# Konsep Dasar Keamanan Dunia Internet

Modul 1

Muhammad Ogin Hasanuddin

KK Teknik Komputer
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Konsep Dasar Keamanan Dunia Internet sebagai Perlindungan Berbagai Ancaman

Konsep Digital Citizenship sebagai Kerangka Keamanan Sosial

# Konsep Dasar Keamanan Dunia Internet sebagai Perlindungan Berbagai Ancaman

Serangan terhadap keamanan internet di definisikan sebagai upaya untuk mendapatkan akses ilegal ke berbagai sistem komputer yang akan menyebabkan kerusakan serta membuat ketidaknyamanan bagi individu hingga gangguan ekonomi dan sosial.

Penyerang akan melalukan berbagai tindakan seperti menghapus atau mencuri informasi penting bahkan bisa mengekspos informasi pribadi secara publik, juga mengunci data sehingga mereka meminta tebusan.

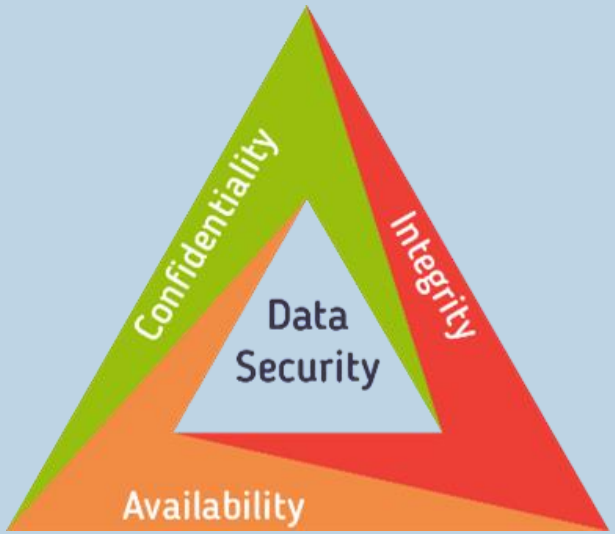
Penyerangan tersebut dapat dilakukan oleh satu atau sekelompok orang bahkan organisasi di mana saja, sehingga diperlukan pengamanan yang meliputi proses, pelatihan dan teknologi.

Tujuan dari keamanan internet adalah untuk melindungi data yang dikenal sebagai Confidentiality, Integrity, and Availability (CIA):

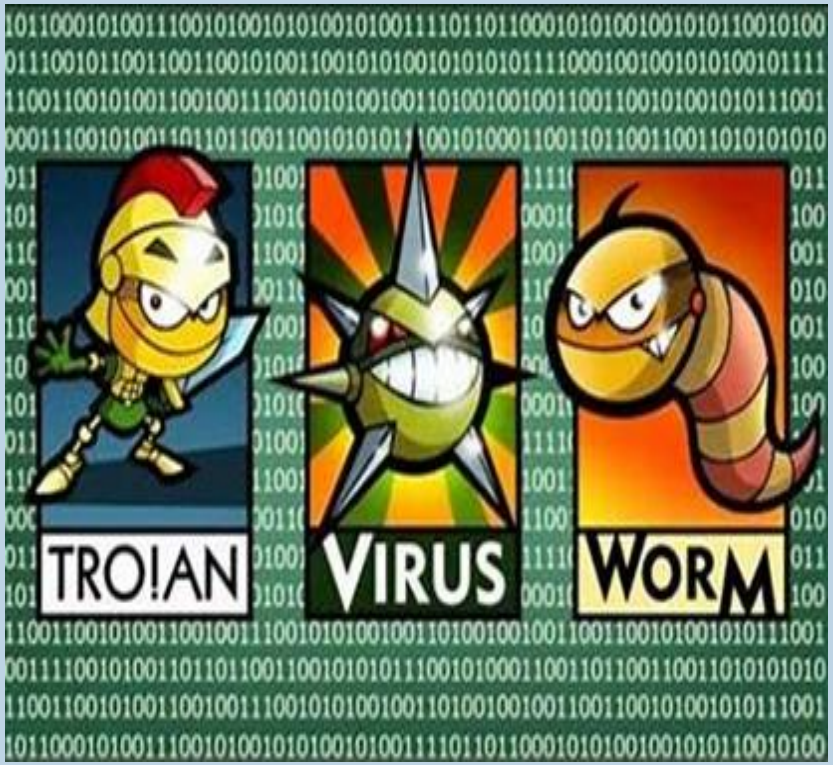
Kerahasiaan : Informasi hanya dapat dilihat oleh orang yang tepat

