Sistem Keamanan Komputer

Dr. Andreas Hadiyono

Pengertian
Keamanan

Keamanan adalah suatu yang sangat penting untuk menjaga agar suatu data dalam jariangan tidak mudah hilang. Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil ditembus.

Peningkatan Keamanan Data

Cara meningkatkan keamanan data

Rahasia (Privacy)

Keaslian (Authenticity)

Convert Channel

Definisi Keamanan

AVAILABILITY

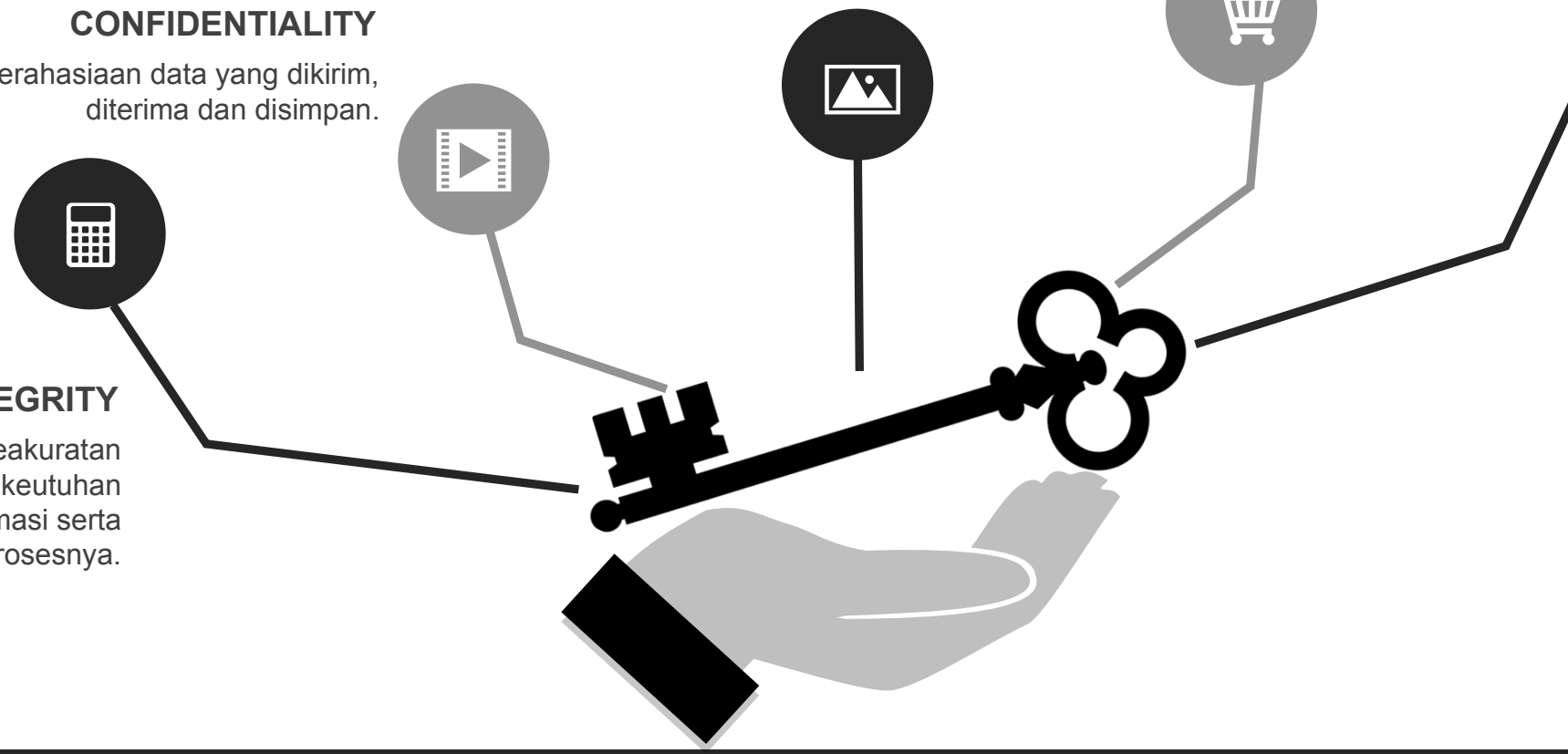
Menjamin data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

AUTHENTICATION

Menentukan atau mengonfirmasi bahwa seseorang (atau sesuatu) adalah autentik atau asli.

CONFIDENTIALITY

Menjamin kerahasiaan data yang dikirim, diterima dan disimpan.



NONREPUDIATION

Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

INTEGRITY

Menjaga keakuratan dan keutuhan informasi serta metode prosesnya.

Metode Authentication

SOMETHING YOU KNOW
Meliputi kerahasiaan informasi, contohnya adalah password dan PIN

