

# MATA KULIAH CYBER SECURITY

Program Studi Magister Informatika

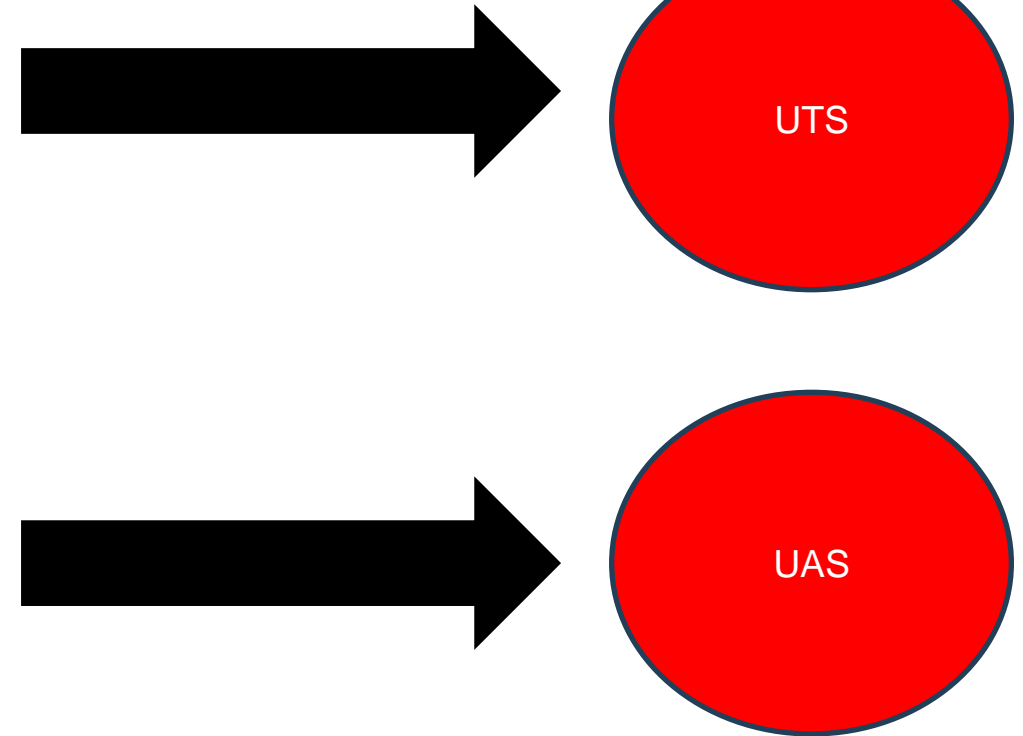
Universitas AMIKOM Yogyakarta  
Tahun 2025

*Creative Economy Park"*



# Outline Mata Kuliah Selama 1 Semester

1. Ruang lingkup keamanan cyber menurut framework Cyber Security Body of Knowledge (CyBoK)
2. Serangan infrastruktur jaringan
3. Malware
4. Serangan aplikasi desktop dan web
5. Social engineering
6. Solusi pengamanan data dan sistem modern
7. Regulasi dan kebijakan cyber law di Indonesia
8. Implementasi kebijakan keamanan TI
9. Penetration testing
10. Digital Forensic



# Cyber Security

PERTEMUAN 7

Universitas AMIKOM Yogyakarta  
Tahun 2025

*Creative Economy Park"*



# Cyber Security Governance

(Tata Kelola Keamanan Siber)

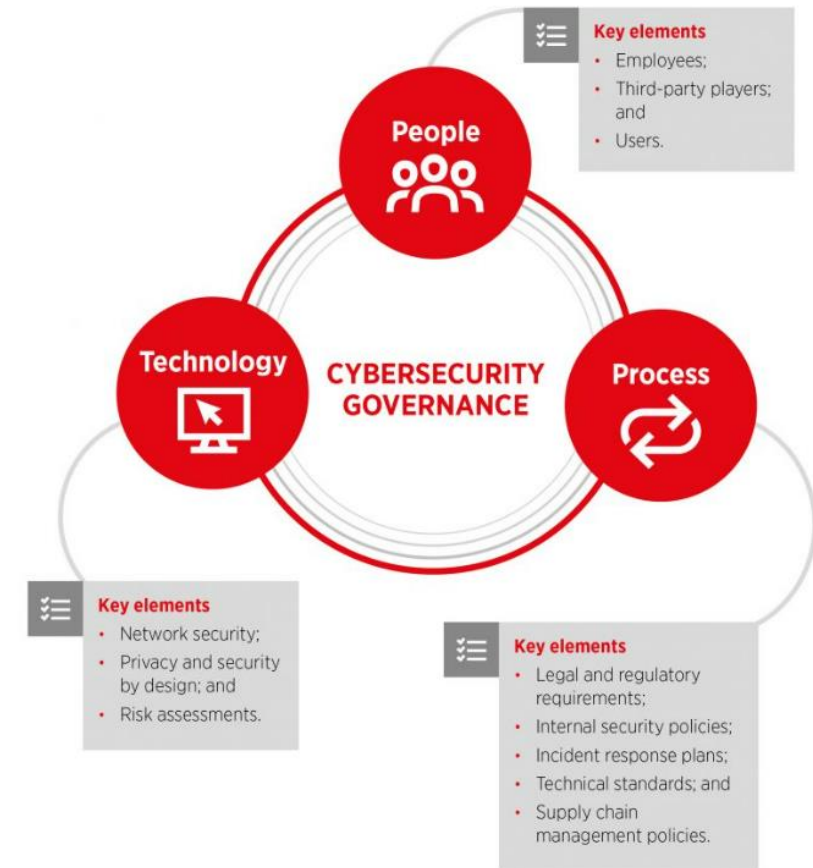
Minggu 7



# Cybersecurity Governance

- **Tata Kelola Keamanan Siber** adalah suatu pendekatan terstruktur untuk merancang, mengimplementasikan, mengelola, memonitor, dan memperbarui **keamanan siber** dalam suatu organisasi.
- **Tujuannya** adalah untuk **melindungi** sistem komputer, jaringan, data, dan informasi dari ancaman keamanan yang mungkin timbul. Tata kelola keamanan siber mencakup kebijakan, prosedur, teknologi, dan orang-orang yang bekerja bersama-sama untuk **menciptakan lingkungan yang aman** secara digital.

A cybersecurity governance framework for mobile money providers



# Referensi untuk memahami mengenai tata kelola keamanan siber

## 1. NIST Cybersecurity Framework:

- National Institute of Standards and Technology (NIST). ([2018](#)). Framework for Improving Critical Infrastructure Cybersecurity. NIST Cybersecurity Framework.

## 2. ISO/IEC 27001:

- International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.

## 3. COBIT (Control Objectives for Information and Related Technologies):

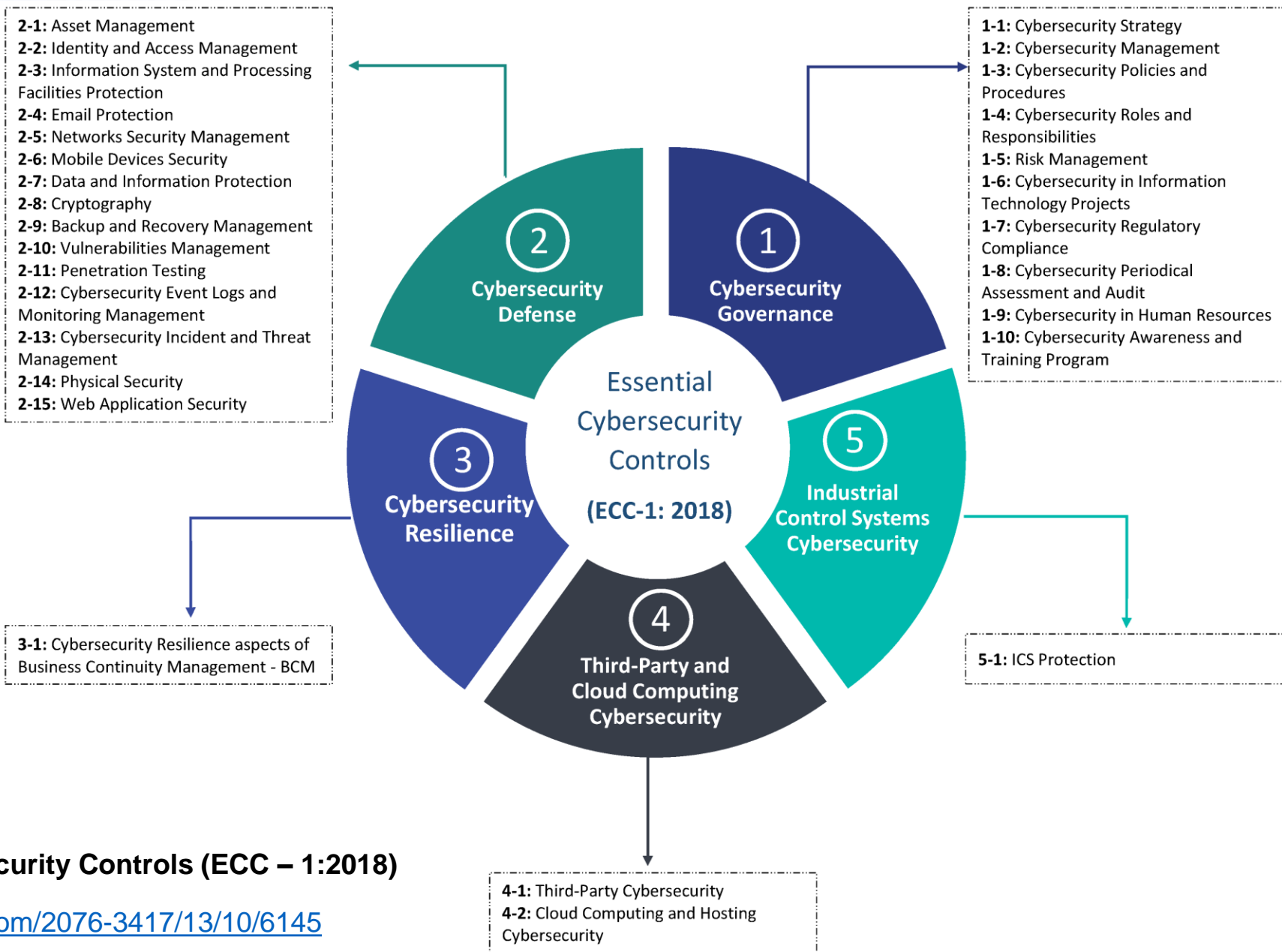
- ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology.

