CALVIN
INSTITUTE OF TECHNOLOGY
God's People for God's Glory

Keamanan dan Pengelolaan Data

Minggu 1

Dosen Pengajar: Steven Bandong S.Si., M.T

Tata Tertib Kelas

- Dosen dan mahasiswa bersama-sama secara aktif membentuk komunitas belajar yang baik
- Silahkan bertanya kalau ada yang tidak dimengerti
- Laporan / program / tugas apa pun yang anda serahkan harus jelas beda dan jelas adalah kontribusi anda atau kelompok dan bukan dari orang lain (misnya: tugas proyek).

Confidential. Not to be copied / distributed

Topik Minggu Ini dan Capaian Pembelajaran

Topik minggu ini:

1. Menjelaskan lima tujuan utama keamanan.
2. Menjelaskan penggunaan utama kriptografi.
3. Menguraikan empat jenis algoritma kriptografi.
4. Memahami konsep infrastruktur kunci publik.

Indikator penilaian:

1. Ketepatan dalam menjelaskan lima tujuan utama keamanan
2. Ketepatan dalam menjelaskan penggunaan utama kriptografi.
3. Ketepatan dalam menjelaskan empat jenis algoritma kriptografi
4. Ketepatan dalam menjelaskan infrastruktur kunci publik

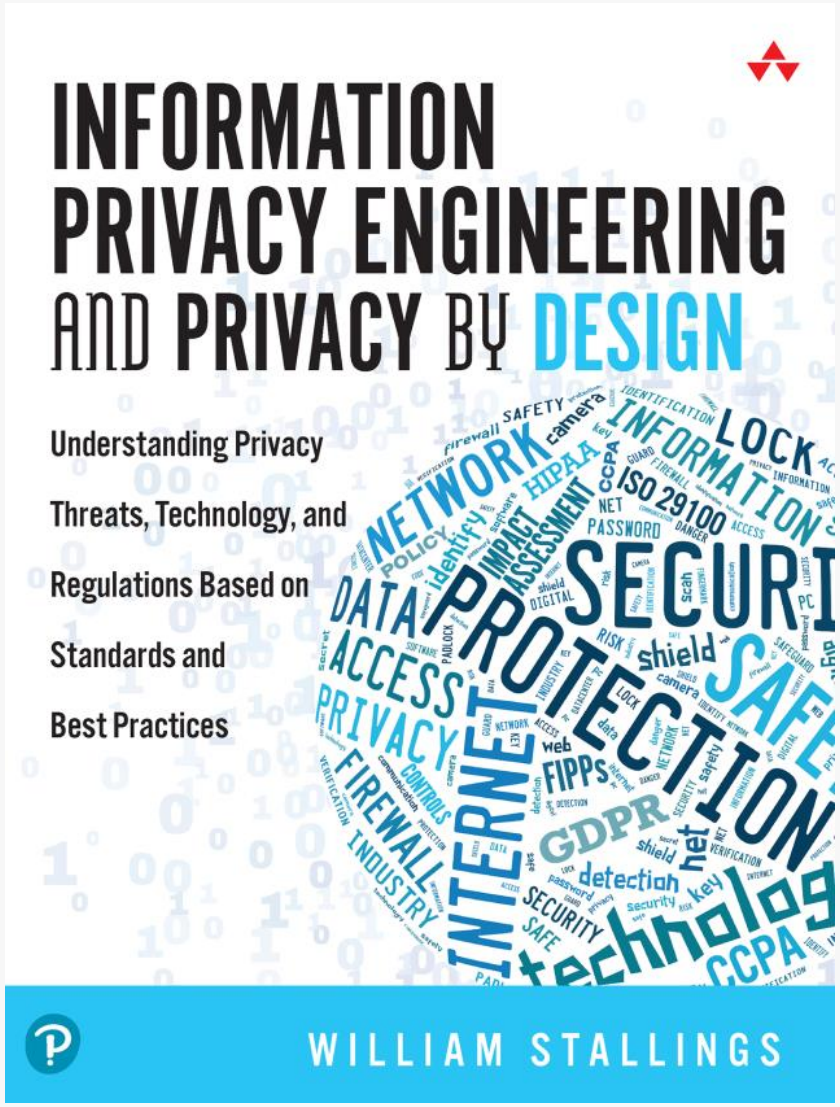
Confidential. Not to be copied / distributed