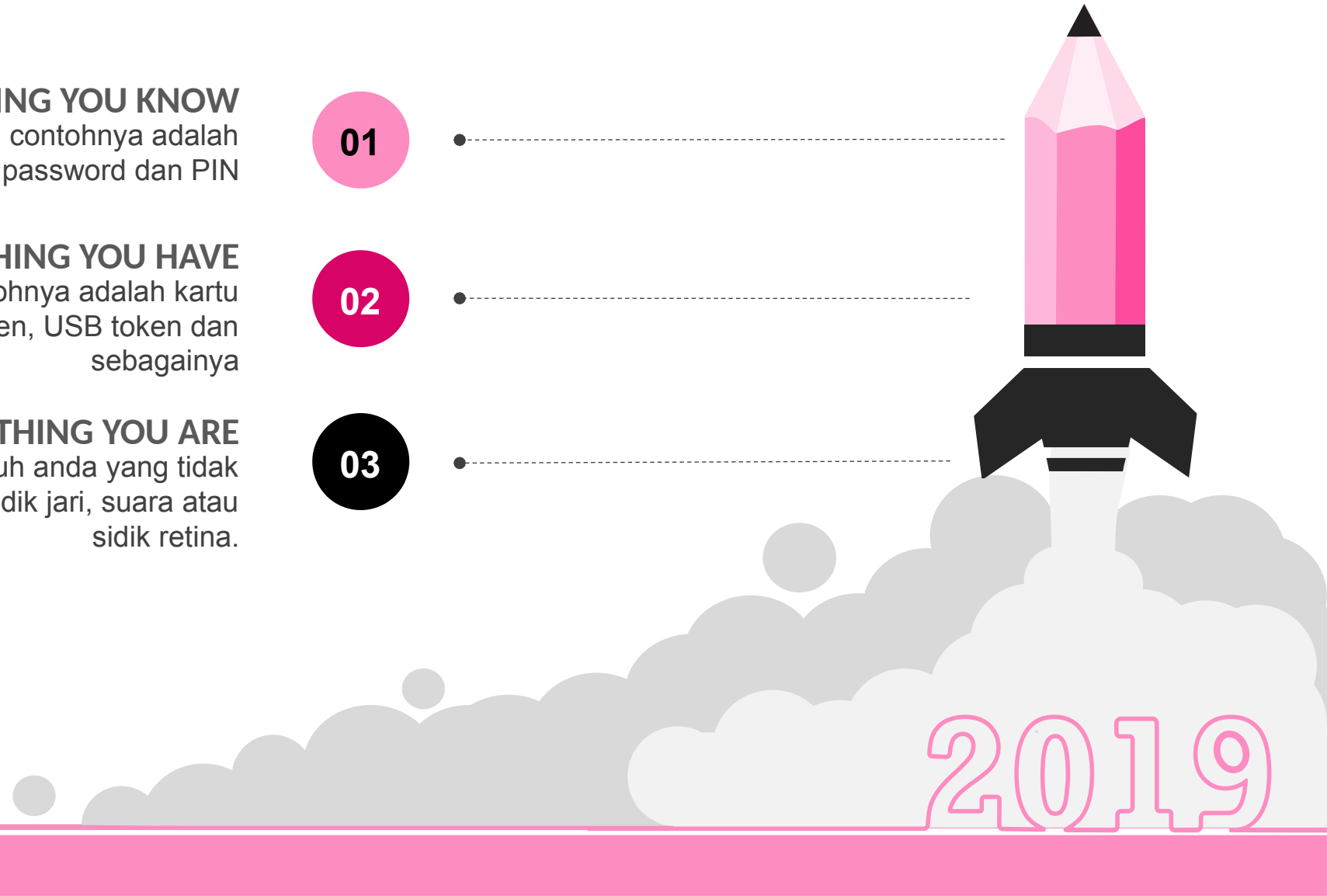
01

SOMETHING YOU HAVE
Barang yang sifatnya unik contohnya adalah kartu magnetik/smartcard, hardware token, USB token dan sebagainya

02

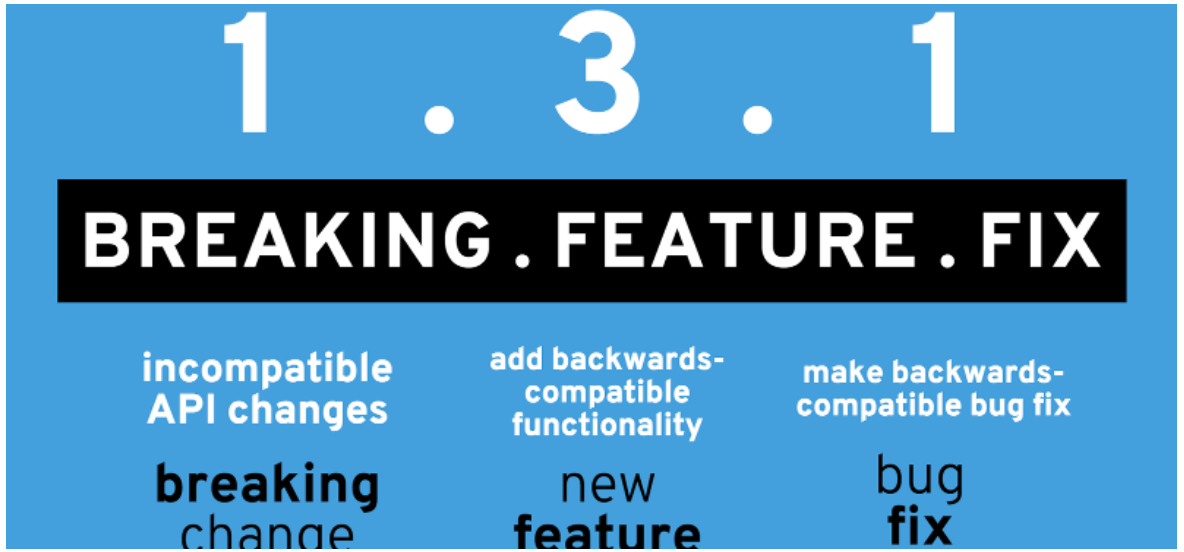
SOMETHING YOU ARE
Meliputi keunikan bagian-bagian tubuh anda yang tidak mungkin ada pada orang lain seperti sidik jari, suara atau sidik retina.

03



Teknik Data Integrity

Dua contoh Teknik Data Integrity



VERSIONING

Keuntungan dari kontrol versi adalah salinan repository yang memiliki semua file dan riwayatnya, dapat disimpan di banyak komputer. Kontrol versi juga memungkinkan Anda untuk membuat penanda yang merujuk keadaan file pada titik waktu tertentu. Ini sering digunakan untuk menunjukkan perubahan besar, seperti versi baru.