## 4. ITIL (Information Technology Infrastructure Library):

- AXELOS. (2019). ITIL 4: The IT Infrastructure Library.

## 5. SANS Institute:

- SANS Institute. (2021). Critical Security Controls for Effective Cyber Defense.



## Essential Cybersecurity Controls (ECC – 1:2018)

<https://www.mdpi.com/2076-3417/13/10/6145>

# Cyber Securities and Cyber Terrorism

Course : PGDCL-05



Vardhaman Mahaveer Open University,  
Kota

**Cyber securities  
and  
Cyber Terrorism**

- Dalam bukunya *Cyber Securities and Cyber Terrorism*, L.R. Gurjar membahas berbagai isu terkait privasi dan keamanan daring.
- Secara khusus, dalam Unit 8 yang berjudul "*Online Privacy and Security Issues*", penulis menguraikan sejumlah topik penting yang mencerminkan tantangan utama dalam privasi dan keamanan digital.
- Sumber: [https://assets.vmou.ac.in/PGDCL05.pdf?utm\\_source=chatgpt.com](https://assets.vmou.ac.in/PGDCL05.pdf?utm_source=chatgpt.com)



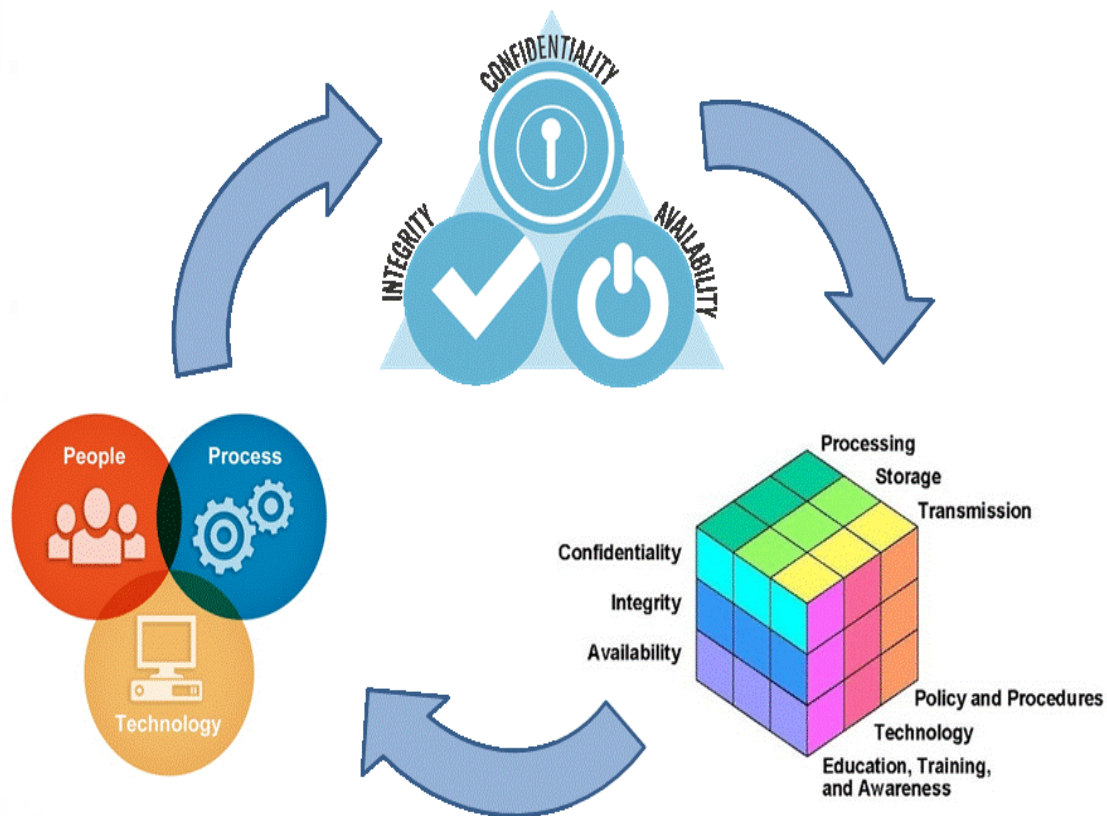


## 8 Issue Online Privacy and Security Issues

1. **Risiko Daring (Online Risks)** Ancaman terhadap data pribadi akibat aktivitas daring, termasuk pencurian identitas dan penyalahgunaan informasi pribadi.
2. **Isu Privasi Daring dan Pengawasan Daring (Online Privacy Issues and Online Surveillance)** Kekhawatiran tentang pengumpulan dan pemantauan data pribadi oleh pemerintah dan perusahaan tanpa persetujuan pengguna.
3. **Masalah Kebijakan Privasi (Privacy Policy Problems)** Kurangnya transparansi dan pemahaman dalam kebijakan privasi yang diterapkan oleh berbagai platform digital.
4. **Upaya OECD dalam Privasi (OECD Work on Privacy)** Inisiatif dan pedoman yang dikeluarkan oleh OECD untuk melindungi privasi individu di era digital.
5. **Perlindungan Data dalam Transmisi (Protecting Data in Transit)** Langkah-langkah untuk memastikan keamanan data saat dikirim melalui jaringan, termasuk penggunaan protokol keamanan.
6. **Enkripsi Pesan (Message Encryption)** Penggunaan teknik enkripsi untuk melindungi isi pesan dari akses yang tidak sah selama transmisi.
7. **Enkripsi Ujung ke Ujung (End to End Encryption)** Metode enkripsi yang memastikan hanya pengirim dan penerima yang dapat membaca pesan, tanpa intervensi pihak ketiga.
8. **Kebijakan Keamanan Siber Pemerintah India 2013 dan Pedoman untuk Kafe Siber (Indian Government Cyber Security Policy, 2013 and Guidelines for Cyber Café in India)** Kebijakan dan pedoman yang diterapkan oleh pemerintah India untuk meningkatkan keamanan siber dan melindungi privasi pengguna.