Integritas : Informasi hanya dapat diubah oleh orang yang tepat

Ketersediaan: Informasi dapat dilihat dan diakses kapan pun dibutuhkan




# Malware




Perangkat lunak yang digunakan oleh penjahat dunia internet untuk melakukan tindakan yang membahayakan disebut dengan *malware*. Malware memiliki dua komponen utama yaitu mekanisme propagasi dan payload.

1. Propagasi, proses dari tindakan malware dalam suatu sistem
    a. Trojan, mengelabui pengguna dengan menjadi perangkat lunak yang asli
    b. Virus, mempengaruhi file lainnya dalam suatu PC pengguna
    c. Worm,menginfeksi perangkat dengan mengeksploitasi kerentanan aplikasi
2. Payload, tindakan yang dilakukan oleh malware kepada sistem yang telah terinfeksi. Beberapa jenis muatannya seperti ransomware yang mengunci sistem hingga korban harus membayar tebusan

# Kriptografi

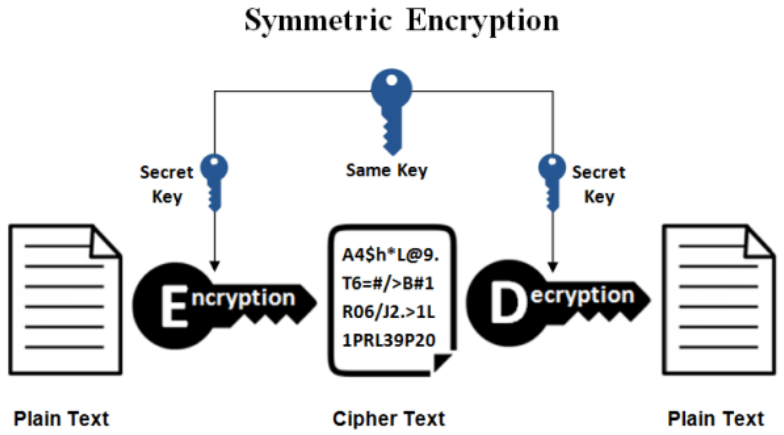
Kriptografi memiliki dua istilah dan frasanya sendiri, diantaranya yaitu :

1. *Plaintext,* meliputi pesan apa pun termasuk dokumen, musik, gambar, film, data, dan program komputer, menunggu untuk diubah secara kriptografis.
2. *Ciphertext,* suatu plaintext yang diubah menjadi pesan rahasia dan meliputi data terenkripsi/aman.

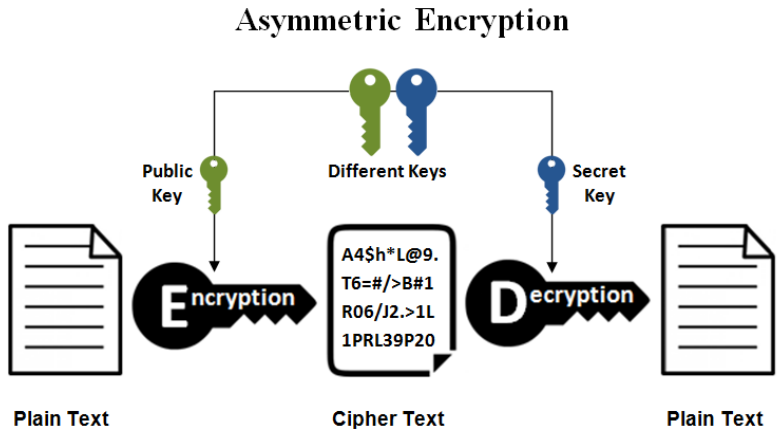
# Enkripsi

Enkripsi merupakan mekanisme dimana pesan plaintext diubah menjadi ciphertext yang tidak dapat dibaca dan bertujuan untuk meningkatkan kerahasiaan data yang dibagikan dengan penerima. Kunci enkripsi terbagi menjadi dua bentuk yaitu :

