dan Public Key Infrastructure.

2.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-02	Mahasisiwa mampu memahami dan menerapkan kriptografi Asymetric cryptography & Public Key Infrastructure: Komponen-komponen, kebijakan, penerapan hash function, secret sharing

2.3 TEORI PENDUKUNG

Dalam kriptografi, ***MD5* (*Message-Digest algorithm* 5)** ialah fungsi *hash* kriptografik yang digunakan secara luas dengan *hash* value 128-bit. Pada standard Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan untuk melakaukan autentikasi suatu data digital atau pengujian integritas sebuah file.

MD5 didesain oleh Ronald Rivest pada tahun 1991 untuk menggantikan *hash function* sebelumnya, yaitu MD4 yang berhasil diserang oleh kriptanalis. Perlu ditegaskan bahwa Algoritma MD5 dengan ukuran input berapapun akan menghasilkan pesan ringkas yang panjangnya sama/ tetap yang dinyatakan dalam kode heksadesimal yang panjangnya 128 bit, perlu diingat bahwa satu karakter heksadesimal = 4 bit, berarti panjang outputnya 32 karakter heksa.

Terkadang kita menginginkan isi arsip tetap terjaga keasliannya, bila terjadi perubahan kecil pada arsip tersebut maka akan mengalami kesulitan dalam mendeteksinya jikalau ia berukuran besar.

Fungsi *hash* dapat digunkan untuk menjaga keutuhan data, caranya bangkitkan *message digest* dari isi arsip dengan menggunakan algoritma *MD5* dan datanya bisa disimpan dalam basis data, kemudian verifikasi isi arsip dapat dilakukan secara berkala dengan membandingkan *message digest*.

Jika terjadi perbedaan antara isi arsip sekarang dengan *message digest* dari arsi asli maka disimpulkan ada modifikasi terhadap isi arsip. Aplikasi ini didasarkan pada kenyataan bahwa perubahan 1 bit pada pesan akan mengubah secara rata- rata setengah dari bit-bit message digest, dengan kata lain fungsi *hash* sangat peka terhadap perubahan sekecil apa pun pada data masukan.

Contoh : file txt yang berisi teks berikut

Aplikasi dari fungsi hash antara lain untuk memverifikasi kesamaan Salinan suatu arsip dengan arsip aslinya yang tersimpan di dalam sebuah basisdata terpusat, kemudian apa pengertian dari Fungsi *Hash* Satu Arah(one-way *Hash*) yaitu fungsi *hash* yang bekerja dalam stu arah, dan pesan yang sudah diubah menjadi message digest tidak dapat dikembalikan lagi menjadi pesan semula, bila dua pesan yang berbeda akan selalu menghasilkan nilai *Hash* yang berbeda pula.

Memiliki hash MD5 : 4B97E98235F061A3923C4B005E9704A9

Jika huruf “A” pada awal kalimat aplikasi diganti dengan huruf “a” sehingga menjadi “aplikasi” ternyata nilai hash MD5-nya berubah sangat signifikan yaitu : 44333411A4F8A0FDB901F1596D743668

2.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:
Komputer.

1. Software MD5 Check Utility V2.31. Software ini ukurannya cukup kecil yaitu 99,3 Kb, dan dapat di download pada link berikut http://www.thefreecountry.com/utilities/free-md5- sum-tools.shtml
2. Beberapa file yang sudah ada pada computer
3. Tidak tertutup kemungkinan menggunakan software lain yang mengimplementasikan metode kriptosistem MD5, yang cukup banyak tersedia diinternet.