Sumber: [https://assets.vmou.ac.in/PGDCL05.pdf?utm\\_source=chatgpt.com](https://assets.vmou.ac.in/PGDCL05.pdf?utm_source=chatgpt.com)

# Cybersecurity Governance



**Gambar Konsep Cybersecurity Governance**

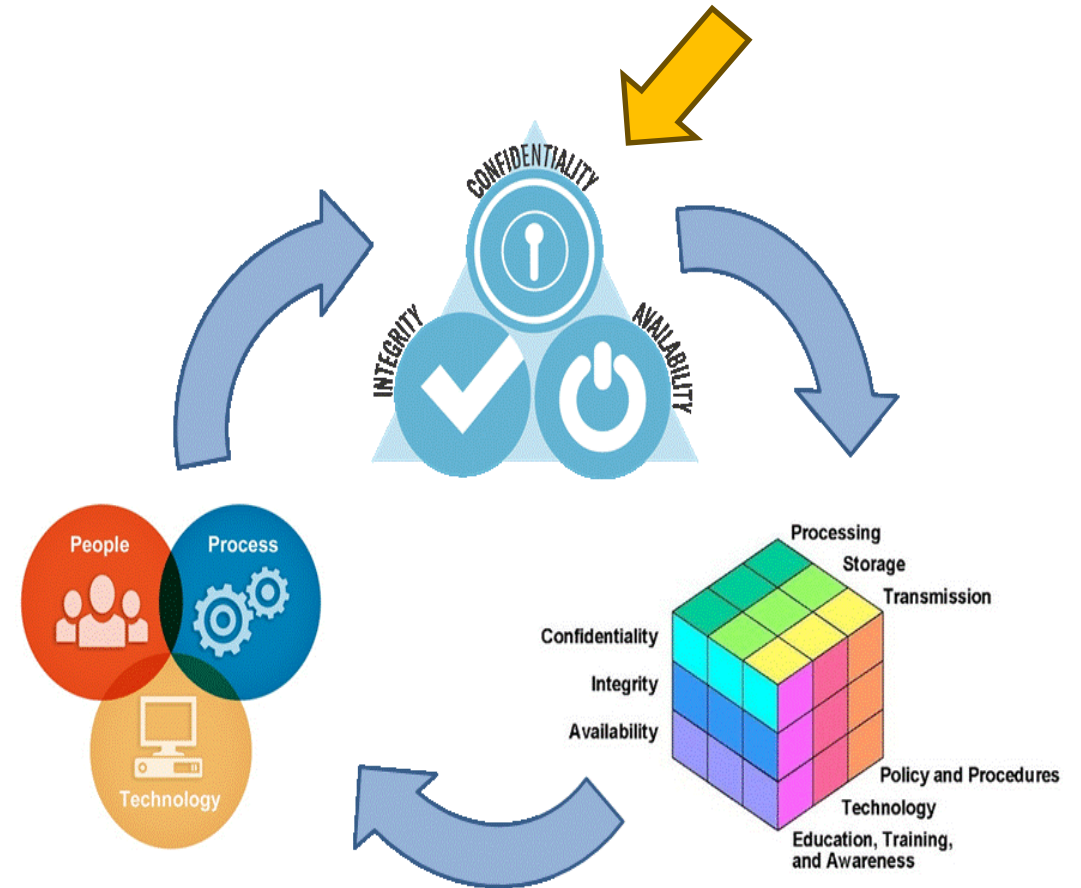
# Elemen Utama Cyber Security (CIA Triad)

## Elemen Utama Cyber Security (CIA Triad)

Elemen ini adalah landasan dari keamanan informasi:

- **Confidentiality (Kerahasiaan)** Menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang.
- **Integrity (Integritas)** Menjamin bahwa data tidak diubah tanpa otorisasi.
- **Availability (Ketersediaan)** Menjamin bahwa data dan sistem tersedia saat dibutuhkan.

*Ketiganya membentuk siklus yang berkelanjutan dan saling mendukung.*



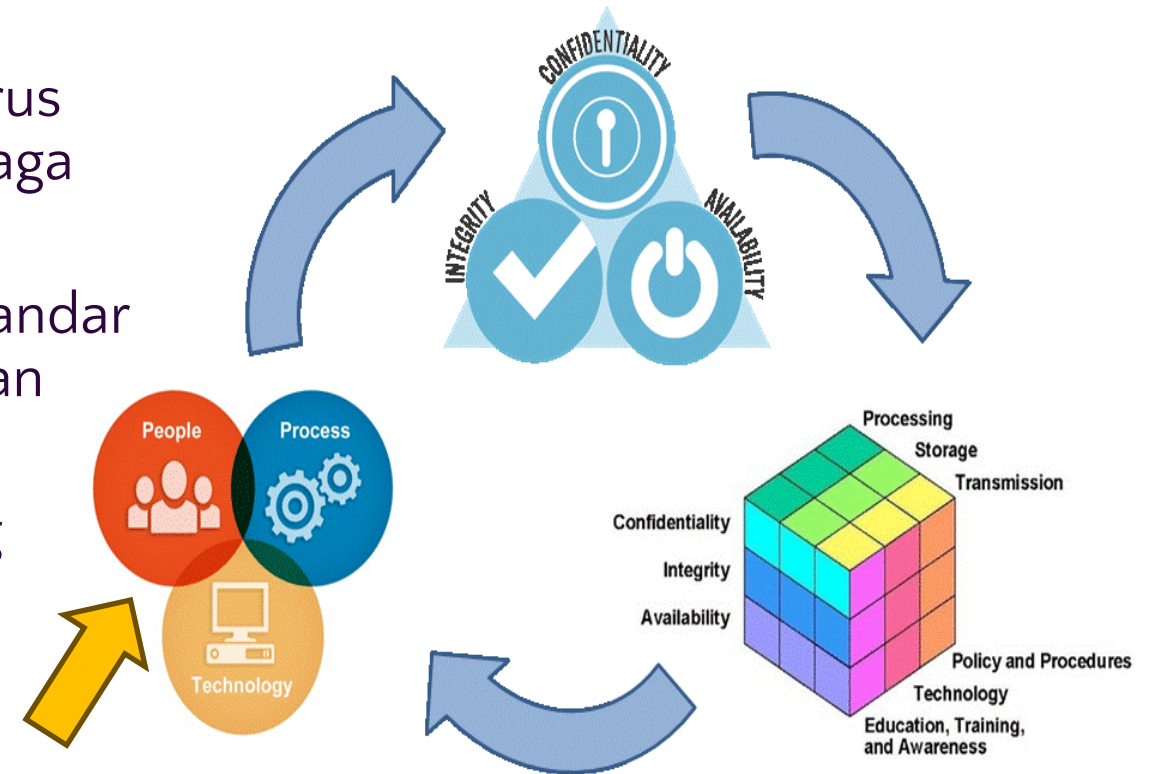


# Pilar Cyber Security: People, Process, Technology

Tiga pilar ini adalah aktor utama dalam pelaksanaan dan pengelolaan keamanan siber:

- **People (Manusia)** Operator, pengguna, administrator, hingga eksekutif – mereka harus dilatih dan sadar akan perannya dalam menjaga keamanan.
- **Process (Proses)** Kebijakan, prosedur, dan standar operasional yang dirancang untuk memastikan tindakan keamanan yang konsisten.
- **Technology (Teknologi)** Alat dan sistem yang digunakan untuk melindungi aset informasi.

*Ketiga pilar ini harus saling mendukung dan dikembangkan secara seimbang.*





# Cyber Security Cube

Model kubus ini menambahkan dimensi operasional dan domain keamanan:

## Dimensi Horizontal (Tujuan Keamanan):

- *Confidentiality*
- *Integrity*
- *Availability*

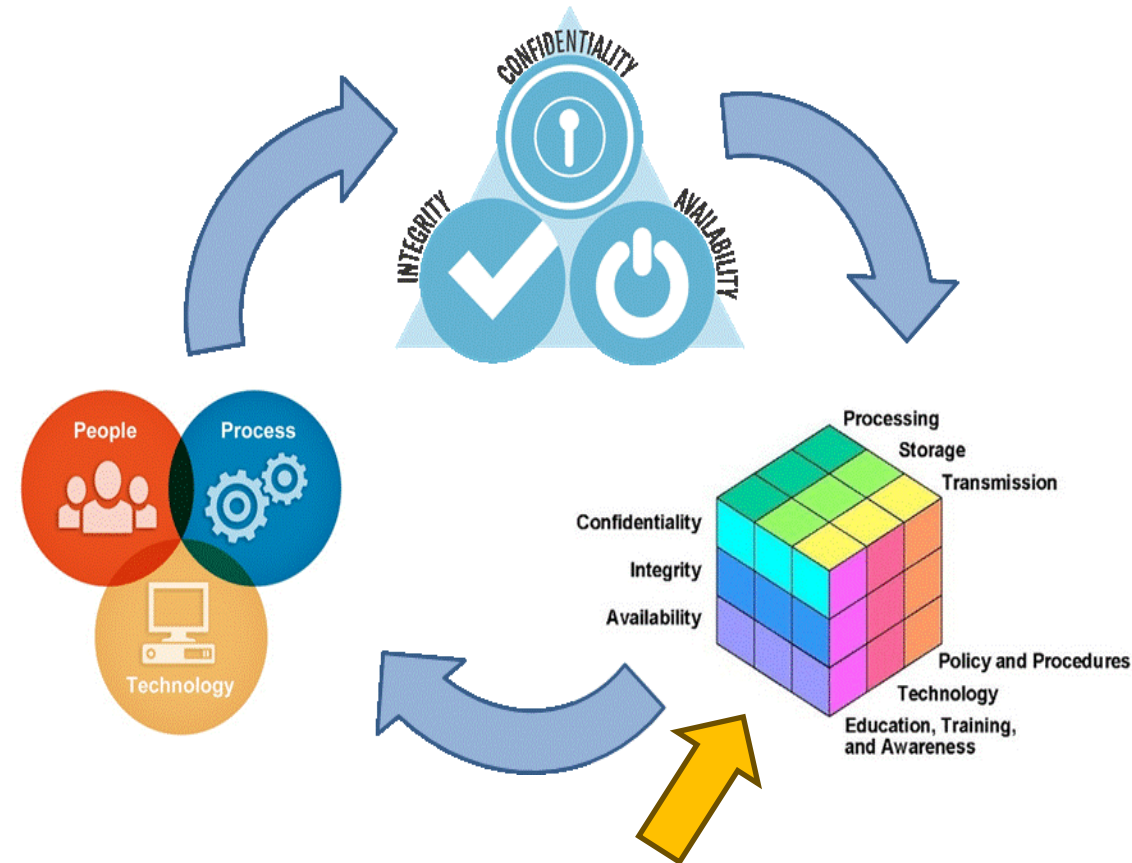
## Dimensi Vertikal (Tahapan Informasi):

