PERTEMUAN 6
KEAMANAN INFORMASI

A. TUJUAN PEMBELAJARAN

1. Ketepatan mahasiswa dalam memahami dan menjelaskan mahasiswa mampu menjelaskan keamanan informasi dan teknik kriptografi.
2. Mahasiswa memahami bahwa pentingnya sebuah keamanan data.

B. URAIAN MATERI

1. Pembahasan Keamanan Dan Informasi

a. Keamanan Informasi

Pada era serba digital ini, pertukaran informasi semakin cepat dan mudah. Dengan kecepatan informasi semakin meningkat berbanding lurus juga dengan isu-isu keamanan informasi. Berkenaan dengan keamanan sebuah informasi sering kita mengira adalah keamanan jaringan (*network security*). Sebenarnya objek yang kita lindungi adalah sebuah data atau informasi. Betul sekali informasi dikirim melalui sistem jaringan, namun tetap objek utama yang ingin diamankan informasinya. Kita lihat beberapa kasus berhubungan kemanan infomasi:

1) Pada 2013, Masalah virus masih menjadi isu yang mendominasi. Pencurian identitas mulai ramai. Pada tahun itu *Cyber war* mulai menjadi bahan berbincangan.
2) Bursa Singapura terdapat ada masalah software. Perdagangan saham sempat terhenti pada tahun 2014.
3) Serangan Heartbleed Bug terjadi pada tahun 2014, yang dapat mencuri data-data penting seperti *username, password,* kartu kredit dan bahkan kartu penjamin sosial.
4) Pada tahun 2016, CCTV dipakai menjadi bagian dari *Distributed DoS attack.* Salah satu piranti yang dapat dikoneksikan ke *Internet of Things*, CCTV tersebut dapat dijadikan target serangan selanjutnya dijadikan zombie untuk menyerang atau merusak tempat lain.
5) Pada 2016 di Panama, salah satu Firma hukum (Mossack Fonseca) terjadi pembobolan data. Data yang dibobol data tabungan atau invetasi orang orang ternama dari berbagai negara (slah satunya Indonesia).

Panama Papers Breach dijadikan nama pada kasus ini. Kasus ini terjadi diduga *Slider plugin* pada sistusnya (woerdpress) sudah kadaluwarsa dan rentan.

6) Masih di tahun 2016, DNS servers terkena serangan DDoS. Serangan memanfaatkan bantuan botnet maka bandwidth jaringan akan habis mode (Gbps).
7) Amazon Web Service ptatfom cloud berhenti beberapa jam. Beberapa perusahaan penyedia layanan publik menggunakan AWS S3 ikut berhenti juga. Ternyata menjadi penyebab masalah tersebut adalah salah satu operator salah ketik (typo). Terjadi pada tahun 2017.
8) Salah satu Universitas di Amerika Serikat mengalami masalah pada internal jaringannya. Setelah ditelusuri terdapat paket ynag jumlahnya banya dari mesin minuman (segmen Iot). Piranti IoT diserang secara brute-force (coba-coba password). Kemudian berdampak pada DNS kampus kampus tersebut, 2017.
9) Tahun 2017, mahasiswa di salah satu universitas di Negeri ini, minta bantuan *cracker* untuk mengedit nilai pada *database* Sistem Informasi di kampus tersebut.
10) Tahun 2019, masih ingat beberapa nasabah bank Mandiri di kota Pekanbaru mendadak panik sebab saldo dalam rekeningnya menjadi 0 atau kosong.

REPUBLIKA.CO.ID, JAKARTA -- Puluhan nasabah Bank Mandiri di Kota Pekanbaru, Provinsi Riau, panik akibat saldo tabungan mereka tiba-tiba kosong dan tidak bisa melakukan transaksi nontunai.

"Saya cek di ATM dan *internet banking* Mandiri, saldo saya jadi nol rupiah," kata seorang nasabah bernama R Andika Permana di Pekanbaru, Sabtu (20/7).