2.5 PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-02	Jelaskan Perbedaan Kriptografi Klasik dan Modern	30
2.	CPL-07	CPMK-02	Sebutkan dan jelaskan jenis jenis algoritma yang termasuk dalam kriptografi Modern	30
3.	CPL-07	CPMK-02	Jelaskan perbandingan (Kelebihan dan Kekurangan) antara algoritma enkripsi MD5 dan SHA1	40

2.6 LANGKAH PRAKTIKUM

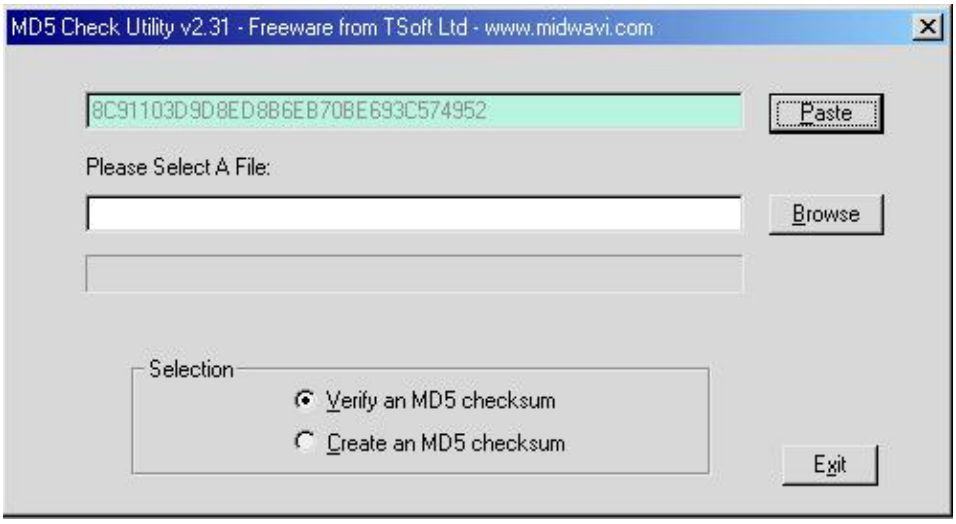
Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-02	Selesaikan langkah praktikum	Hasil praktikum langkah	100

Langkah-Langkah Praktikum:

B. PENGGUNAAN TOOL

1. Pastikan anda telah mengcopy file MD5.rar dengan nilai hash MD5 : 8C91103D9D8ED8B6EB70BE693C574952 , dalam file tersebut terdapat 2 file MD5.exe dan MD5 Readme.txt
2. Esktrak file tersebut dan jalankan file MD5 (untuk menjalankan aplikasi ini tidak perlu diinstal), sehingga akan menampilkan use interface seperti berikut :



Gambar 2.1 *UI MD5 Check Utility*

Catatan: nilai pada *textbox* yang atas (sebelah paste) sesuai isi *clipboard*, kalau *clipboard* kosong *textbox* tersebut juga kosong.

C. AUTENTIKASI FILE

1. Bukalah sembarangan file yang ada di computer anda namun dengan syarat file yang digunakan mudah untuk dilakukan pengeditan, missal MS Word, atau teks. (Hal ini digunakan untuk mempermudah penjelasan dan keterkaitan pemberian contoh selanjutnya). Perlu diingat nama file dan lokasi penyimpanan serta ukuran dari file tersebut.
2. Hitunglah nilai hash-nya dengan aplikasi di atas, dengan cara :
   - Pilih create an MD5 Checksum
   - Pilih file yang sudah dibuat
   - Lalu pilih OK
   - Akan muncul nilai hash, silahkan di copy-paste pada notepad
3. Buatlah sedikit perubahan pada file tersebut walaupun hanya 1 bit atau 1 byte, misalnya huruf “a” diganti huruf “B”, lali simpan file tersebut.
4. Verifikasilah nilai hash tersebut dengan nilai asli (cek langkah 2) dengan cara :
   - Copy nilai hash yang ada pada notepad (hasil Langkah 2)
   - Pilih verify an MD5 Checksum pada aplikasi MD5
   - Pilih paste
   - Pilih Browse dan pilih hasil file yang sudah di edit (Langkah no 3)
5. Untuk membuktikan dan memastikan, lakukan autentikasi (langkah 1-4) untuk format file lain dengan ukuran yang lebih besar.

D. DIGITAL SIGNATURE

1. Autentikasi juga dapat dilakukan pada bagian/komponen dari dokumen, salah satunya autentikasi tandatangan digital.

E. APLIKASI LAIN

Aplikasi yang disediakan yaitu software MD5 Check Utility V2.31 hanya merupakan salah satu software yang mengimplementasikan metode MD5. Banyak apliaksi sejenis yang beredar secara freeware.