- *Processing*
- *Storage*
- *Transmission*

## Dimensi Ketiga (Mekanisme Pendukung):

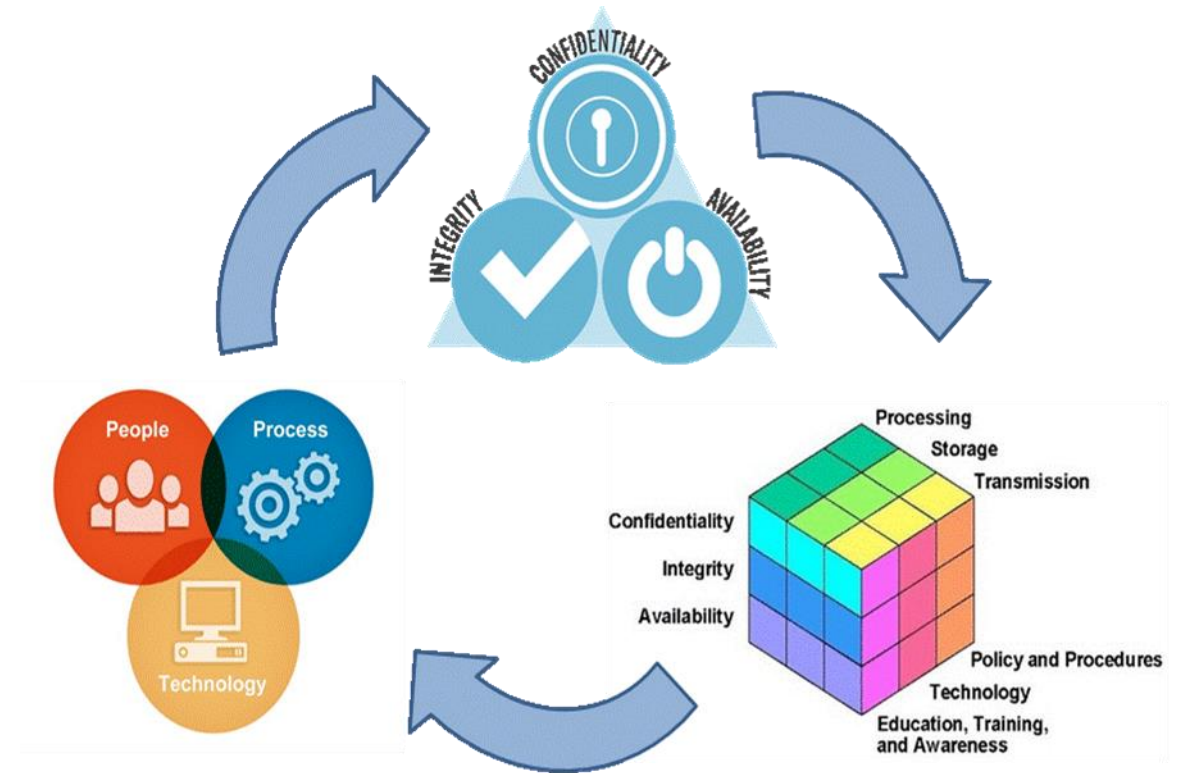
- *Policy and Procedures*
- *Technology*
- *Education, Training, and Awareness*

*Kubus ini menggambarkan bagaimana dimensi keamanan, loka: mekanisme pengamanan saling berpotongan.*

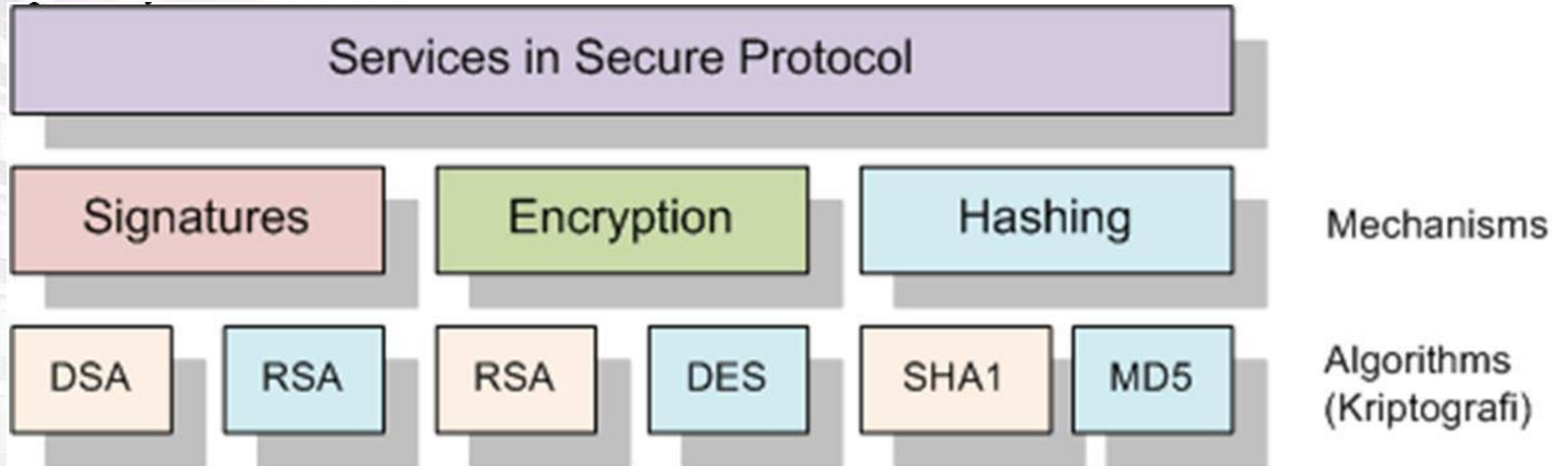


# Relasi Antar Entitas

- **CIA Triad** adalah **tujuan** utama yang harus dicapai.
- **People, Process, Technology** adalah **aktor dan metode** untuk mencapai tujuan CIA.
- **Cybersecurity Cube** adalah **kerangka kerja strategis dan operasional** yang menggabungkan kedua elemen di atas dalam konteks implementasi nyata.
- Ketiga model ini **saling melengkapi dan tidak bisa berdiri sendiri**, menunjukkan bahwa manajemen keamanan siber adalah integrasi antara kebijakan, perilaku manusia, dan teknologi yang kuat.



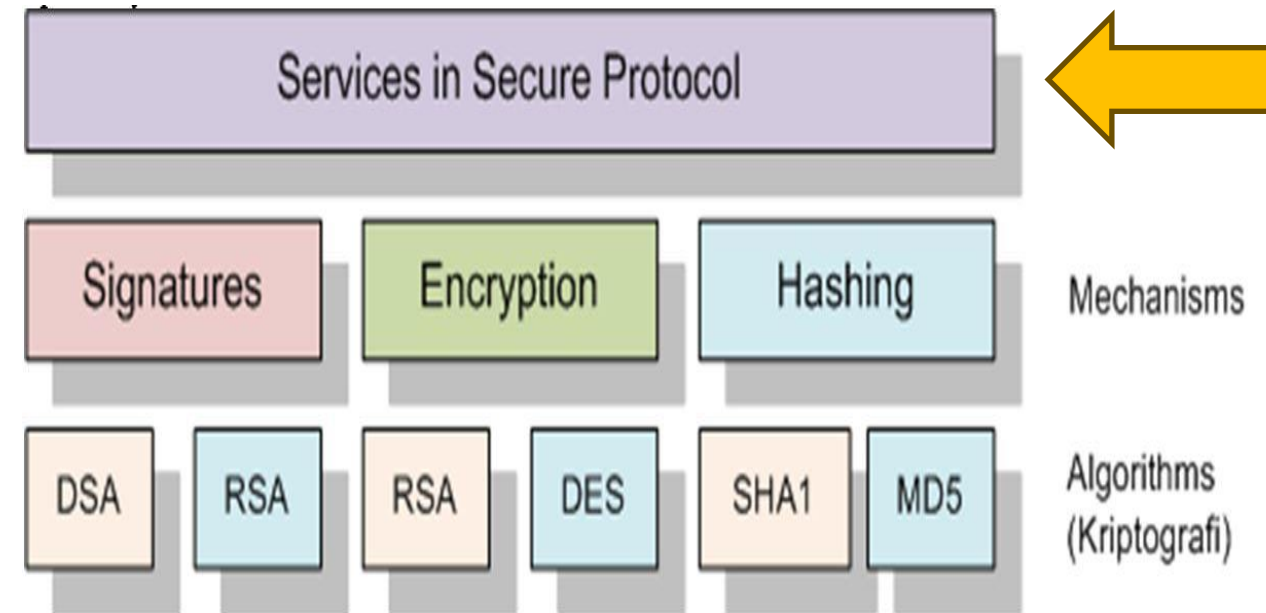
# Skema dalam struktur *information security*



# 1. Lapisan Atas: Services in Secure Protocol

Lapisan ini merepresentasikan **layanan utama** yang disediakan dalam protokol keamanan, yaitu:

- **Signatures** Digunakan untuk **menjamin keaslian (authenticity)** dan **integritas** data serta **non-repudiasi**. Contohnya: tanda tangan digital dalam e-mail atau dokumen resmi.
- **Encryption** Menyediakan **kerahasiaan (confidentiality)** dengan mengubah data asli menjadi bentuk terenkripsi agar tidak bisa dibaca oleh pihak tidak sah.
- **Hashing** Memberikan jaminan **integritas** dengan menghasilkan nilai ringkas dari data (hash) untuk mendeteksi perubahan atau manipulasi data.