Data Governance and Security

Modul ini disusun dalam konteks masyarakat saat ini dan organisasi di dalamnya. Perilaku sosial, yang sering kali terjadi di lingkungan virtual, menciptakan berbagai masalah etika yang berpusat pada keamanan informasi dan tata kelola. Selain mengeksplorasi isu-isu sosial dan etika ini, kerangka hukum dan peraturan yang telah dikembangkan dalam beberapa tahun terakhir untuk mencoba menangani masalah-masalah ini juga akan dibahas. Anda juga akan mempelajari tentang keamanan dalam organisasi serta diperkenalkan pada berbagai ancaman umum dan langkah penanggulangannya.
-Northumbria University Newcastle

Di era big data, keamanan dan tata kelola menjadi prioritas utama bagi bisnis. Bisnis memiliki kewajiban etis dan hukum untuk melindungi data pelanggan mereka serta mengelola data internal mereka sendiri. Hal ini menjadikan pemahaman dan pengembangan kebijakan serta prosedur keamanan data dan tata kelola data sebagai prioritas utama. Unit ini memperkenalkan mahasiswa pada praktik terkini dan regulasi pemerintah terkait keamanan data, kerangka kerja tata kelola data, serta isu etika yang berhubungan dengan pembuatan, pengelolaan, dan distribusi data.
-Victoria University Melbourne Australia

Data Governance and Security



Cybersecurity

"Cybersecurity is the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

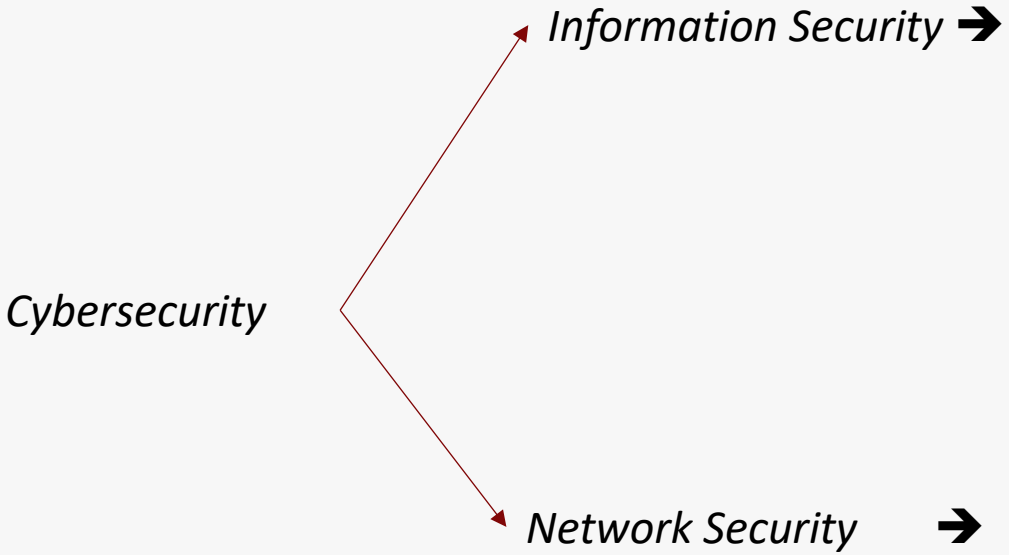
- NISTIR
(Small Business Information Security: The Fundamentals, 2016)