2.7 POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-02	Tuliskan Langkah - langkah dalam mengenkripsi disertai dengan Screen Capture dan jelaskan tujuan pada setiap langkah langkahnya!	50
2.	CPL-07	CPMK-02	Analisis dan simpulkan apakah semua jenis file dapat di enkripsi dengan algoritma MD5?, Jelaskan jawaban anda!	50

2.8 HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-02	20%		
2.	Praktik	CPL-07	CPMK-02	30%		
3.	Post-Test	CPL-07	CPMK-02	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 3: INFORMATION HIDING

Pertemuan ke : 3

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 35 %
- Praktik : 40 %
- Post-Test : 25 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-03	Memahami prinsip otentikasi pengguna sistem elektronik dan prinsip kontrol akses untuk meningkatkan keamanan.

3.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

1. Memahami konsep, prinsip information hiding, teknik steganografi dan watermarking untuk proteksi hak cipta.

3.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-03	Mahasiswa mampu menerapkan penyembunyian pesan dengan information hiding, teknik LSB dalam steganografi dan watermarking.

3.3 TEORI PENDUKUNG

Steganography berbeda dengan cryptography, letak perbedaan adalah komponen input dan hasil keluarannya. Proses steganography membutuhkan minimal 2 komponen input/objek yaitu file host (stego medium) yang akan dijadikan sebagai induk penyembunyian dan informasi digital yang akan di sembunyikan. Hasil dari cryptography biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya data seolah-olah berantakan (namun dapat dikembalikan ke data semula), sedangkan hasil keluaran dari steganography secara visual (indrawi) memiliki bentuk yang sama dengan data aslinya, tentu saja persepsi ini oleh indra manusia, tetapi tidak oleh computer atau pengolah data digital lainnya. Selain itu pada steganography keberadaan informasi disembunyikan/tidak diketahui dan terjadi penyampulan tulisan (covered writing). Sedangkan pada cryptography informasi dikodekan dengan enkripsi atau metode pengkodean dan informasi diketahui keberadaannya tetapi tidak dimengerti maksudnya. Istilah dalam information hiding dapat dijelaskan sebagai berikut:

File host : file objek yang akan disisipi data digital lain
File informasi : file yang akan disisipkan dalam data digital lain

File stego medium : file induk yang sudah disisipi file informasi

3.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Command prompt
3. Notepad

3.5 PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Jelaskan Apa itu Information Hidding dan Steganografi!	30
2.	CPL-07	CPMK-03	Jelaskan Perbedaan Steganografi dan Kriptography!	30
3.	CPL-07	CPMK-03	Jabarkan Konsep dari Stegabografi disertai ilustrasi gambar!	40

3.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum	Hasil praktikum langkah	100

Langkah-Langkah Praktikum:

a. Penggunaan tool
   1. Pastikan anda sudah mengcopy file software S-Tool4. Jalankan program tersebut (tanpa harus diinstall)

b. Penyembunyian data
   1. tentukan file host/induk (yang akan disisipi) kemudian drag and drop pada window tersebut
   2. tentukan file informasi yg akan disembunyikan, drag and drop pd file host yg telah ada pada window Stool masukan password sesuai dgn selera

c. Sehingga terbentuk stego medium yang telah disisipi dengan file informasi dengan nama window hiden data,simpanlah file tersebut. Lakukan analisa atas file stego medium dan host yg belum ditempeli.
   1. Lakukan revealing dgn click kanan. Betulkah data yg termuat (hasil revealing)
   2. Lakukan modifikasi terhadap file stego medium

d. Lakukan Langkah b-c tersebut dengan menggunakan minimal 2 jenis data host yang berbeda, missal :
   1. Gambar
   2. Audio
   3. Dokumen