DIGITAL SIGNATURE

Tanda tangan,dengan digunakannya papan dan pena khusus di mana pemakai menulis tanda tangan, dengan cara penciriannya bukan membandingkan bentuk tanda tangan, tetapi membandingkan gerakan (arah) dan tekanan pada pena saat menulis. Seseorang dapat meniru tanda tangan tetapi sulit meniru persis cara (gerakan dinamis dan irama tekanan) saat pembuatan tanda tangan.

Teknologi Autentifikasi

PASSWORD

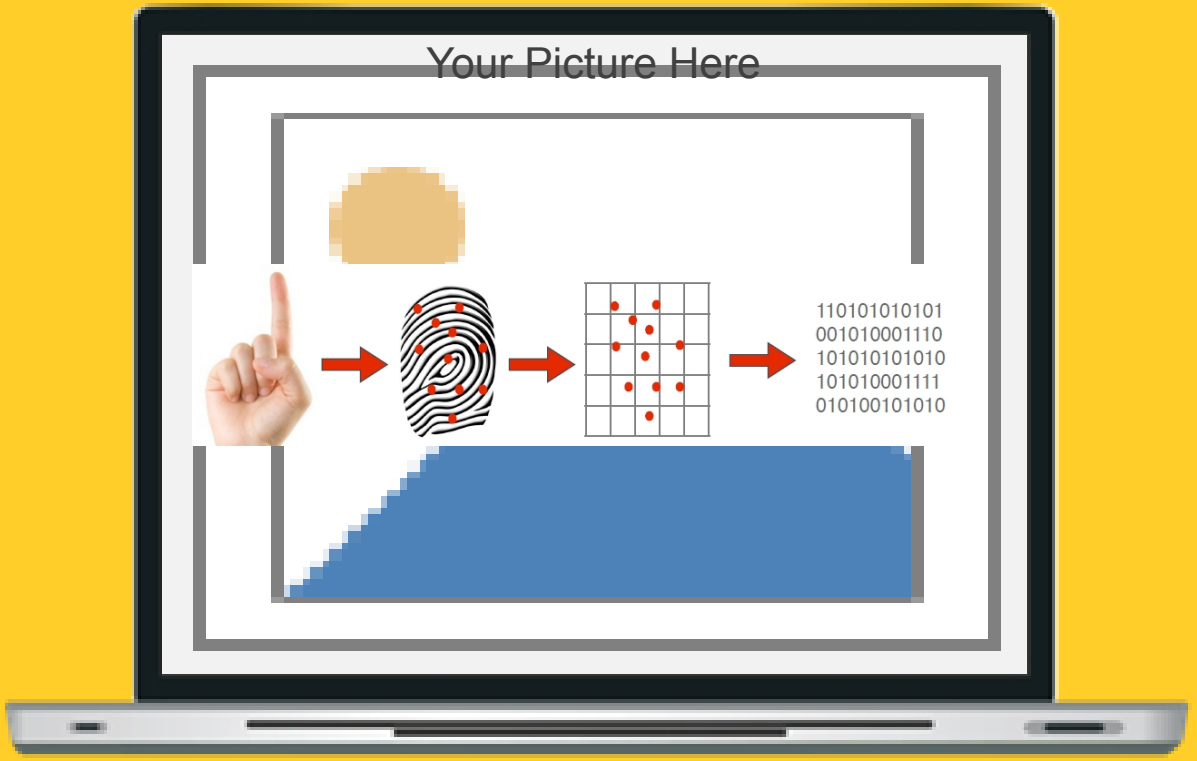
Merupakan bentuk mekanisme dari otentikasi. Seperti yang telah diketahui, password diberikan oleh pengguna dan komputer yang memvalidasi. Jika password telah melakukan kesepakatan dengan user, maka identitas user telah terotentikasi.Tujuan dari sistem otentikasi adalah untuk memastikan bahwa entitas sudah teridentifikasi dengan benar.

BIOMETRIC

Biometric menggambarkan pendeteksian dan pengklasifikasian dari atribut fisik. Terdapat banyak teknik biometric yang berbeda, diantaranya :

- Pembacaan sidik jari (Finger Scan)
- Pembacaan retina/iris
- Pengenalan suara (Voice Scan)
- Dinamika tanda tangan.

Pembacaan Sidik Jari (Finger Scan)



Pembacaan sidik jari sukses apabila :

- Kesesuaian konfigurasi pola global antara kedua buah sidik jari
- Kesesuaian kualitatif (qualitative concordance), yaitu minutiae yang bersesuaian harus identik.
- Faktor kuantitatif, yaitu banyaknya detail minutiae bersesuaian yang ditemukan harus memenuhi syarat minimal yaitu 12 minutiae
- Detail minutiae yang bersesuaian harus identik

 # minutiae refers to specific plot points on a **fingerprint**

Retina Scan

Retina Scan adalah salah satu teknologi biometric yang bekerja pada belakang selaput mata (selaput jala). Retinal scan sampai sekarang penggunaannya masih sangat jarang, mungkin dikarenakan biaya yang sangat tinggi, dan kebanyakan orang berpendapat, dengan menggunakan teknologi ini bisa menimbulkan gangguan pada mata.

Retina Scan

Kelebihan Retina Scan

- Sulit untuk dimanipulasi karena menggunakan konsep ‘something you are’, berupa keunikan retina mata setiap individu
- Mencegah individu yang tidak mempunyai otorisasi untuk melakukan akses terhadap asset organisasi
- Memungkinkan dilakukan audit trial terhadap setiap kejadian yang ada, di mana retina scan dapat diketahui siapa yang melakukan akses terhadap asset atau data perusahaan (who), di mana (where), dan kapan individu melakukannya (when).