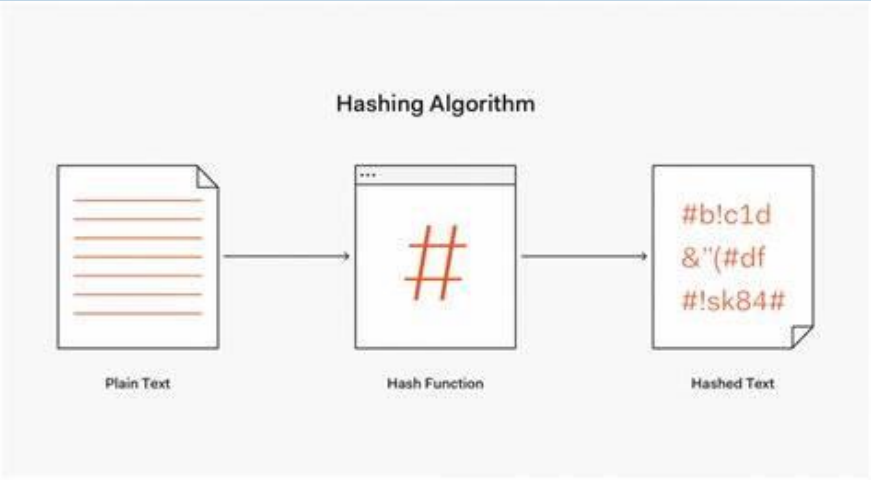
Kunci simetris, berdasar pada gagasan bahwa kunci kriptografi yang sama digunakan untuk enkripsi pesan teks biasa dan deskripsi pesan teks sandi dan cepat membuat metode enkripsi.




Kunci asimetris, berdasar pada distribusi yang aman dengan mengubah cara kunci kriptografi yang dibagikan. Kunci publik dapat dibagikan dengan siapa saja, sehingga individu dan organisasi tidak perlu khawatir tentang distribusinya yang aman.



# Hashing




Hashing menggunakan algoritma yang dikenal sebagai fungsi hashing untuk mengubah teks asli menjadi nilai tetap yang unik, itu disebut sebagai nilai hash. Setiap kali teks di hash menggunakan algoritma yang sama, akan menghasilkan nilai hash yang sama. Hashing berbeda dengan enkripsi karena tidak menggunakan kunci dan nilai hash tersebut tidak dapat mendekripsi kembali ke aslinya.

# Autentifikasi

Ada beberapa metode autentifikasi, di antaranya yaitu :

a. Sesuatu yang kita ketahui, termasuk :

1. Kata sandi
2. Nomor PIN
3. Pertanyaan Keamanan

b. Sesuatu yang kita miliki, termasuk :