3.7 POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Lakukan kembali proses Menyisipkan informasi berupa: a. Nama Lengkap b. NIM c. Kelas d. Hoby e. Ceritakan Sedikit tentang apa yang akan anda lakukan setelah lulus dari TIF UAD semua informasi diatas disimpan dalam file gambar foto terbaik diri anda, laporan berupa langkah dan hasil dari proses penyisipan informasi	100

3.8 HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-03	20%		
2.	Praktik	CPL-07	CPMK-03	30%		
3.	Post-Test	CPL-07	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 4: AUTHENTICATION

Pertemuan ke : 4

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 35 %
- Praktik : 40 %
- Post-Test : 25 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-03	Memahami prinsip otentikasi pengguna sistem elektronik dan prinsip kontrol akses untuk meningkatkan keamanan.

4.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

1. Memahami dan mengimplementasikan prinsip autentikasi.

4.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-03	Mahasisiwa mampu menganalisa dan menerapkan prinsip autentikasi pengguna elektronik berbasis password, token,biometric dan Remote User Authentication.

4.3 TEORI PENDUKUNG

Auntetikasi adalah suatu Langkah untuk menentukan atau mengidentifikasi bahwa seseorang (atau sesuatu) adalah autentik atau asli. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Sedangkan melakukan autentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya. Pada suatu sistem komputer, autentikasi biasanya terjadi pada saat login atau permintaan akses.

Selain itu authentification juga merupakan salah satu dari banyak metode yang digunakan untuk menyediakan bukti bahwa dokumen tertentu yang diterima secara elektronik benar-benar datang dari orang yang bersangkutan dan tak berubah caranya adalah dengan mengirimkan suatu kode tertentu melaui e-mail dan kemudian pemilik e-mail mereplay email tersebut atau mengetikan kode yang telah dikirimkan.

4.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Sublime / Notepad++ / Atom
2. XAMPP

4.5 PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Jelaskan apa itu authentikasi!	30
2.	CPL-07	CPMK-03	Bagaimana cara kerja atau konsep dari authentikasi!	40
3.	CPL-07	CPMK-03	Analisislah kapan authentikasi diperlukan pada sebuah sistem!	30

4.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum	Hasil praktikum langkah	100

Langkah-Langkah Praktikum:

1. Membuat suatu folder autentifikasi pada local web server masing-masing.
2. Membuat file index.php dengan kode php sebagai berikut:

```
 <form name="FormLogin" method="post" action="auth.php">
  <tr bgcolor="#dfe9ff" >
   <td width="73" height="18"><font size="2" face="Verdana, Arial, Helvetica,  sans-
serif"> User
    </font></td>
   <td width="948"><font size="2" face="Verdana, Arial, Helvetica, sans-serif">
    :
    <input name="TxtUserID" type="text"  size="10" maxlength="30">
    </font></td>
  </tr>
  <tr bgcolor="#dfe9ff" >
   <td height="18" ><font size="2" face="Verdana, Arial, Helvetica, sans-
serif"> Password</font></td>
   <td><font size="2" face="Verdana, Arial, Helvetica, sans-serif"> :
    <input name="TxtPassID" type="password" size="10" maxlength="30">
    </font></td>
  </tr>
  <tr>
   <td ><font size="2" face="Verdana, Arial, Helvetica, sans-serif"> </font></td>
```

```
    <td > <font size="2" face="Verdana, Arial, Helvetica, sans-serif">
      <input type="submit" name="TbLogin" value="Login">
      </font></td>
  </tr>
  <tr>
    <td><font size="2" face="Verdana, Arial, Helvetica, sans-serif"> </font></td>
    <td><font size="2" face="Verdana, Arial, Helvetica, sans-serif"> </font></td>
  </tr>
</form>
```