**Skema dalam struktur *information security***



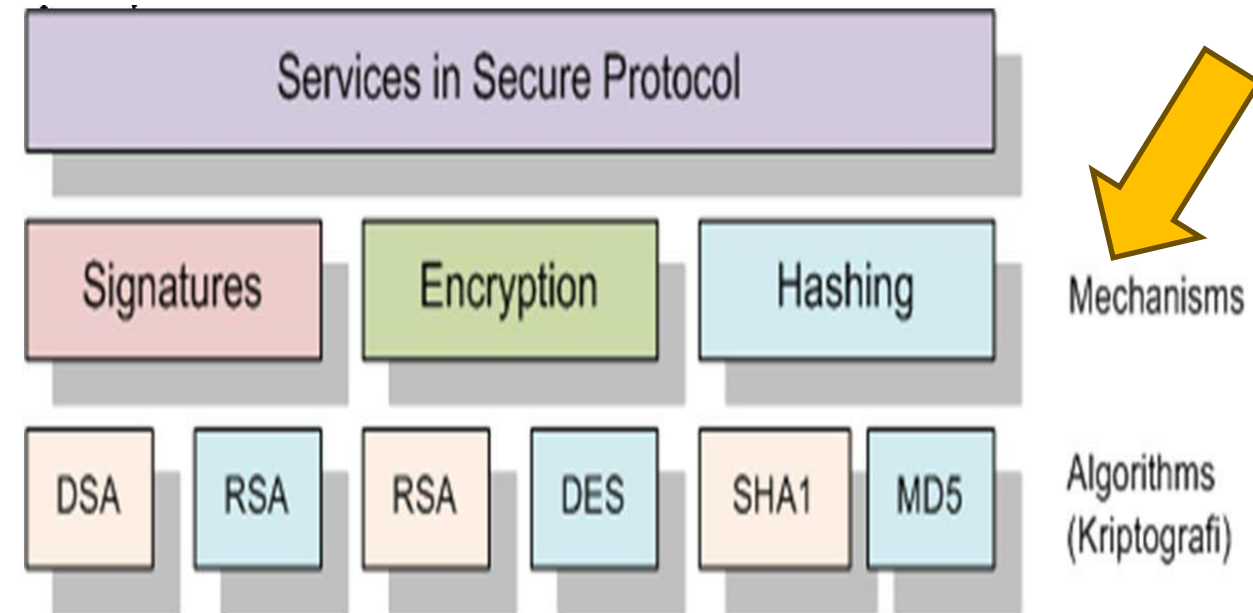
## 2. Lapisan Tengah: Mechanisms

### 2. Lapisan Tengah: Mechanisms

Ini adalah **mekanisme teknis** yang digunakan untuk mengimplementasikan layanan keamanan:

- **Signature Mechanism** → menggunakan algoritma seperti **DSA** dan **RSA**.
- **Encryption Mechanism** → didukung oleh algoritma seperti **RSA** (asymmetric) dan **DES** (symmetric).
- **Hashing Mechanism** → menggunakan algoritma seperti **SHA1** dan **MD5**.

Mekanisme ini berperan sebagai **penghubung** antara layanan yang dibutuhkan dan algoritma yang digunakan.

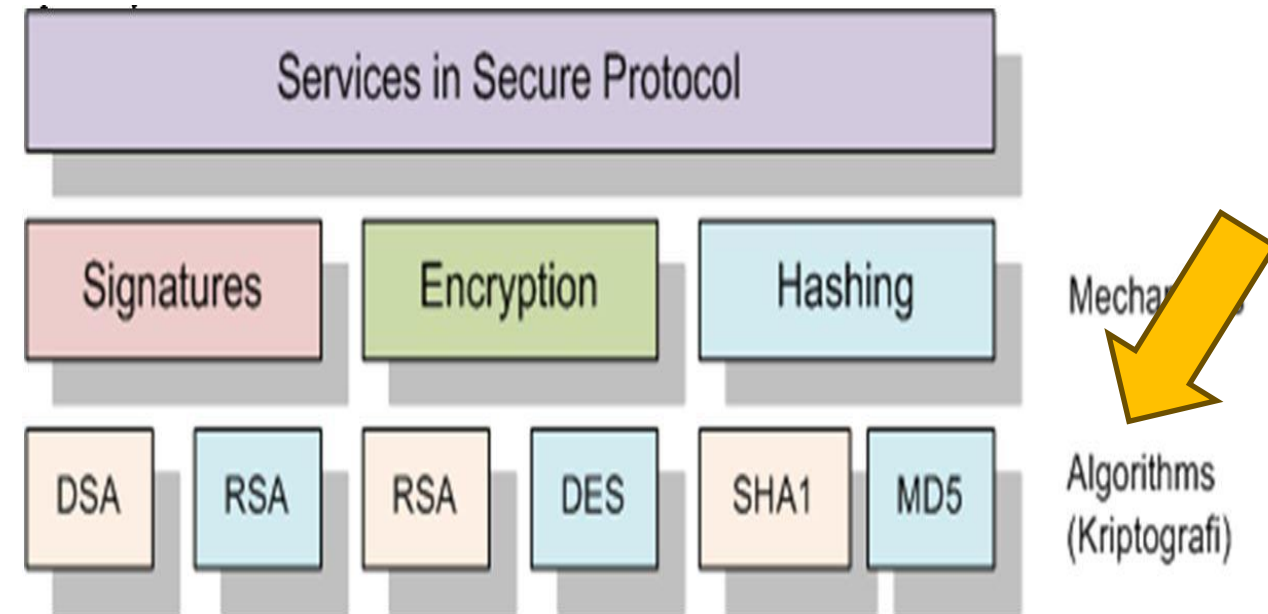


Skema dalam struktur *information security*

### 3. Lapisan Bawah: Algorithms (Kriptografi)

Lapisan ini adalah **fondasi matematis** dan **logika kriptografi** yang digunakan oleh mekanisme untuk menjalankan layanan:

- **DSA (Digital Signature Algorithm):** Digunakan untuk digital signature.
- **RSA (Rivest-Shamir-Adleman):** Algoritma kriptografi kunci publik, dapat digunakan untuk **enkripsi** maupun **tanda tangan digital**.
- **DES (Data Encryption Standard):** Algoritma enkripsi simetris.
- **SHA1 (Message-Digest Algorithm 5), MD5 (Message-Digest Algorithm 5):** Fungsi hash yang digunakan untuk mengubah data menjadi hash (fingerprint digital).



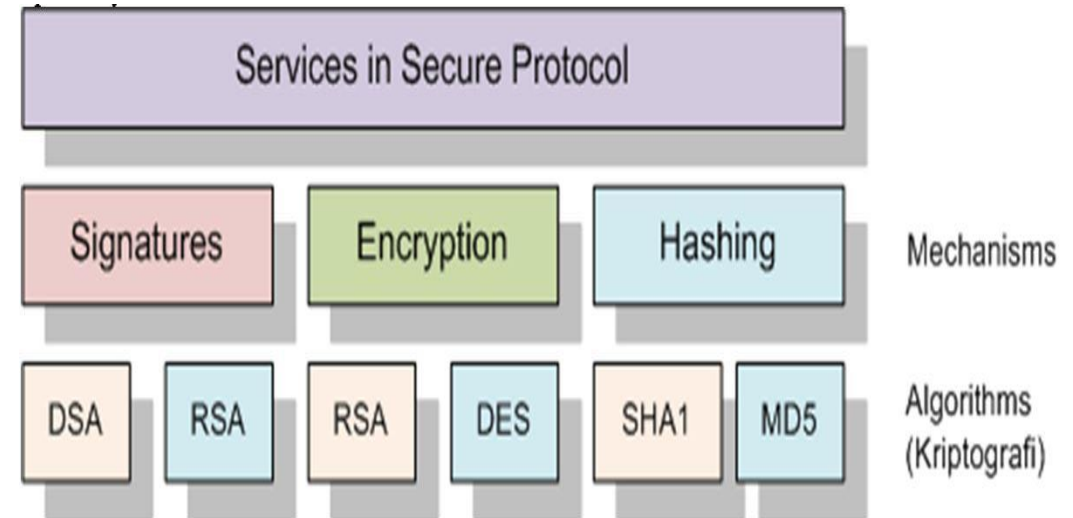
**Skema dalam struktur *information security***

# Hubungan Antar Layer

1. **Services** Kebutuhan/layanan keamanan (apa yang ingin dicapai).
2. **Mechanisms** Cara/mekanisme untuk mewujudkan layanan tersebut.
3. **Algorithms** Teknologi atau metode matematis yang digunakan dalam mekanisme.