Retina Scan

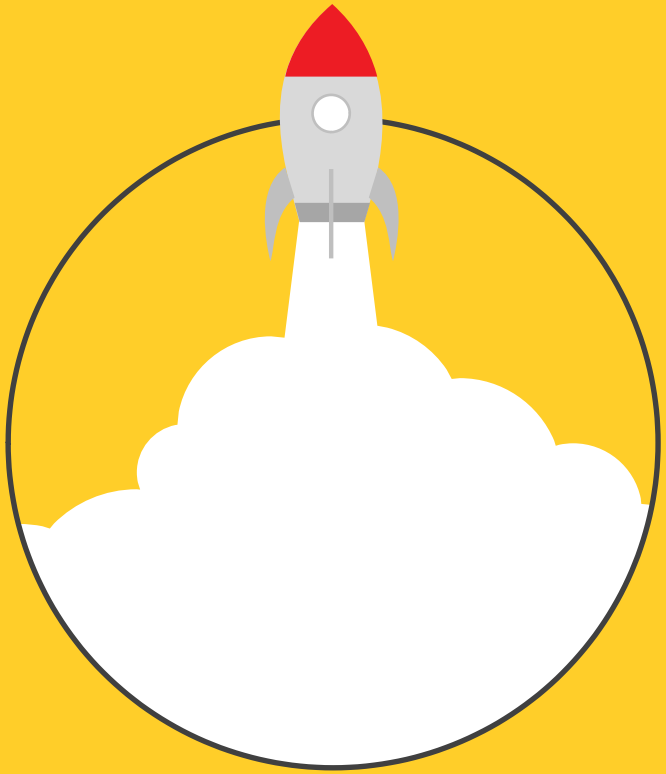
Kelemahan Retina Scan

- Retinal scan tidak selalu akurat
  Retinal scan ini tidak bisa 100 persen akurat dan kurang cocok sebagai alat keamanan universal karena meski biasanya seumur hayat manusia pola pembuluh darah kapiler retinanya tidak berubah, namun penyakit diabetes, glaucoma, dan katarak mampu mengubahnya.
- Biaya sangat mahal untuk implementasinya

Voice Scan

Aspek yang dapat menjadi perbandingan dalam menentukan pemilik suara

- Dasar suara/bunyi
- Bunyi sengau (yang keluar dari hidung)
- Gerakan jakun
- Irama
- Tingkat suara atau bunyi
- Frekuensi dan durasi



Enkripsi

Penjelasan singkat Enkripsi

Pengertian Enkripsi

Enkripsi adalah sebuah metode pengubahan bentuk wujud atau data menjadi wujud yang sangat sulit untuk dipahami tanpa menggu-nakan sebuah pola ataupun kunci tertentu. Dengan demikian semua data penting yang di input di internet tidak akan mudah dicuri.

Sejarah Enkripsi

Kata enkripsi berasal dari bahasa Yunani kryptos yang berarti tersembunyi atau rahasia. Dulu ketika masih banyak orang yang belum bisa membaca, menuliskan pesan rahasia dengan cara biasa sudah terbilang cukup pada masa itu. Namun tentu hal tersebut tentu sangat tidak efektif, hingga kemudian mulailah dikembangkan skema enkripsi untuk mengubah pesan menjadi bentuk yang tidak dapat dibaca guna menjaga kerahasiaan dari pesan tersebut ketika akan diantar ke sebuah tempat yang lain.

Pada tahun 700 sebelum masehi orang-orang Sparta menulis pesan yang sesitif pada kulit yang dililit pada sebuah tongkat yang disebut scytale. Ketika tulisan tersebut dilepas akan menghasilkan karakter yang acak sehingga tidak mampu dibaca. Namun bila digunakan tongkat dengan diameter yang sama, maka kumpulan karakter acak itu dapat diuraikan kembali (decrypt) sehingga mampu dibaca oleh penerima

Lanj. Sejarah Enkripsi

Diwaktu yang lain, orang Romawi menggunakan apa yang disebut Sandi Chaesar. Enkripsi jenis ini terbilang sederhana dimana masing-masing huruf pada teks di-gantikan oleh huruf lain yang memiliki selisih tertentu dalam alfabet. Jika misalnya angka yang ditentukan adalah tiga, maka pesan “nesabamedia” akan menjadi “qhvdedphgld”. Sekilas mungkin ini terlihat sulit untuk di uraikan kembali, namun bila anda memperhatikan kata yang sering digunakan seperti penggunaan huruf D=A, akan mempermudah proses enkripsi.

Dan hingga pada pertengahan tahun 1970-an, enkripisi melakukan sebuah lompatan yang besar, dimana B. Whit-field Diffie dan Martin Hellman memecahkan salah satu masalah mendasar dari kriptografi, yaitu bagaimana cara mendistribusikan kunci enkripsi dengan aman untuk digu-nakan kepada mereka yang membutuhkannya. Hal terse-but kemudian dikembangkan bersama dengan RSA dan mencitpakan sebuah implementasi public-key menggu-nakan algoritma asimetris, yang mana kemudian menjadi era baru untuk enkripsi hingga saat ini.

Jenis Enkripsi

Jenis Key

Jenis Data

Jenis Key

Single key (Enkripsi Simetris)

Simetris adalah enkripsi yang paling sederhana yang hanya melibatkan satu kunci rahasia untuk menyandikan dan menguraikan informasi. Enkripsi simetris merupakan teknik lama dan paling terkenal. Metode ini menggunakan kunci rahasia yang bisa berupa angka, kata atau string huruf acak. Ini adalah gabungan *plain text* (teks polos) yang dipadukan dengan sebuah konten dengan cara tertentu. Pengirim dan penerima harus mengetahui kunci rahasia yang digunakan untuk mengenkripsi dan mendekripsi semua pesan. Contoh enkripsi simetris adalah Blowfish, AES, RC4, DES, RC5, dan RC6, sedangkan algoritma simetris yang paling umum digunakan adalah AES-128, AES-192, dan AES-256.