3. Membuat file auth.php dengan kode sebagai berikut:

```
<?
session_start();
if ($_POST['TbLogin']) {
        $TxtUserID   = $_POST['TxtUserID'];
        $TxtPassID   = $_POST['TxtPassID'];
        if (trim($TxtUserID)=="") {
                $pesan[] = "Data User Name kosong";
        }
        if (trim($TxtPassID)=="") {
                $pesan[] = "Data Password kosong";
        }

        if (($TxtUserID=="admin") && ($TxtPassID=="admin")) {
                $SES_USERPLG = $TxtUserID;
                session_register("SES_USERPLG");

                $SES_UIDPLG = $TxtPassID;
                session_register("SES_UIDPLG");

                echo "<B>Berhasil Login.<br> Menu Admin ada disini</b>";
                exit;
        }
        else {
                $pesan[] = "User dan Passord lama belum benar";
        }

        if (! count($pesan)==0 ) {
                $TxtUserID = $_POST['TxtUserID'];

                echo "<br><br>";
                echo "<div align='left'>";
                echo "  <b> Kesalahan Input : </b><br>";
                foreach ($pesan as $indeks=>$pesan_tampil) {
```

```
                                $urut_pesan++;
                                echo "<font color='#FF0000'>";
                                echo "   ";
                                echo "$urut_pesan . $pesan_tampil <br>";
                                echo "</font>";
                        }
                        echo "</div><br>";
                }
        }
        ?>
```

4. Lakukan pengujian pada halaman web diatas melalui web browser dengan login yang benar, user: admin, password: admin, lalu lakukan Kembali dengan mengisi user yang kosong dan salah.

4.7 POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Buatlah suatu sistem authentikasi (web) dengan menggunakan php dan phpmyadmin semenarik mungkin	50
2.	CPL-07	CPMK-03	Pada sistem tambahkan alert jika user salah mengisi username atau password	25
3.	CPL-07	CPMK-03	Tambahkan fitur logout	25

4.8 HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-03	20%		
2.	Praktik	CPL-07	CPMK-03	30%		
3.	Post-Test	CPL-07	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 5: PASSWORD MANAGEMENT

Pertemuan ke : 5

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 35 %
- Praktik : 40 %
- Post-Test : 25 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah
CPMK-03	Mahasiswa mampu memahami pengertian dan pentingnya keamanan data dan sistem komputer

5.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:
1. Memahami dan mengimplementasikan prinsip autentikasi.

5.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-03	Mahasisiwa mampu menganalisa dan menerapkan prinsip autentikasi pengguna elektronik berbasis password, token,biometric dan Remote User Authentication.

5.3 TEORI PENDUKUNG

Untuk dapat mengakses system operasi Linux digunakan mekanisme password. Pada distribusi-distribusi Linux yang lama, password tersebut disimpan dalam suatu file text yang terletak di /etc/passwd. File ini harus dapat dibaca oleh setiap orang (world readable) agar dapat digunakan oleh program-program lain yang menggunakan mekanisme password tersebut.

Contoh isi file /etc/passwd:

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
rms:x:100:100:Richard M Stallman:/home/rms:/bin/bash
```

```
dmr:x:101:101:Dennis M Ritchie:/home/dmr:/bin/bash
linus:x:102:102:Linus Torvalds:/home/linus:/bin/bash
```

Keterangan :
Field pertama : nama login
Field kedua : password yang terenkripsi
Field ketiga : User ID
Field keempat : Group ID
Field kelima : Nama sebenarnya Field
Field keenam : Home directory user Field
Field ketujuh : User shell

Password login yang terdapat pada file /etc/passwd dienkripsi dengan menggunakan algoritma DES yang telah dimodifikasi. Meskipun demikian hal tersebut tidak mengurangi kemungkinan password tersebut dibongkar (crack). Karena penyerang (*attacker*) dapat melakukan *dictionary-based attack* dengan cara:

Menyalin file /etc/passwd tersebut.

Menjalankan program-program yang berguna untuk membongkar password, contohnya adalah John the Ripper (www.openwall.com/john/) .

Untuk mengatasi permasalahan ini pada distribusi-distribusi Linux yang baru digunakan program *Utility shadow* password yang menjadikan file /etc/passwd tidak lagi berisikan informasi password yang telah dienkripsi, informasi tersebut kini disimpan pada file /etc/shadow yang hanya dapat dibaca oleh root.

Berikut ini adalah contoh file /etc/passwd yang telah di-shadow :

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
rms:x:100:100:Richard M
Stallman:/home/rms:/bin/bash
dmr:x:101:101:Dennis M
Ritchie:/home/dmr:/bin/bash
linus:x:102:102:Linus
Torvalds:/home/linus:/bin/bash
```

Dengan demikian, penggunaan shadow password akan mempersulit *attacker* untuk melakukan *dictionary-based attack* terhadap file password.