Ia mengaku kaget ketika ingin mengambil uang tunai di ATM pada Sabtu pagi pukul 08.00 WIB. Pada mesin ATM tertulis bahwa saldo tabungannya tidak mencukupi, dengan angka tertera nol rupiah.

Ketika dicek dengan *internet banking,* ia juga mendapatkan jawaban yang sama. Panik, ia langsung menuju kantor Bank

Sumber: https://www.republika.co.id/berita/puxa73382/network

Gambar 8. 1 Berita kasus nasabah Bank Mandiri

Sudah disinggung diawal bab, kecepatan informasi semakin meningkat juga dengan kasus keamanan informasi. Isu tersebut karena meningkatnya penggunaan jaringan internet dan era rekaman. Disamping itu strategi untuk

menemukan celah keamanan informasi semakin canggih dan berkembang sehingga kelemahan dapat diketahui.

Sebuah survei yang dilaksanakan dengan Information USA mengkonfirmasi bahwa 22% manajer tidak melupakan perlindungan mesin catatan sebagai hal yang penting. Bagaimana membujuk mereka untuk memasukkan modal ke dalam perlindungan? Kurangnya kesadaran akan masalah proteksi (*loss of protection awareness*) merupakan hal penting adanya masalah proteksi. Pengguna masih banyak melakukan kebiasaan kurang baik, termasuk membagikan kata sandi admin.

Kasus keamanan informasi yang biasanya berada dalam bentuk catatan teknis harus diterjemahkan ke dalam angka ekonomi agar kontrol dapat menangkapnya. Misalnya, di Inggris telah ada survei tentang berapa banyak harga agen jika mesin mereka tidak lagi tersedia (turun).

b. Pembahasan Security Life Cycle

Kebanyakan dari kita menganggap permasalahan perlindungan data dapat diselesaikan melalui cara membeli produk perlindungan, termasuk *firewall*, anti-virus, dan sebagainya. Sesuatu yang bisa kita mantapkan dikenal sebagai “aset”. Untuk alasan ini, langkah pertama dalam melindungi aset adalah memutuskan barang-barang yang perlu Anda lindungi. Segala dirasa suatu aset perlu diputuskan dengan pemegang atau pemilik sistem (Program, data, aplikasi, dll.) sebab merekalah yang bisa membedakan mana aset penting atau tidak. Metode tersebut dikenal sebagai evaluasi dan mampu diselesaikan dengan jalan pelatihan atau pengakuan dari pihak terkait. Seringkali pemilik perangkat lunak mengetahui di mana barang-barang tersebut berada tetapi pihak operasional (profesional TI yang bertugas mengamankan sistem) tidak mengetahuinya.

Ketika sudah terpetakan mana aset yang masih berguna atau tidak, selanjutnya yang dilakukan adalah menghargai aset itu (dirupiahkan). Dengan memberi nilai aset tersebut, kita ketahui nilai asetnya, jangan sampai biaya perlindungannya lebih mahal dari pada asaet. Contohnya aset senilai Rp.10.000.000,00 sedangkan biaya perlindungan Rp 15.000.000,00.

Sesuatu yang berhubungan terhadap teknologi informasi, pendataan aset-aset ini cukup sulit dilakukan sebab terdapat aset tidak terlihat mata secara langsung. Piranti tersebut terbagi menjadi tiga yaitu; *software* (perangkat lunak), *hardware* (perangkat keras) dan *data*. Kemudian ketika

ketiga komponen tersebut sudah diketahui nilainya dan aset-aset apa saja yang akan diamankan langkah berikutnya adalah:

1) Membuat desain keamanan

   Langkah ini membuat kebijakan dan prosedur (*policies procedures*). Misalnya pembatasan otoritas akses pada sistem tersebut, hal ini di tuliskan dalam kebijakan.

2) Setelah desain dibuat selanjutnya diaplikasikan secara teknis dengan *security device*.