Contoh alurnya:

- Jika ingin layanan **kerahasiaan** → butuh **encryption mechanism** → menggunakan algoritma seperti **RSA** atau **DES**.
- Jika ingin menjamin **integritas data** → gunakan **hashing mechanism** → dengan algoritma **SHA1** atau **MD5**.



**Skema dalam struktur *information security***

# Mekanisme Operasi

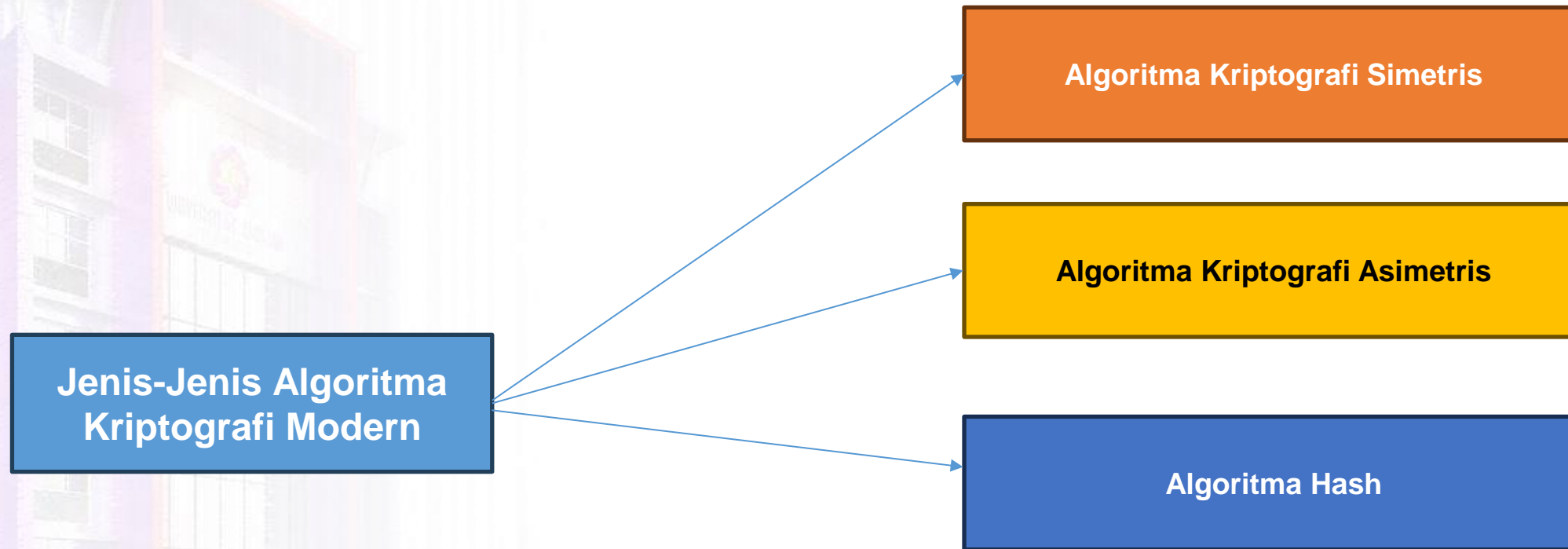
- Pengguna atau sistem meminta layanan keamanan (misalnya enkripsi untuk kerahasiaan).
- Sistem memilih mekanisme yang sesuai (misalnya encryption).
- Sistem menjalankan algoritma yang cocok untuk menghasilkan hasil yang aman (misalnya RSA untuk enkripsi dengan kunci publik).

## Kesimpulan

- **Layer Service** menjawab: apa yang ingin diamankan.
- **Layer Mechanism** menjawab: bagaimana cara mengamankan.
- **Layer Algorithm** menjawab: alat atau metode apa yang digunakan.

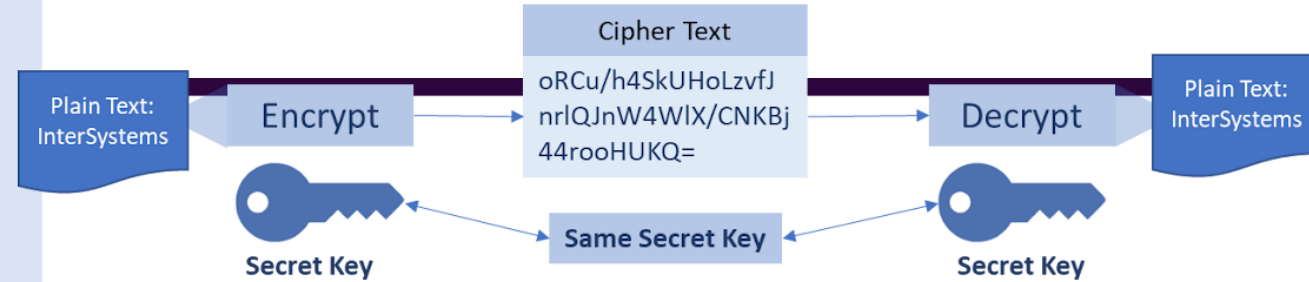


# Jenis-Jenis Algoritma Kriptografi Modern



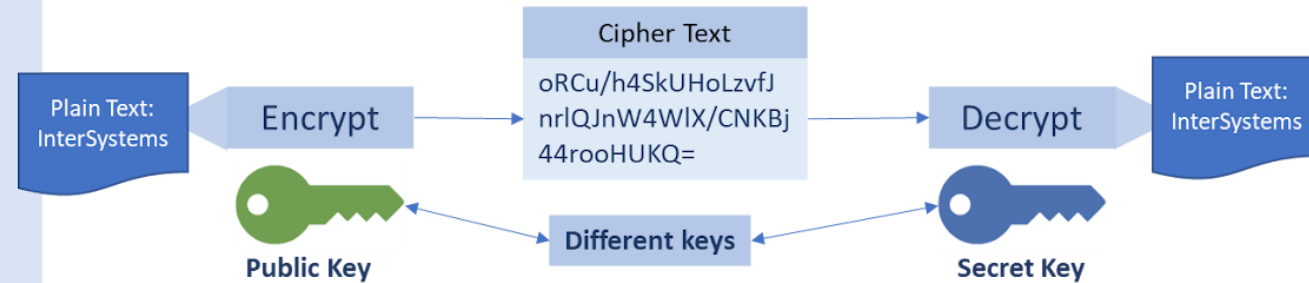
## Symmetric Keys

- **DES** – Embedded Python
- **TripleDES** – Embedded Python
- **AES** - %SYSTEM.Encryption -  
 AESCBCDecrypt(),  
 AESCBCDecryptStream(),  
 AESCBCEncrypt(),  
 AESCBCEncryptStream(),  
 AESCBCManagedKeyDecrypt(),  
 AESCBCManagedKeyDecryptStream(),  
 AESCBCManagedKeyEncrypt(),  
 AESCBCManagedKeyEncryptStream(),  
 AESGCMDecrypt(), AESGCMEncrypt()



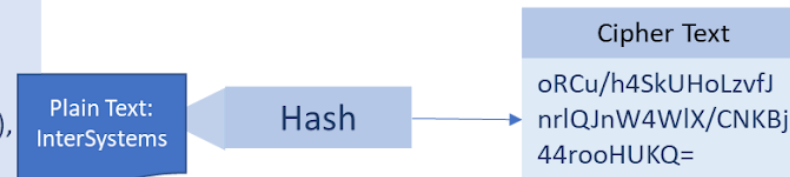
## Asymmetric Keys

- **Elliptic curves** - Embedded Python
- **RSA** - %SYSTEM.Encryption -  
 RSADecrypt(), RSAEncrypt()