Selain menggunakan shadow password beberapa distribusi Linux juga menyertakan program *hashing* MD5 yang menjadikan password yang dimasukkan pemakai dapat berukuran panjang dan relatif mudah diingat karena berupa suatu passphrase.

Mekanisme yang telah disediakan sistem operasi tersebut di atas tidaklah bermanfaat bila pemakai tidak menggunakan password yang "baik". Berikut ini adalah beberapa kriteria yang dapat digunakan untuk membuat password yang "baik" :

2. Jangan menggunakan nama login anda dengan segala variasinya.
3. Jangan menggunakan nama pertama atau akhir anda dengan segala variasinya.
4. Jangan menggunakan nama pasangan atau anak anda.
5. Jangan menggunakan informasi lain yang mudah didapat tentang anda, seperti nomor telpon, tanggal lahir.

6. Jangan menggunakan password yang terdiri dairi seluruhnya angka ataupun huruf yang sama.
7. Jangan menggunakan kata-kata yang ada di dalam kamus. Atau daftar kata lainnya.
8. Jangan menggunakan password yang berukuran kurang dari 6 karakter.
9. Gunakan password yang merupakan campuran antara huruf kapital dan huruf kecil.
10. Gunakan password dengan karakter-karakter non alfabet.
11. Gunakan password yang mudah diingat, sehingga tidak perlu ditulis,
12. Gunakan password yang mudah diketikkan, tanpa perlu melihat pada keyboard.

Beberapa tool yang bisa dipakai untuk melihat kuat tidaknya password adalah Jhon the Ripper. Kita bisa memakai utility ini untuk melihat kuat tidaknya suatu password yang ada pada komputer.

5.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Sistem operasi Linux
3. Notepad

5.5 PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Apa itu password management?	30
2.	CPL-07	CPMK-03	Sebutkan kriteria apa saja yang dapat digunakan untuk membuat password yg baik?	30
3.	CPL-07	CPMK-03	Menurut kalian bagaimana cara memanagement password kita agar tidak lupa dan tidak mudah diketahui orang lain?	40

5.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum	Hasil praktikum langkah	100

Langkah-Langkah Praktikum:

1. Login sebagai root dan buatlah beberapa 5 user baru, selanjutnya beri password setiap komputer. Berikan 3 user baru *bad password* yang hanya terdiri dari 4 karakter. Selanjutnya sisanya buat strong password buat minimal 8 karakter didalamnya kombinasi angka huruf dan karakter spesial seperti $#@%^&.
2. Lakukan installasi John the Ripper, ambil source yang sudah disiapkan oleh dosen/asisten praktikum.
3. Jalankan John the Ripper :

```
# cd /var/lib/john #
```

```
umask 077
# unshadow /etc/passwd /etc/shadow > mypasswords
# john mypasswords
```

Untuk melihat password jalankan command berikut

: # john -show mypasswords

Anda dapat menginstruksikan john the ripper unutk melihat password user atau gorup tertentu dengan option sebagai berikut : -users:u1,u2,... or -groups:g1,g2,...,

```
# john -users:nama_user1,nama_user2,nama_user3 mypasswords
```

4. Untuk memastikan password kita baik atau tidak, buatlah program dibawah ini, untuk melakukan testing bagaimanan password yang baik dan yang jelek.

```
#include <stdlib.h> #include <unistd.h>
#include <stdio.h> #include <crack.h>

#define DICTIONARY "/usr/lib/cracklib_dict" int main(int argc, char
*argv[]) {

      char *password; char *problem; int
      status = 0;

      printf("\nEnter an empty password or Ctrl-D to quit.\n");

      while ((password = getpass("\nPassword: ")) != NULL && *password ) { if ((problem =
            FascistCheck(password, DICTIONARY)) != NULL) {

                  printf("Bad password: %s.\n", problem); status = 1;

            } else {

                  printf("Good password!\n");

            }

      }

      exit(status);

}
```