3) Setelah diterapkan, kasus atau masalah kemanan informasi atau data mungkin terjadi. Tahap inilah kita invetigasi penyebab ketika terjadi masalah keamanan, apakah ini benar-benar masalah keamanan atau hal biasa, ketika benar-benar sebuah kasus maka akan diproses lebih lanjut sesuai desain *procedure* sebelumnya.

Hal terebut yang membentuk siklus, *Security life cycle.* Kebanyakan kita beranggapan *security* atau keamanan itu sebuah produk (membeli suatu produk keamanan).

Sumber: https://www.kuasaiteknologi.com/

Gambar 8. 2 Security life cycle

c. Pembahasan Prinsip-prinsip Keamanan

Adapun prinsip-prinsip prinsip utama dalam keamanan informasi, antara lain:

1) Aspek Keamanan

   Berbicara mengenai perlindungan informasi kira-kira ada 3 hal yang perlu terlindungan adalah kerahasiaan, integritas, dan ketersediaan. Selain tiga hal tersebut masih banyak terdapat aspek

keamanan yang lainya.

a) Kerahasiaan (*Confidentiality*)

Kerahasiaan adalah komponen keamanan yang biasanya dipahami. Komponen kerahasiaan menyatakan bahwa catatan paling efektif dapat diakses atau dipertimbangkan dengan bantuan menggunakan badan hukum. Biasanya komponen ini adalah yang terbaik untuk ditangkap manusia. Ketika melibatkan catatan non-publik, komponen ini juga disebut Privasi.

Serangan pada komponen kerahasiaan dapat berupa penyadapan informasi (melalui jaringan), *keylogger* dipasang guna mencegat apa pun yang diketikan melalui *keyboard*, dan mencuri mesin atau disk yang digunakan dalam menyimpan informasi. Perlindungan terhadap komponen kerahasiaan dapat dilengkapi dengan bantuan penggunaan kriptografi, dan pembatasan akses.

b) Integrity

Masalah integritas menyatakan informasi atau data tidak bisa dirubah tanpa izin pemiliknya atau yang berhak. Misalnya, jika kita mendapatkan pesan transaksi berikut (beralih dari akun 0001 ke akun 0002 nilai transaksi), maka catatan transaksi tidak dapat diubah secara sembarangan.

TRANSFER 0001 KE 0002 250000000

Penyerangan terhadap faktor integritas dapat dilakukan melalui cara *man in the middle,* artinya informasi atau data ditangkap ditengah perjalanan kemudian mengubahnya dan melanjutkan ke tujuan. Data atau informasi yang tiba di tujuan (program web server) tidak mengetahui bahwa data ataui nformasi telah mengalami perubahan di tengah perjalanan.

Perlindungan untuk masalah integritas dapat diselesaikan melalui cara penggunaan kode otentikasi pesan.

c) Availability

Terlalu mengandalkan sistem teknologi informasi berakibatkan sistem (data atau informasi) harus dapat diambil ketika membutuhkan. Jika perangkat tidak selalu tersedia, dapat memicu masalah yang dapat menyebabkan kerugian ekonomi atau bahkan nyawa. Oleh karena itu, faktor ketersedian merupakan bagian dari

keamanan.

Kasus pada faktor ketersediaan dengan tujuan membuat layanan menjadi lamban sehingga tidak ada fungsinya. Kasus ini bias akita kenal *Denial of Service* (DOS).

Kemanan terhadap faktor ketersedian bisa dilakukan melalui cara menghadirkan redundansi. Misalnya, penggunaan jaringan komputer bisa menggunakan beberapa layanan. Jika salah satu layanan diserang (atau dirusak), maka ada lagi yang dapat digunakan.

2) Aspek keamanan lainya

Diluar 3 aspek fundamental yang telah disebutkan diatas, terdapat beberapa aspek tambahan lainya:

a) Non-repudiation

Aspek ini digunakan untuk membuat pelaku tidak bisa menyangkal apa yang telah mereka lakukan. Umumnya berkaitan erat pada sistem yang berkaitan dengan transaksi. Contoh penggunaannya pada sistem peleangan elektronik.