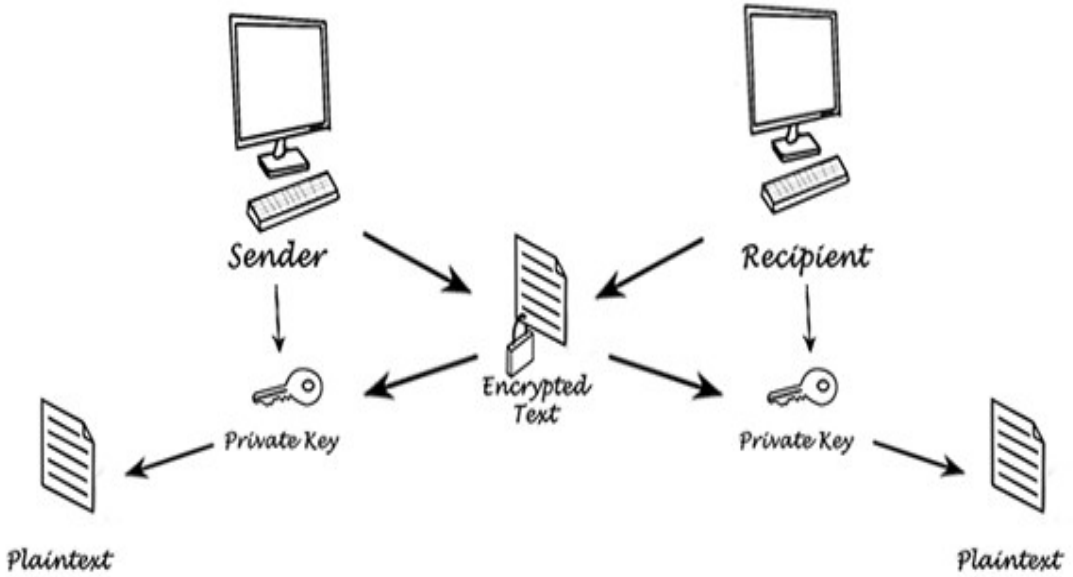
Kelemahan enkripsi simetris ini bahwa semua pihak yang terlibat harus menukar kunci yang digunakan untuk mengenkripsi data sebelum mereka dapat mendekripsinya.

Jenis Key

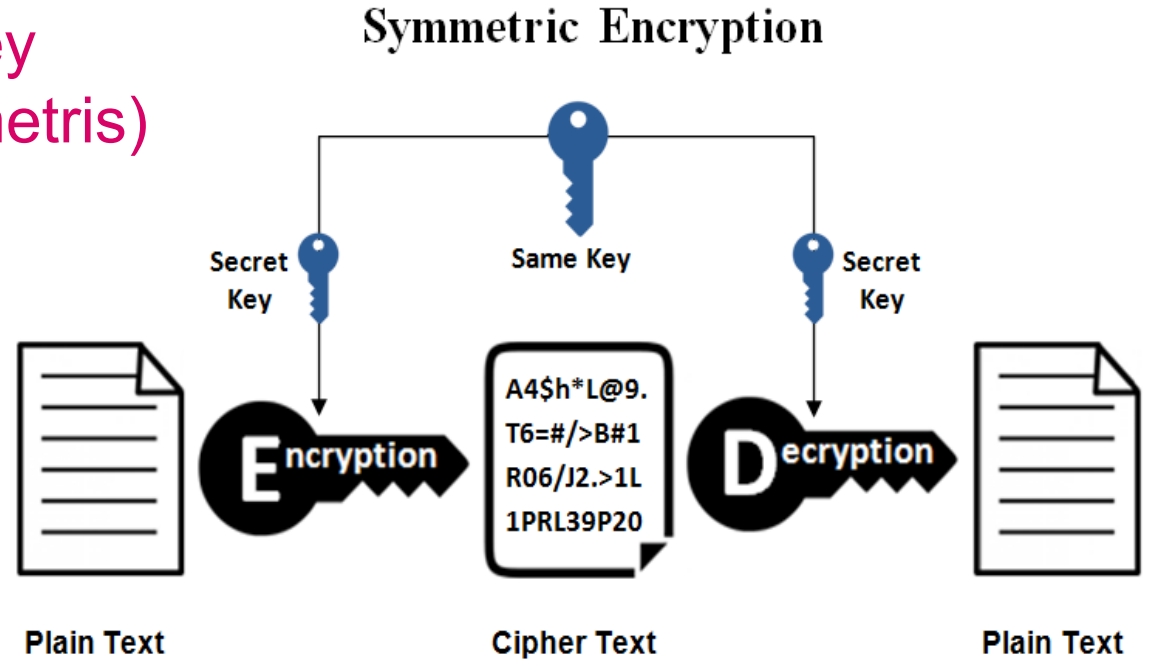
Single key (Enkripsi Simetris)

Kelemahan enkripsi simetris ini bahwa semua pihak yang terlibat harus menukar kunci yang digunakan untuk mengenkripsi data sebelum mereka dapat mendekripsinya.

Contoh: Seseorang mengirimkan data yang dienkripsi kepada seorang rekannya, jika rekannya ingin mendekripsinya maka ia harus mendapatkan kuncinya dari si pengirim. Intinya Seorang pengirim data dapat melakukan enkripsi dan deksripsi data dengan menggunakan satu kunci yang sama.



Single key
(Enkripsi Simetris)



Jenis Key

Double Key (Enkripsi Asimetris)

Enkripsi asimetris juga dikenal sebagai kriptografi menggunakan kunci publik (public-key), yang merupakan pengembangan dari metode enkripsi simetris dan lebih menjamin keamanan. Enkripsi asimetris menggunakan dua kunci yaitu kunci publik (public key) dan kunci pribadi (private key). Kunci publik tersedia secara bebas bagi siapa saja yang mungkin ingin mengirimkan pesan kepada Anda, namun Kunci pribadi (kunci kedua) dirahasiakan sehingga hanya Anda yang mengetahuinya.