5. Kompilasi program yang sudah anda buat dan jalankan, berikut contoh kompilasi dan cara menjalankan.

```
$ gcc cracktest.c -lcrack -o cracktest

$ ./cracktest

Enter an empty password or Ctrl-D to quit. Password: xyz

Bad password: it's WAY too
short. Password: elephant

Bad password: it is based on a dictionary word.
Password: kLu%ziF7

Good password!
```

6. Dalam suatu system kita juga bisa mencari user yang tidak diberi password, jalankan perintah berikut :
   # awk -F: '$2 == "" { print $1, "has no password!" }' /etc/shadow

5.7 POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Jelaskan Langkah instalasi sampai bisa membuat menggunakan aplikasi 1password	50
2.	CPL-07	CPMK-03	Berikan contoh password yang baik sesuai dengan kriteria yang ada	50

5.8 HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-03	20%		
2.	Praktik	CPL-07	CPMK-03	30%		
3.	Post-Test	CPL-07	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**

PRAKTIKUM 6: DIGITAL SIGNATURE

Pertemuan ke : 6

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Bobot Penilaian : 100%
- Pre-Test : 35 %
- Praktik : 40 %
- Post-Test : 25 %

Pemenuhan CPL dan CPMK:

CPL-07	Mampu memilih, membuat dan menerapakan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-03	Memahami prinsip otentikasi pengguna sistem elektronik dan prinsip kontrol akses untuk meningkatkan keamanan.

6.1 DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:
1. Memahami dan mengimplementasikan prinsip autentikasi.

6.2 INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-03	Mahasisiwa mampu menganalisa dan menerapkan prinsip autentikasi pengguna elektronik berbasis Digital signature.

6.3 TEORI PENDUKUNG

Tanda tangan digital digital merupakan salah satu cara untuk memberikan authentication, integrity, dan non-repudiation pada dokumen digital yang akan dikirimkan/didistribusikan. Prinsip yang digunakan dalam tanda tangan digital adalah data yang dikirimkan harus ditanda tangani oleh pengirim dan tanda tangan bisa diperiksa oleh penerima untuk memastikan keaslian data yang dikirimkan. Proses ini menganalogikan proses penandatanganan dokumen kertas oleh yang berwenang sebelum dikirimkan. Dengan cara ini pengirim bertanggung jawab terhadap isi dokumen dan dapat dicek keaslian dokumen oleh penerima. Menurut Arrianto Mukti Wibowo [1] sifat dimiliki oleh tanda tangan digital adalah:

1. Otentik, tak bisa/sulit ditulis/ditiru oleh orang lain. Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti, sehingga penandatangan tak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya.

2. Hanya sah untuk dokumen (pesan) itu saja ayau kopinya yang sama persis. Tanda tangan itu tidak bisa dipindahkan ke dokumen lainnya, meskipun dokumen lain itu hanya berbeda sedikit. Ini juga berate bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak lagi sah.
3. Dapat diperiksa dengan mudah, termasuk oleh pihak-pihak yang belum pernah bertatap muka langsung dengan penandatangan.