Non repudiation dapat diterapkan dengan penggunaan (*message authentication code)* kode otentikasi pesan (hash) dan logging.

b) Authentication

Authentication dipergunakan untuk memverifikasi pernyataan bahwa orang tersebut adalah betul yang diklaim. Misalnya suatu akun dengan nama Isti, bagaimana membuktikkan pengguna benar bernama Isti.

Verifikasi seseorang dalam dunia nyata lebih mudah dibanding di dunia maya. Semisal seseorang akan membuat pernyataan palsu bahwa dia seorang perempuan dan kenyataan memiliki ciri-ciri fisik laki-laki. Tetapi ketika *online* atau di dunia maya, dia dapat menyatakan bahwa dia perempuan dengan menggunakan nama akun perempuan dan foto profilnya seorang perempuan .

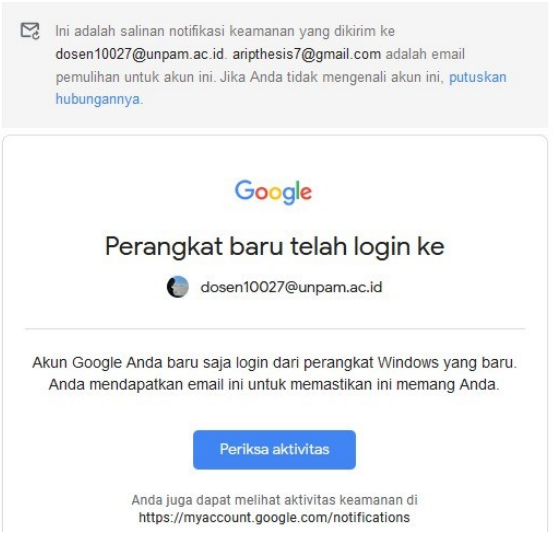
Dalam otentikasi ini dapat dilakukan dengan bantuan berbagai faktor. Adapun faktor-faktor yang bisa membantu dalam dunia maya diantaranya:

- Hal yang diketahui

  Seperti *name*, *username*,PIN atau *password*.
- Organ fisik dimiliki

  Seperti retina, sidik jari dan *biometric*.
- Hal yang dimiliki

  Seperti kunci, kartu dan token.
- (*Proximity*) keberadaan pengguna di lokasi tertentu.
- Dengan bantuan pihak ketiga.
-



Gambar 8. 3 Contoh *Authentication* gmail

c) Authorization

Pada aspek *Authentication* dapat kita ketahui siapa dan peran seseorang (pengguna) tersebut. *Authorization* merupakan memeberikan hak akses terhadap pengguna dan *roles* yang dimiliki. Aspek *authorization* perlu adanya aspek *authentication*, sehingga posisinya setelah *authentication.*

2. Pembahasan Kriptografi

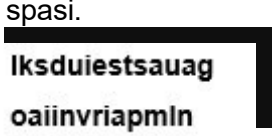
Dalam pengamanan data atau informasi terdapat dua cara, yaitu membaurkan data (kriptografi) dan menyembunyikan data (steganografi).

a. Kriptografi

Teknik kriptografi tidak menyembunyikan pesan/data/informasi namun pesan tersebut dirubah sehingga sukar mendapatkan pesan yang asli. Merubah pesan dengan transposisi (merubah posisi huruf) dan (mengganti

huruf dengan angka atau kata lain) substitusi. Informasi atau pesan masih dapat dilihat oleh penyerang atau *hacker* namun seperti *file* sampah.

Banyak cara untuk melakukan transposisi, contoh menulis pesan dijadikan 2 baris dengan bergantian. Misalnya kita menulis pesan rahasia "lokasi di Universitas Pamulang". Perhatikan transposisi kalimat tersebut abaikan spasi.