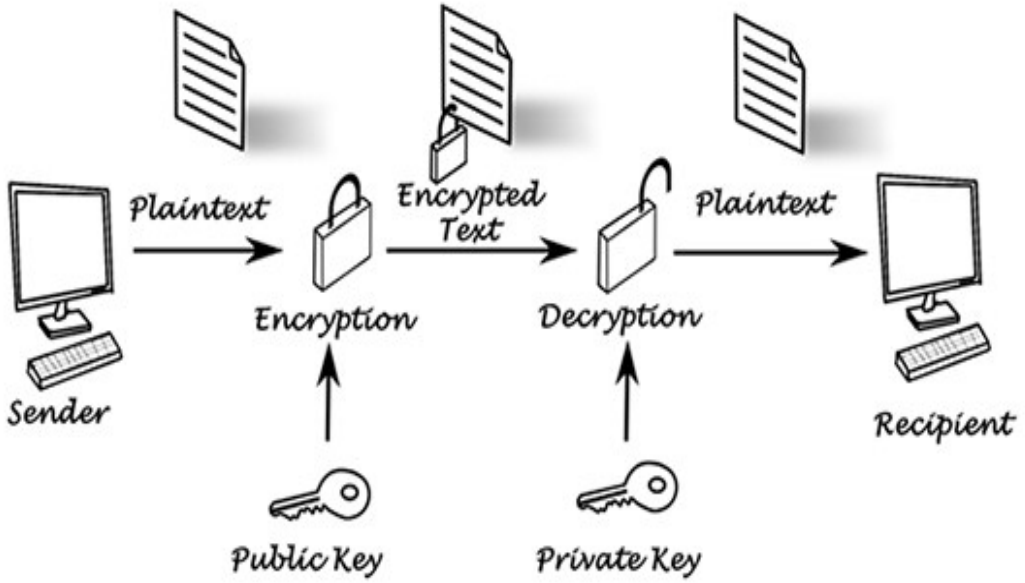
Pesan yang dienkripsi menggunakan kunci publik hanya dapat didekripsi dengan menggunakan kunci pribadi, sementara pesan yang dienkripsi menggunakan kunci pribadi dapat didekripsi dengan menggunakan kunci publik. Keamanan kunci publik tidak diperlukan karena tersedia untuk umum dan bisa ditransmisikan melalui internet. Kunci asimetris memiliki kekuatan yang jauh lebih baik dalam menjamin keamanan informasi yang ditransmisikan selama komunikasi berlangsung.

Jenis Key

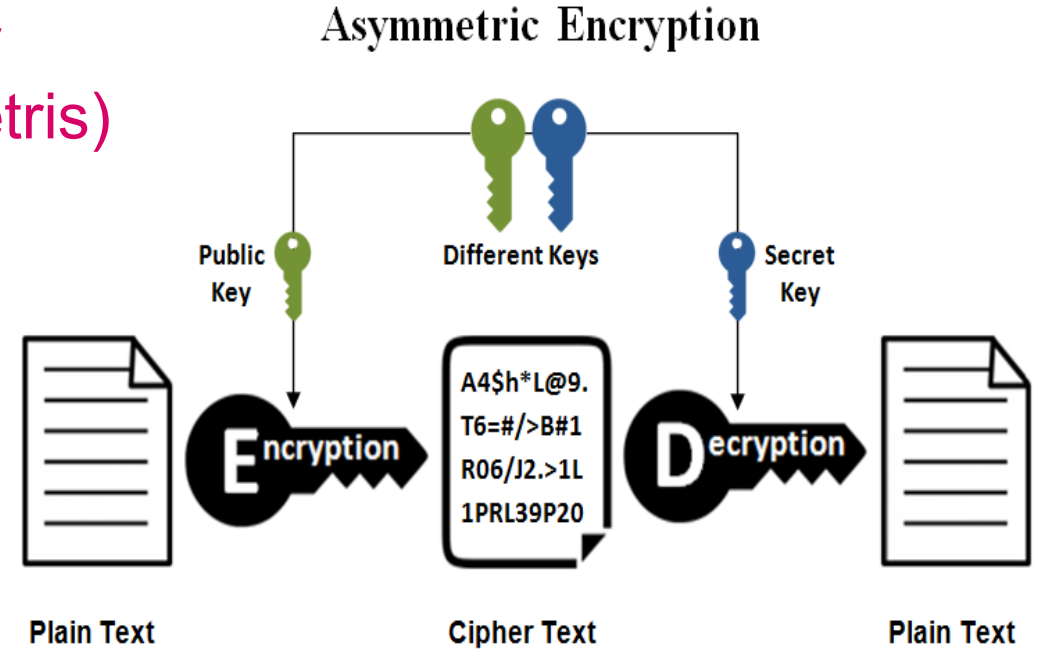
Double Key (Enkripsi Asimetris)

Enkripsi asimetris banyak digunakan dalam saluran komunikasi sehari-hari, terutama melalui Internet. Algoritma enkripsi asimetris yang populer digunakan antara lain EIGamal, RSA, DSA, Elliptic, dan PKCS.

Contoh: Seseorang mengirimkan sebuah data yang telah dienkripsi kepada rekannya. Data tersebut dienkripsi dengan public key yang dimilikinya dan hanya bisa didekripsi oleh rekannya tersebut menggunakan privat key. Pada skenario ini public key digunakan untuk mengenkripsi data tersebut dan privat key digunakan untuk mendekripsinya.