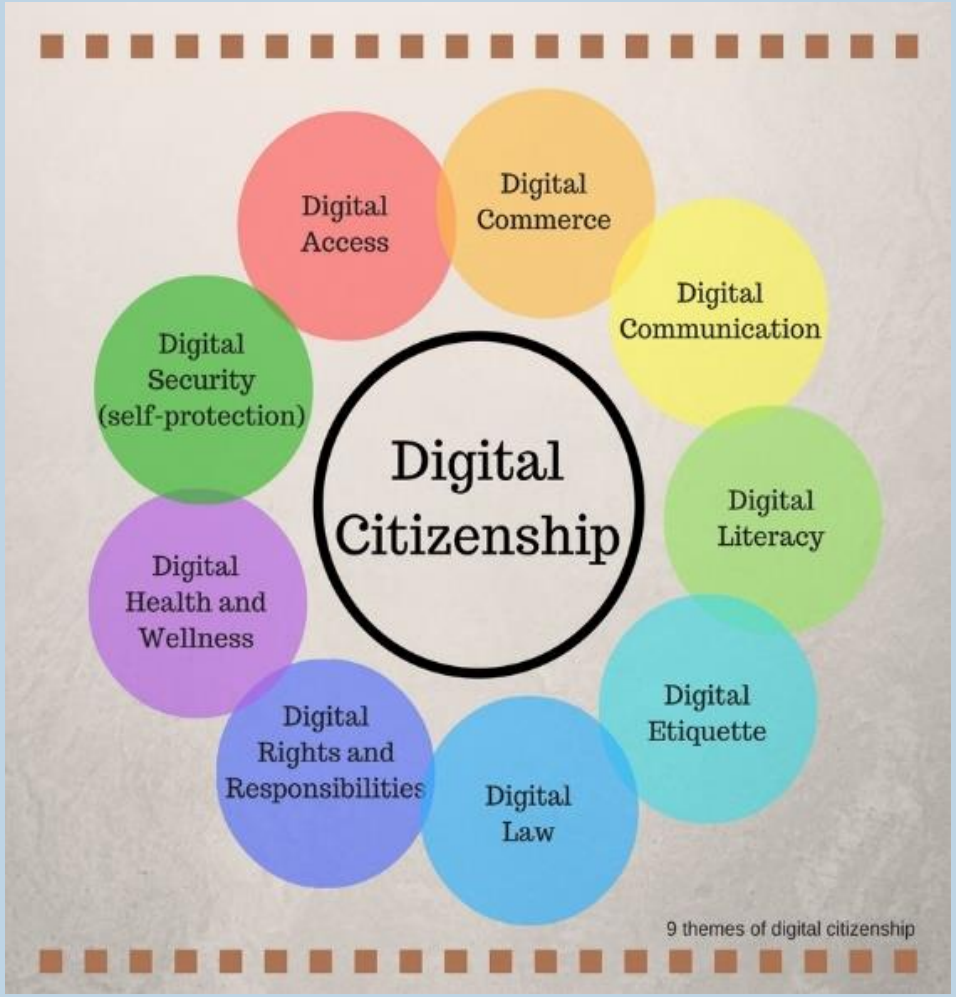
1. Kartu identitas
2. Komputer
3. Handphone

c. Sesuatu yang lainnya, termasuk :

1. Sidik jari
2. Pengenalan wajah
3. Bentuk lainnya dari ID biometric (karakteristik fisik yang secara unik mengidentifikasi individu tersebut)

# Konsep Digital Citizenship sebagai Kerangka Keamanan Sosial

Menggunakan teknologi dengan baik dan memahami bagaimana tindakan online memengaruhi diri sendiri dan orang lain. Keduanya merupakan keterampilan dasar yang diperlukan untuk memahami pentingnya mengelola dan memonitor perilaku dalam menggunakan teknologi di lingkungan pendidikan saat ini. Profesor Matematika di Harold Washington College di Chicago, Illinois, Ignacio Estrada, mengatakan, "Jika seorang anak tidak dapat belajar dengan cara kita mengajar, mungkin kita harus mengajar dengan cara mereka belajar." dan yang dikatakan oleh George Couros, pendidik pengajaran inovatif Kanada, “Teknologi tidak akan pernah menggantikan guru-guru hebat, tetapi teknologi di tangan guru-guru hebat adalah transformasi.”



# Pandangan Pedadogi


1. Online berarti kita dapat memperhatikan dengan seksama bagaimana tindakan seseorang memengaruhi orang lain dan meluangkan waktu untuk merenungkan kiriman konten sebelum mengirimnya.
2. Publik, menganalisis cara merepresentasikan diri saat online dalam membangun dan memberikan jejak digital yang positif. Setiap tindakan, postingan, suka, dan komentar meninggalkan jejak di dunia digital yang tidak mudah dilupakan.
3. Pribadi, dapat terhubung dengan orang lain dengan aman antar dua orang.
4. Patuh, mengikuti pedoman hak cipta dan mengenali kepemilikan konten digital..
5. Tanggap, mengevaluasi sumber dengan strategi literasi digital termasuk memahami berbagai perspektif.


Thank You
See You Next
Chapter