Huruf 'l' posisi di baris kesatu, huruf 'o' di baris dua, huruf 'k' Kembali ke baris satu, huruf 'a' Kembali ke baris kedua, dan sampai g secara bergantianke baris satu dan ke baris dua. Pesan yang dikirimkan menjadi **"lksduiestsauagoaiinvriapmln"** terlihat pesan susah dibaca bukan. Kemudian dari penerima pesan akan melakukan proses sebaliknya maka akan diketahui pesan aslinya.

Salah satu contoh kriptografi substitusi adalah **Caesar cipher**. Proses dasarnya perhatikan, huruf "A" sampai "Z" kita urutkan. Kemudian baris dibawahnya kita geser huruf sejumlah lima tempat. Lebih jelas hasilnya kita lihat huruf berikut.

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
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

Misalnya kita akan mengirimkan pesan "INFORMASI", caranya kita menggunakan huruf yang dibawahnya sebagai pengganti tiap-tiap hurufnya. Perhatikan huruf "I" digantikan "N', "N" menjadi "S", dan seterusnya, maka "INFORMASI" akan menjadi "NSKTWRFXN".

1) Struktur sistem kriptografi

Adapun terdapat komponen-komponen utama dari sistem kriptografi diantaranya.

a) *Ciphertext*

Merupakan data yang didapatkan melalui proses enkripsi. *Ciphertext* mempunyai bentuk *file* biner atau ASCII. Kita perkirakan penyerang memungkinkan bisa mengakses *ciphered text*.

b) *Plain text*

Merupakan data (berupa teks atau pesan) asli/original yang belum diproses. Data asli dapat berupa *file* biner bukan hanya

berupa teks (ASCII).

c) Algoritma dan kunci (*black box*)

Merupakan proses tranformasi dari *plain text* menjadi *ciphered text*. Penyerang dapat mengetahui algoritma namun tidak mengetahui kunci.

Keterkaitan tiga komponen diatas dapat dirumuskan seperti berikut. *Ciphertext c* adalah hasil proses enkripsi E dengan kunci k terhadap pesan m. *Ciphertext* ini yang akan dikirim pada penerima pesan.

$$c = E_k(m) \quad (1)$$

Proses penulisan enkripsi dapat kita lakukan seperti dibawah ini.

$$c = ENKRIP \ \ (k, m) \quad (2)$$

Pada penerima, pesan (*plain text*) didapat dari hasil dekripsi (D) dengan kunci k terhadap *ciphertext c*.

$$m = D_k(c) \quad (3)$$

Proses penulisan deskripsi dapat kita lakukan seperti berikut.

$$m = DEKRIP(k, c) \quad (4)$$

b. Jenis-jenis Kriptografi

1) Kriptografi kunci Publik (kriptografi asimetrik)

Pada kriptografi ini, terdapat dua kunci yang akan digunakan. Masing-masing pengguna mempunyai kunci sepasang (kunci publik dan privat) yang saling berkaitan. Apabila suatu pesan dikunci menggunakan kunci publik, maka hanya dapat dibuka dengan kunci privat pasangannya. Begitu juga sebaliknya apabila dikunci menggunkan kunci privat, hanya dapat dibuka dengan kunci privat pasanganya. Kunci publik dapat diketahui secara umum dan disimpat di publik. Sedangkan kunci privat hanya dapat diakses pemiliknya saya. Apabila kunci privat

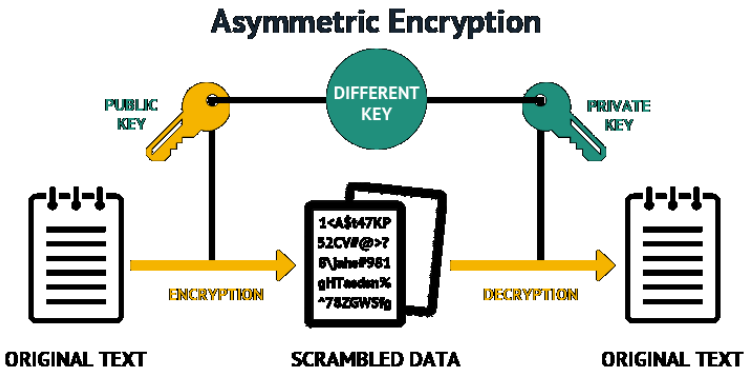
dicuri, maka identitas pemiliknya juga tercuri.