Double Key
(Enkripsi Asimetris)



Jenis Data

Pada enkripsi

Dokumen

Enkripsi dokumen adalah proses di mana dokumen dilindungi dengan kunci kriptografi (kata sandi, kunci publik, token, dll.) sehingga hanya individu dengan kunci dekripsi yang sesuai (kata sandi, kunci pribadi, token, dll.) yang dapat membukanya. Ini digunakan untuk melindungi dokumen dalam perjalanan (dikirim melalui email) dan sisanya (Disimpan pada disk atau di cloud) agar tidak diakses oleh pengguna yang tidak sah.

Program enkripsi dokumen dapat berupa **aplikasi mandiri** (seperti PGP, yang mengenkripsi file apa pun dan bukan hanya dokumen) atau **plugin untuk aplikasi tertentu** seperti MS-Word atau Adobe Acrobat yang memungkinkan dokumen dienkripsi saat disimpan ke disk.

Tidak semua enkripsi dokumen sama. Sementara sebagian besar program enkripsi dokumen memberikan enkripsi AES 256 bit yang disetujui NIST, program tersebut memiliki tiga metode perlindungan - beberapa memberikan **perlindungan kata sandi**, yang lain menggunakan **token hardware**, sedangkan sisanya **menyediakan teknologi kunci publik (PKI)**. Setiap skema memiliki kelebihan dan kekurangannya sendiri. Kata sandi dapat diberikan (dan seringkali lemah dan karenanya mudah rusak), token harus didistribusikan dan dipelihara, dan teknologi kunci publik harus memiliki hierarki manajemen.

Audio

Dua konsep yang perlu dipertimbangkan sebelum memilih teknik pengkodean untuk audio:

- **Format audio digital**
- **Media transmisi audio** (jalur yang diambil audio dari pengirim ke penerima) juga harus dipertimbangkan kapan penyandian pesan rahasia dalam audio.

Tiga format audio digital utama yang biasanya digunakan:

- **Sample Quantization** yang merupakan Arsitektur pengambilan sampel linier 16-bit digunakan oleh audio populer format seperti (.WAV).
- **Temporal Sampling Rate** menggunakan frekuensi yang dapat dipilih (dalam KHz) untuk sampel audio
- **Perceptual Sampling** Format ini mengubah statistik audio secara drastis dengan melakukan penyandian hanya pada bagian yang dirasakan pendengar yang mempertahankan suara tetapi mengubah sinyal. Format ini digunakan oleh audio digital paling populer di Internet saat ini dalam ISO MPEG (MP3.

Video

Enkripsi video adalah proses menjaga keamanan video Anda dari pengintaian. Terdapat dua alasan untuk mengenkripsi video, yaitu **Personal dan Digital Rights Management (DRM)**.

Personal encryption, seperti namanya, digunakan untuk privasi pribadi. Misalnya, ketika Anda membuat video dan ingin membagikannya dengan keluarga, teman, pelanggan, dll., Tetapi pada saat yang sama, Anda tidak ingin konten dilihat oleh orang yang tidak berwenang.

Digital Rights Management melibatkan lebih banyak kompleksitas. Berbagai tingkat DRM adalah:

- Streaming video kualitatif dan kuantitatif
- Video yang berpusat pada regional
- Video yang berpusat pada perangkat atau media
- Video yang berpusat pada software
- Streaming adaptif

Video

Dua **Jenis** enkripsi video:

- **Video offline**

Advanced Encryption Standard (AES) – 128, 192 or 256 bits
Google Widevine
Apple Fair Play for videos from iTunes
Marlin
Windows Protected Media Path or PMP

- **Video online/streaming**

RTMFP and RTMP(E)
Soon-to-arrive HTML5 DRM standard

Sistem enkripsi yang paling aman adalah **AES**, yang telah diadopsi oleh pemerintah Amerika Serikat dan sekarang digunakan di seluruh dunia.

Gambar

Gambar dienkripsi karena berbagai alasan, yaitu:

- **Mengidentifikasi pencipta suatu gambar**
- **Melindungi informasi hak cipta**
- **Menghalangi pembajakan**
- **Memblokir gambar agar tidak dilihat oleh pengguna yang seharusnya tidak memiliki akses**

Dengan mengenkripsi gambar, Anda dapat mengirimnya melalui email atau melalui Internet tanpa khawatir gambar Anda dilihat oleh orang-orang yang tidak ingin Anda lihat. Mengenkripsi gambar pada komputer di rumah Anda juga akan memberi Anda ukuran keamanan jika hacker mendapatkan akses ke hard drive Anda, dan mengenkripsi gambar pada laptop atau smartphone Anda juga akan membuat gambar Anda lebih aman jika komputer atau laptop Anda hilang atau dicuri.

Gambar

Gambar dapat dienkripsi dengan cara yang sama seperti teks dienkripsi oleh software. Dengan menjalankan urutan operasi matematika, yang disebut algoritma, pada data biner yang terdiri dari gambar, software enkripsi **mengubah nilai angka-angka dengan cara yang dapat diprediksi**. Kunci software diperlukan untuk **membuka kunci kode enkripsi**, dan itu dibuat oleh software yang sama yang dapat mengacak gambar. **Gambar terenkripsi dan kunci dikirim ke penerima secara terpisah untuk meminimalkan kemungkinan peretas dapat mencegat keduanya**. Kunci software, yang biasanya merupakan jenis kata sandi, **diketik ke dalam software dekripsi untuk menguraikan gambar yang disandikan**. Keamanan enkripsi tergantung pada seberapa sulit data yang dienkripsi untuk tidak dienkripsi.