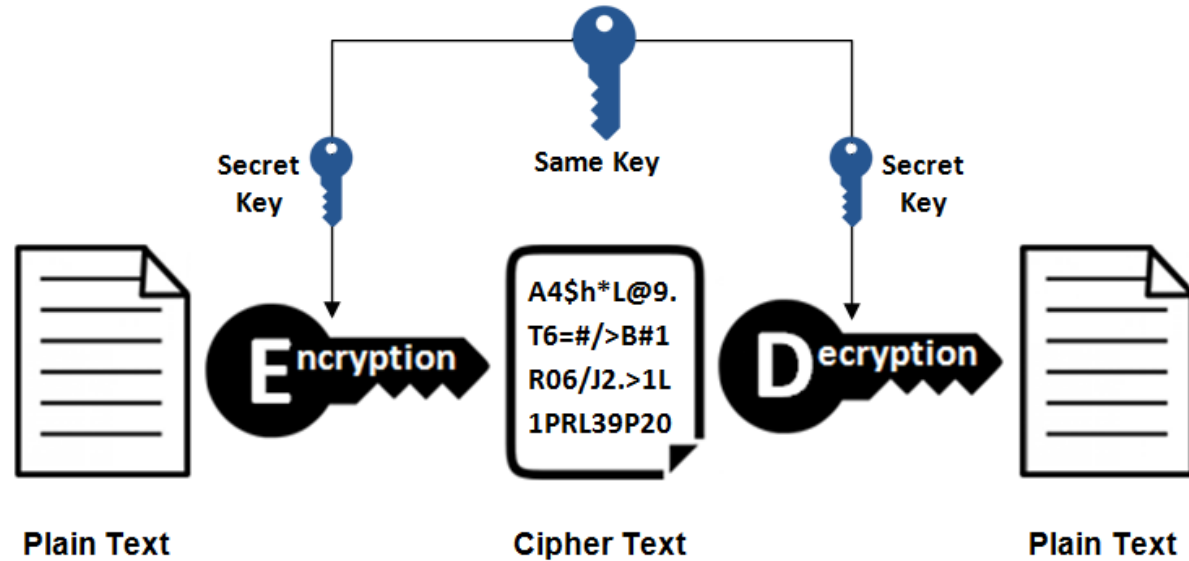
## One-Way Hash

- **MD5** - %SYSTEM.Encryption -  
 MD5Hash(), MD5HashStream()
- **SHA** - %SYSTEM.Encryption - SHAHash(),  
 SHAHashStream(), SHA1Hash(),  
 SHA1HashStream(), SHA3Hash(),  
 SHA3HashStream()

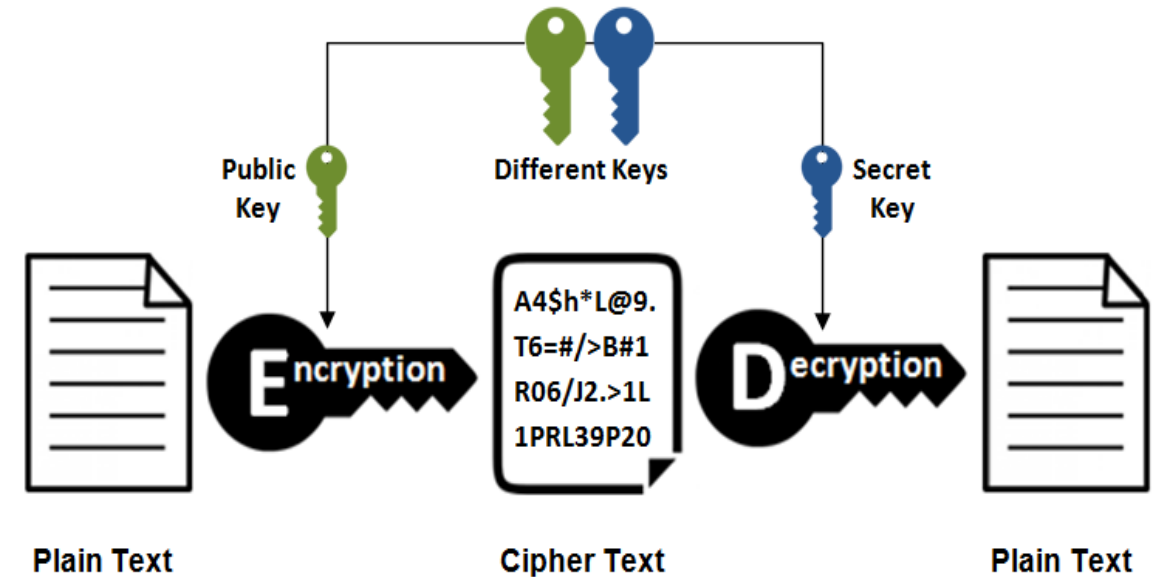


# Cara Kerja Enskripsi Simetrik dan Asimetrik

## Symmetric Encryption



## Asymmetric Encryption



- **Kunci Simetris** bagian yang menjalankan operasi enkripsi dan dekripsi berbagi kunci rahasia yang sama.
- **Kunci Asimetris** pihak yang melakukan operasi enkripsi dan dekripsi berbagi kunci rahasia yang sama untuk enkripsi. Namun, untuk dekripsi, masing-masing mitra memiliki kunci pribadi. Kunci ini tidak dapat dibagikan dengan orang lain, karena merupakan bukti identitas.
- **Hash** digunakan saat Anda tidak perlu mendekripsi, tetapi hanya mengenkripsi. Ini adalah pendekatan umum saat menyimpan kata sandi pengguna.

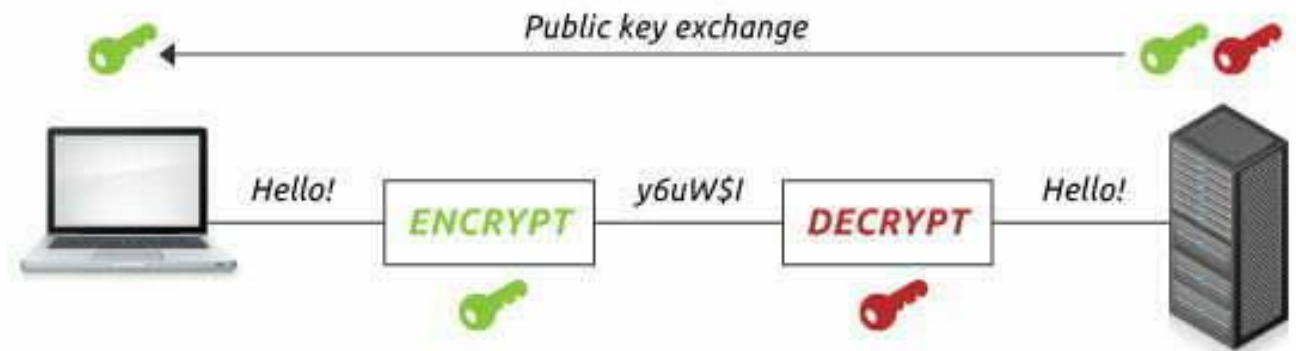


# Algoritma Kriptografi Simetris

## 1. Algoritma Kriptografi Simetris

Contoh: **DES, AES, RC4**

- Menggunakan **satu kunci** (shared/secret key) untuk enkripsi dan dekripsi.
- Cocok untuk data dalam jumlah besar karena cepat



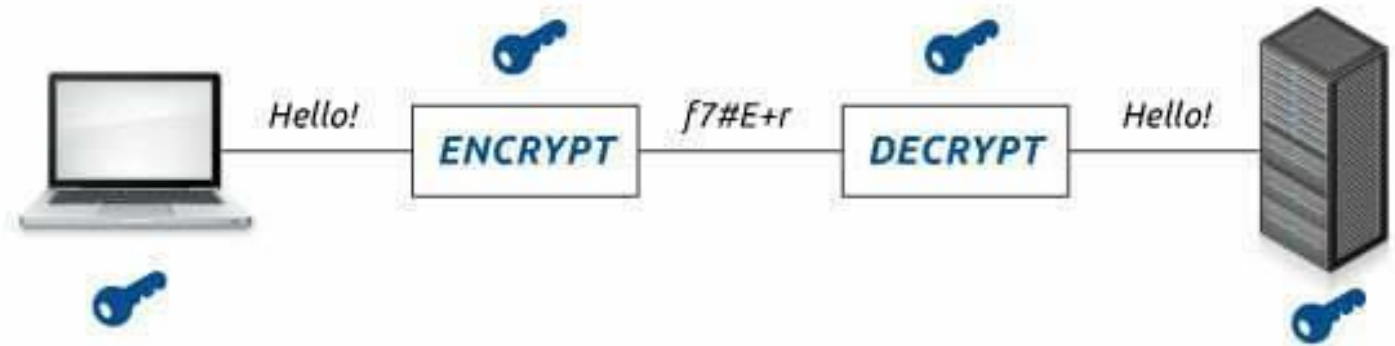
<https://pusatssl.com/order/knowledgebase/16/Enkripsi-Simetris-dan-Asimetris.html>

# Algoritma Kriptografi Simetris

## 2. Algoritma Kriptografi Asimetris

Contoh: RSA, ECC, DSA

- Menggunakan **dua kunci**: **kunci publik** untuk enkripsi, **kunci privat** untuk dekripsi.
- Cocok untuk pertukaran kunci dan tanda tangan digital.