Contoh pada komunikasi antara Arip dengan Isti. Isti mempunyai kunci public KI_{pub} dan privat KI_{priv}. Arip juga mempunyai kunci privat KA_{priv} dan kunci public KA_{pub}. Apabila Isti akan mengirim pesan "m" kepada Arip, maka *ciphertext c* adalah hasil enkripsi publik Arip (Isti
mengenkripsi kunci public Arip).

$$c = EKA_{pub}(m) \quad (5)$$

Penerima Arip, akan menerima *ciphertext c*. Untuk mendapatkan pesan semula, dilakukan proses dekripsi dengan kunci privatnya Arip. Proses dekripsi ini hanya dapat dilakukan Arip. Isti yang bertindak sebagai pengirim sudah tidak bisa membuka kembali pesan yang telah dikirimkan.

$$m = EKA_{priv}(c) \quad (6)$$



Sumber: https://sslindonesia.com/perbedaan-public-key-dan-private-key-ssl-indonesia/

Gambar 8. 4 Ilustrasi kriptografi asimetrik

Contoh algoritma kriptografi kunci publik diantaranya RSA[8] dan *Elliptic Curve Cryptosystem* (ECC). Algoritma ini mempunyai komputasi yang lumayan tinggi jadi waktu yang dibutuhkan cukup lama ketika memproses data.

2) Kriptografi kunci Privat (simetrik)

Sistem kriptografi kunci privat, terdapat satu kunci yang dipegunakan ketika mengunci dan membuka (simetrik). Disebut

kriptografi kunci privat sebab kunci yang dipakai harus dirahasiakan.

Kendala operasi sistem kriptografi ini terletak pada distribusi kunci. Contoh, ketika Isti akan mengirim pesan ke Arip, maka Isti dan Arip memiliki kunci yang sama. Selanjutnya Isti mengirim pesan ke Endin, maka Isti dan Endin mempunyai kunci sendiri berbeda kuncinya Isti dan Arip. Begitu juga ketika Arip dan Endin berkomunikasi atau mengirim pesan maka Arip dan Endin memiliki kunci sendiri. Maka ketika komunikasi semakin diteruskan ke pihak-pihak lainya, jumlah kunci yang digunakan akan menjadi banyak seiring penambahan jumlah pengguna (n).

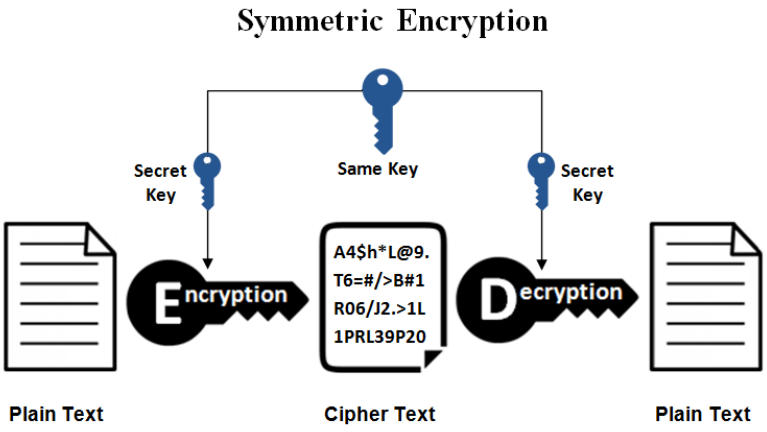
$$numkeys = \frac{(n)(n-1)}{2} \tag{7}$$