Gambar

Software enkripsi untuk menyandikan gambar, seperti:

- **Microsoft** menyediakan **BitLocker** dengan **Windows 7**
- **Mac OS X** dilengkapi dengan **FileVault**
- Salah satu program **pihak ketiga** adalah **TrueCrypt**, yang dapat membuat sistem operasi umpan untuk membingungkan para peretas.
- **Dropbox, PowerFoler, dan Cloudfogger** adalah sistem penyimpanan file online yang menyertakan enkripsi sebagai bagian dari keamanan data mereka.

Beberapa program enkripsi akan memungkinkan Anda mengolah gambar, dan sebagian besar dapat menangani file gambar umum seperti BMP, TIF, RAW, PSD, dan JPG. Aplikasi telepon memungkinkan Anda untuk mengenkripsi gambar Anda langsung di ponsel Anda. Aplikasi enkripsi untuk smartphone berbasis **Android** termasuk **WhisperCore dan Droid Crypt**, dan aplikasi **iPhone** termasuk **Kryptos dan SecuMail**.

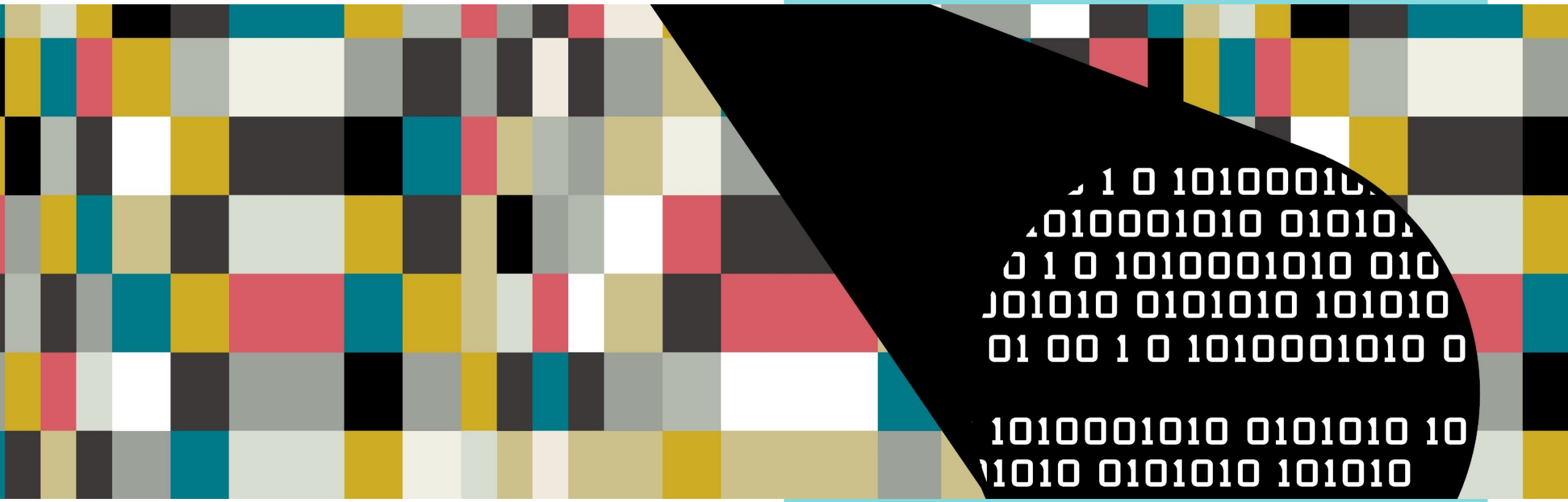
Steganografi

Penjelasan singkat Steganografi

Pengertian

Steganografi

Steganografi atau Steganography adalah sebuah ilmu, teknik atau seni menyembunyikan sebuah pesan rahasia dengan suatu cara sehingga pesan tersebut hanya akan diketahui oleh si pengirim dan si penerima pesan rahasia tersebut. Steganografi berasal dari Bahasa Yunani yaitu Stegano yang berarti “tersembunyi atau menyembun-yikan” dan graphy yang berarti “Tulisan, jadi Steganografi adalah tulisan atau pesan yang disembunyikan. Steganografi kebalikannya kriptografi yang menya-markan arti dari sebuah pesan rahasia saja, tetapi tidak menyembunyikan bahwa ada sebuah pesan.



Steganografi vs Enkripsi (Kriptografi)

Perbedaan Steganografi dan Enkripsi (Kriptografi)

Basis for comparison	Steganography	Cryptography
Basic	It is known as cover writ-ing.	It means secret writing.
Goal	Secret communication	Data protection
Structure of the message	Not altered	Altered only of the transmission.
Popularity	Less popular	More commonly used.
Implemented on	Audio, video, image, text.	Only on text files.
Types of attack	Steganalysis	Cryptanalysis

Kesimpulan Perbedaan

Perbedaan Steganografi dan Enkripsi (Kriptografi)

Perbedaan yang mendasar mengenai kriptografi dan steganografi adalah hasil tampilan pesan ketika sudah disisipi pesan rahasia. Pada kriptografi pesan yang sudah disisipi pesan rahasia akan sangat berbeda dengan pesan sebelum disisipi pesan rahasia. Maka bagi pihak ketiga yang melihat pesan hasil keluaran kriptografi akan curiga walaupun pihak ketiga tersebut juga tidak mengetahui maksud dari pesan tersebut.

Sedangkan pada steganografi, pesan yang sudah disisipi pesan rahasia akan tampak sama (dengan kasat mata) dengan pesan sebelum disisipi pesan rahasia (pesan rahasia tersamarkan dalam cover text). Sehingga pihak ketiga tidak tahu bahwa dibalik pesan asli (cover text) tersembunyi pesan rahasia dibaliknya.

Keuntungan steganografi dibandingkan dengan kriptografi adalah bahwa pesan dikirim tidak menarik perhatian sehingga media penampung/ cover text yang membawa pesan tidak menimbulkan kecurigaan pihak ketiga.

Thank you