Menurut Arrianto Mukti Wibowo, dkk [3] , penggunaan digital signature berawal dari penggunaan teknik kriptografi yang digunakan untuk mengamankan informasi yang hendak ditransmisikan/disampaikan kepada orang yang lain yang sudah digunakan sejak ratusan tahun yang lalu. Dalam suatu kriptografi suatu pesan dienkripsi (encrypt) dengan menggunakan suatu kunci (key). Hasil dari enkripsi ini adalah berupa chipertext tersebut kemudian dikirimkan kepada tujuan yang dikehendakinya. Chipertext tersebut kemudian didekripsi (decrypt) dengan suatu kunci untuk mendapatkan informasi yang telah enkripsi tersebut. Terdapat dua macam cara dalam melakukan enkripsi yaitu dengan menggunakan kriptografi simetris (symetric crypthography/secret key crypthography) dan kriptografi simetris (asymetric crypthography) yang kemudian lebih dikenal sebagai public key crypthography. Teknologi tanda tangan digital memanfaatkan teknologi kunci publik. Sepasang kunci publik-privat dibuat untuk keperluan seseorang. Kunci privat disimpan oleh pemiliknya, dan dipergunakan untuk membuat tanda tangan digital. Sedangkan kunci publik dapat diserahkan kepada siapa saja yang ingin memeriksa tanda tangan digital yang bersangkutan pada suatu dokumen. Proses pembuatan dan pemeriksaan tanda tangan ini melibatkan sejumlah teknik kriptografi yaitu fungsi hash dan sistem kripto kunci public.

6.4 HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Microsoft Word
3. Paint

6.5 PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Jelaskan dengan bahasamu apa itu Digital Signature	30
2.	CPL-07	CPMK-03	Bagaimana Cara mekanisme kerja dari Digital Signatre sertai dengan illustrasi	40
3.	CPL-07	CPMK-03	Berdasarkan sertifikasi kelas Digital Signature, Sebutkan dan jelaskan kelas kelas tersebut	30

6.6 LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-03	Selesaikan langkah praktikum	Hasil praktikum langkah	100

Langkah-Langkah Praktikum:

Digital signature dengan Microsoft Word

a. Jalankan Ms Word terlebih dahulu.
b. Dalam text editor tersebut buatlah suatu naskah yang nantinya merupakan dokumen pribadi anda.
c. Membuat tanda tangan digital:
    1. Pada tampilan menu utama pilih Signature → create key , maka akan muncul jendela baru untuk membuat kunci enkripsi dan kunci dekripsi. Yang perlu diisi cukup nama dan email saja, kemudian Generate key dan kemudian save key.
    2. Setelah disimpan, maka tanda tangan tersebut dapat digunakan kapan saja pada aplikasi Ms Word. File dengan ekstensi .dse merupakan file yang digunakan untuk menyimpan kunci public yang akan digunakan untuk memberikan tanda tangan digital pada dokumen.
    3. File/ kunci tersebut dapat diketahui oleh siapa saja. File dengan ekstensi .dsd merupakan file yang digunakan untuk menyimpan kunci private yang akan digunakan untuk memvalidasi dokumen. File ini hanya boleh diketahui/dimiliki oleh pemilik tanda tangan.
d. Memberikan tanda tangan digital pada dokumen/menandatangani dokumen secara digital. Setelah kita memiliki tanda tangan digital yg terseimpan dalam file dengan eksteni .dse dan .dsd maka kita tinggal membubuhkan tanda tangan tersebut pada dokumen, dengan memilih menu Signature Validate signature. Teks box tidak perlu diisi, cukup buka file kunci private (.dsd) dengan button browse key.
e. Simpan dokumen tersebut, sehingga document tersebut berarti sudah merupakan dokumen yang memuat tanda tangan digital kita. Digital signature pas Ms Word dalam Microsoft Office (word, excel, power point, ouytlook) juga tersedia digital signature, namun penyimpanan kunci/tamda tangannya secara online dan berbayar. Anda bisa memilih prepare pada office button (sudut kiri atas), maka ada beberapa menu pengamanan dokumen dan salah satunya digital signature.

6.7 POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-03	Buatlah Sebuah Surat perjanjian dengan topik bebas (Semenarik mungkin) kemudian sertakan minimal 4 pihak yang terlibat dengan masing masing pihak memiliki tanda tangan digital	50
2.	CPL-07	CPMK-03	Analisislah apakah tanda tangan digital sangat diperlukan pada zaman sekarang ini?, !, keluarkan semua opini kalian (opini yang logis akan mendapatkan nilai yang logis juga)	50

6.8 HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-03	20%		
2.	Praktik	CPL-07	CPMK-03	30%		
3.	Post-Test	CPL-07	CPMK-03	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**