Tabel 8. 1 Jumlah kunci

Jumlah Pengguna	Jumlah Kunci
10	45
100	4950
1000	499500
10000	49995000
100000	4999950000

Kita perhatikan tabel diatas jika pengguna masih 10 orang, maka jumlah kunci belum begitu banyak. Tetapi ketika pengguna sudah mencapai ribuan, jumlah kunci sudah cukup banyak. Berapa jumlah pengguna internet di dunia saat ini? Pengguna internet di Indonesia saja sudah mencapai 212,35 juta dilansir **internetworldstats** maret 2021, berapa banyak kunci yang perlu dipersiapkan jika semuanya saling komunikasi?.

Walaupun terdapat masalah pada distribusi kunci, namun paling bagus kinerjanya.



Sumber: https://sslindonesia.com/perbedaan-public-key-dan-private-key-ssl-indonesia/

Gambar 8. 5 Ilustrasi kriptografi simetrik

3) Kriptografi *hybrid*

Telah dijelaskan diatas, bahwa kriptografi kunci privat mempunyai kelebihan pada algoritma ysng cukup cepat namun terdapat permasalahan pada distribusi kunci. Sedangkan kriptografi kunci publik permasalahan terdapat pada komputasinya cukup tinggi. Solusi dari permasalahan diatas adalah menggabungkan kriptografi privat dan publik menjadi kriptografi *hybrid*.

Pada kriptografi hybrid, proses enkripsi dan dekripsi yang digunakan kriptografi kunci privat kemudian untuk pembuatan *session key* dan kunci sesi ini yang ditukarkan menggunakan kriptografi kunci publik. Ukuran kunci yang kecil maka biaya dalam proses enkripsi menjadi lebih murah.

3. Pembahasan Steganografi *(steganography)*

Steganografi merupakan teknik atau cara untuk menyembunyikan data/pesan/informasi sehingga tidak diketahui dengan mudah yang tidak berhak. Cara penyembunyianya dengan memanfaatkan media lain. Contohnya, dalam menyembunyikan pesan dapat kita sembunyikan dalam audio, gambar atau video. Pada sejarah jaman perang Yunani dengan Persia dalam menyembunyikan pesan dilakukan menggunakan meja yang balut lilin.

Steganografi merupakan bagian dari *Digital Rights Management* (DRM). Terdapat beberapa cara menyisipkan pesan/informasi ke *file* digital. Contoh,

kita dapat menggunakan gambar digital untuk disisipkan pesan. Teknik yang dipakai adalah menggunakan (LSB) *least significant bit* pada data pixel gambar. Contohnya, suatu pixel di gambar digambarkan oleh 8-bit. Hal ini terdapat 256 kombinasi *grey scale*. Jadi kita dapat memanfaatkan bit yang ke-8 dan 7-bit yang digunakan dalam pewarnaan. Pada Bit ke-8 bisa dipakai sebagai
bagian dari data.

Sumber: https://budi.rahardjo.id

Gambar 8. 6 Contoh steganografi watermark

C. SOAL LATIHAN/ TUGAS

1. Berikan contoh kasus kemanan informasi yang anda ketahui selain pada modul, jelaskan!
2. Jelaskan apa yang anda pahami tentang kemanan data atau informasi?
3. Sebut dan jelaskan struktur sistem kriptografi?
4. Buatlah contoh pesan yang trasposisi menggunakan teknik kriptografi!
5. Menurut anda perbedaan apakah yang mendasar antara kriptografi kunci public dan privat, jelaskan!

D. DAFTAR PUSTAKA

Abdul dkk, 2020. *Pengantar Teknologi Informasi*. Labuhanbatu: Labuhanbatu Berbagi Gemilang.

Rahardjo, B. 2017. Keamanan Informasi. Bandung: PT Insan Infonesia, Steven Levy. 2001. Crypto: How the Code Rebels Beat the Government Saving *Privacy in the Digital Age*. Penguin Books.