<https://pusatssl.com/order/knowledgebase/16/Enkripsi-Simetris-dan-Asimetris.html>

# Algoritma Kriptografi Simetris

## 3. Algoritma Hash




Contoh: MD5, SHA1, SHA-256

- Tidak menggunakan kunci.
- Menghasilkan **nilai hash tetap** dari input (biasanya digunakan untuk verifikasi integritas data).






<https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/26-Fungsi-hash-SHA-2024.pdf>

# Perbandingan Berdasarkan Kecepatan Operasi (Real-Time System)

Jenis Algoritma	Kecepatan Operasi	Penjelasan
Simetris	 <b>Cepat</b>	Operasi matematis sederhana, cocok untuk enkripsi data besar secara real-time. Contoh: AES sangat cepat untuk streaming video.
Asimetris	 <b>Lambat</b>	Operasi eksponensial besar, tidak cocok untuk enkripsi data besar secara langsung, hanya cocok untuk otentikasi atau enkripsi kunci simetris.
Hash	 <b>Sangat cepat</b>	Hanya melakukan satu arah perhitungan hash, ideal untuk pengecekan integritas atau tanda tangan digital.



# Perbandingan Berdasarkan Jenis Kunci yang Digunakan

Jenis Algoritma	Jenis Kunci	Penjelasan
Simetris	 Satu kunci (sama untuk enkripsi dan dekripsi)	Masalah utama: distribusi kunci harus aman.
Asimetris	 Sepasang kunci (publik dan privat)	Publik dapat disebar, privat dijaga rahasia. Keamanan bergantung pada kesulitan faktorisasi bilangan besar atau logaritma diskret.
Hash	 Tidak menggunakan kunci	Hanya menghasilkan fingerprint, tidak bisa digunakan untuk dekripsi.



Perbedaan Utama	Enkripsi Simetris	Enkripsi Asimetris
Ukuran teks sandi	Teks sandi yang lebih kecil daripada berkas teks biasa asli.	Teks sandi yang lebih besar daripada berkas teks biasa asli.
Ukuran data	Digunakan untuk mengirimkan data besar. Digunakan untuk mengirimkan data kecil.	
Pemanfaatan Sumber Daya	Enkripsi kunci simetris berfungsi pada penggunaan sumber daya yang rendah. Enkripsi asimetris memerlukan konsumsi sumber daya yang tinggi.	
Panjang Kunci	Ukuran kunci 128 atau 256-bit.	Ukuran kunci RSA 2048-bit atau lebih tinggi.
Keamanan	Kurang aman karena penggunaan kunci tunggal untuk enkripsi.	Jauh lebih aman karena dua kunci berbeda terlibat dalam enkripsi dan dekripsi.

Perbedaan Utama	Enkripsi Simetris	Enkripsi Asimetris
Jumlah kunci	Enkripsi Simetris menggunakan satu kunci untuk enkripsi dan dekripsi.	Enkripsi Asimetris menggunakan dua kunci berbeda untuk enkripsi dan dekripsi
Teknik	Itu adalah teknik lama.	Ini adalah teknik modern.
Kerahasiaan	Satu kunci tunggal untuk enkripsi dan dekripsi memiliki risiko kunci tersebut dibobol.	Dua kunci dibuat secara terpisah untuk enkripsi dan dekripsi yang menghilangkan kebutuhan untuk berbagi kunci.
Kecepatan	Enkripsi simetris adalah teknik yang cepat	Enkripsi asimetris lebih lambat dalam hal kecepatan.
Algoritma	RC4, AES, DES, 3DES, dan QUAD.	Algoritma RSA, Diffie-Hellman, ECC.

# Contoh: Pemulihan dan Pencegahan Insiden Keamanan Informasi Situs Pemerintah

Situs pemerintah yang dikelola oleh pihak ketiga disusupi **malware** jenis **Remote Access Trojan (RAT)**, yang disebarkan dalam empat tahapan serangan:

1. **Survey Attack** Pengintaian sistem.
2. **Delivery Attack** Penyebaran malware (500 komputer terinfeksi).
3. **Breach Attack** Eksploitasi kerentanan.
4. **Affect Attack** Perusakan sistem internal.



# Penjelasan 5 Aktivitas Pemulihan & Kendali Keamanan

Aktivitas	Definisi	Penjelasan
<b>Patching</b>	Proses memperbarui perangkat lunak dengan perbaikan keamanan atau bug.	Mencegah eksploitasi celah keamanan yang dikenal oleh attacker.
<b>Network Perimeter Defences</b>	Strategi untuk melindungi jaringan dari akses luar yang tidak sah.	Meliputi firewall, IDS/IPS, dan segmentasi jaringan.
<b>Malware Protection</b>	Sistem untuk mendeteksi, memblokir, dan menghapus perangkat lunak berbahaya.	Termasuk antivirus, anti-malware, dan endpoint protection.
<b>Security Monitoring</b>	Pemantauan aktif terhadap sistem untuk mendeteksi aktivitas mencurigakan.	Menggunakan SIEM (Security Info and Event Management) dan log monitoring.
<b>Whitelisting &amp; Execution Control</b>	Pengaturan agar hanya aplikasi tertentu yang diperbolehkan berjalan.	Menghindari eksekusi malware atau software yang tidak sah.

# Aktivitas Mitigasi Risiko di Masa Depan

Aktivitas Tambahan	Penjelasan
Audit Keamanan Berkala	Penilaian kerentanan dan kepatuhan terhadap standar keamanan.
Pelatihan Keamanan Siber	Edukasi staf IT dan user tentang ancaman dan praktik aman.
Backup & Recovery Strategy	Sistem pencadangan yang rutin dan teruji untuk pemulihan cepat.
Vendor Risk Management	Evaluasi dan pengawasan keamanan pada penyedia jasa pihak ketiga.
Zero Trust Architecture	Pendekatan keamanan di mana tidak ada entitas yang dipercaya secara default.

# Quotes

## Filosofi Semut

*Dalam Kehidupan*

### istana megah

"dengan kejeniusannya, merancang tempat tinggalnya, yang mampu mengantisipasi panas, hujan dan anti longsor. memiliki ruangan-ruangan khusus dengan fungsi yang berbeda-beda layaknya istana"

### jembatan cinta

"jembatan hidup dibangun dengan kesabaran, toleransi, pengorbanan, cinta dan kasih sayang untuk mencapai tujuan bersama"

### pantang menyerah

"tidak akan mundur dalam keadaan apapun"

*-Pesan Moral -*

Kita tidak boleh kalah oleh **masalah**, karena sesungguhnya masalah di ciptakan **untuk dikalahkan.**



Human, Organisational and Regulatory Aspects	
Risk Management & Governance	Security management systems and organisational security controls, including standards, best practices, and approaches to risk assessment and mitigation.
Law & Regulation	International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare.
Human Factors	Usable security, social & behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours.
Privacy & Online Rights	Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems.
Attacks and Defences	
Malware & Attack Technologies	Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches.
Adversarial Behaviours	The motivations, behaviours, & methods used by attackers, including malware supply chains, attack vectors, and money transfers.
Security Operations & Incident Management	The configuration, operation and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence.
Forensics	The collection, analysis, & reporting of digital evidence in support of incidents or criminal events.
Systems Security	
Cryptography	Core primitives of cryptography as presently practised & emerging algorithms, techniques for analysis of these, and the protocols that use them.
Operating Systems & Virtualisation Security	Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualisation, and security in database systems.
Distributed Systems Security	Security mechanisms relating to larger-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multitenant data centres, & distributed ledgers.
Formal Methods for Security	Formal specification, modelling and reasoning about the security of systems, software and protocols, covering the fundamental approaches, techniques and tool support.
Authentication, Authorisation & Accountability	All aspects of identity management and authentication technologies, and architectures and tools to support authorisation and accountability in both isolated and distributed systems.



# TUGAS

<b>Software and Platform Security</b>	
Software Security	Known categories of programming errors resulting in security bugs, & techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems.
Web & Mobile Security	Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models.
Secure Software Lifecycle	The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default.
<b>Infrastructure Security</b>	
Applied Cryptography	The application of cryptographic algorithms, schemes, and protocols, including issues around implementation, key management, and their use within protocols and systems.
Network Security	Security aspects of networking & telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security.
Hardware Security	Security in the design, implementation, & deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness.
Cyber-Physical Systems Security	Security challenges in cyber-physical systems, such as the Internet of Things & industrial control systems, attacker models, safe-secure designs, and security of large-scale infrastructures.
Physical Layer & Telecommunications Security	Security concerns and limitations of the physical layer including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference.

Any Questions..?

---

*Thank  
you!*



UNIVERSITAS  
**AMIKOM**  
YOGYAKARTA