Cybersecurity

“Cybersecurity adalah pencegahan kerusakan, penggunaan tanpa izin, eksploitasi, dan—jika diperlukan—pemulihan sistem informasi elektronik dan komunikasi, layanan komunikasi elektronik, komunikasi kabel, serta komunikasi elektronik, termasuk informasi yang terdapat di dalamnya, untuk memastikan ketersediaan, integritas, autentikasi, kerahasiaan, dan non-repudiation (tidak dapat disangkal)..“

- NISTIR
(Small Business Information Security: The Fundamentals, 2016)

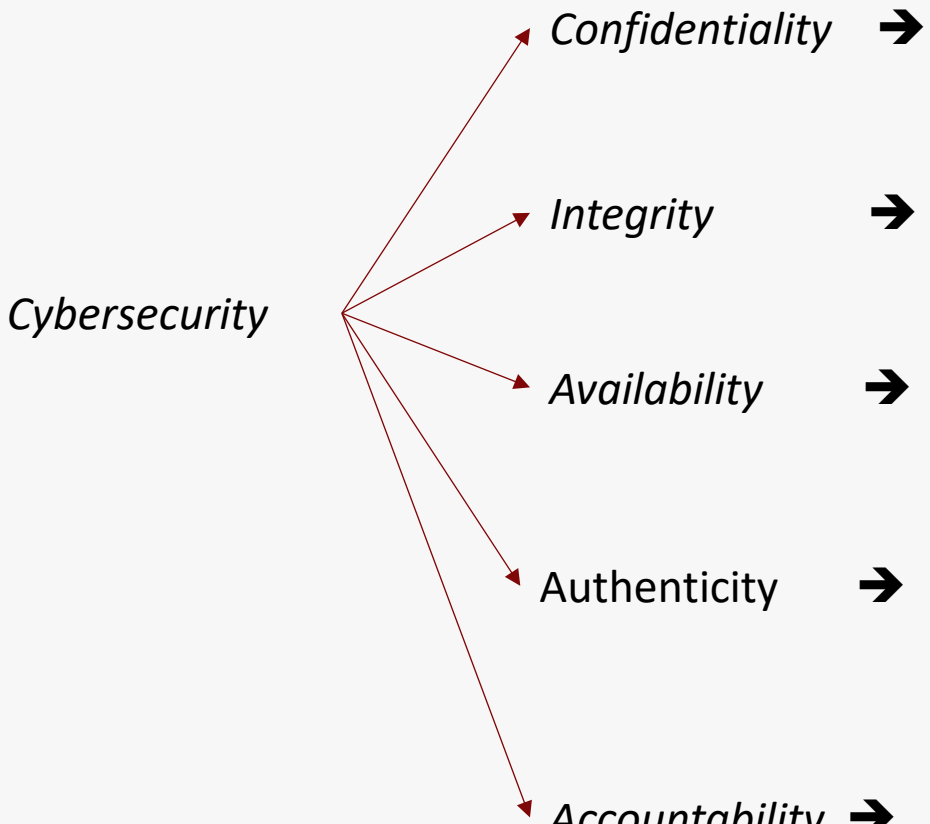
Cybersecurity



Melindungi kerahasiaan, integritas, dan ketersediaan informasi. Termasuk autentikasi, akuntabilitas, non-repudiation, dan keandalan.

Melindungi jaringan dari akses tidak sah dan memastikan fungsi berjalan dengan baik.

Tujuan Utama Cybersecurity



Menjaga kerahasiaan informasi dari akses atau pengungkapan yang tidak sah

Data Integrity: Memastikan data hanya dimodifikasi oleh pihak yang berwenang.
System Integrity: Memastikan sistem berfungsi tanpa manipulasi yang tidak sah

Memastikan informasi dan layanan tersedia untuk pengguna yang berwenang tanpa gangguan.

Menjamin bahwa data dan pengguna dapat diverifikasi sebagai asli dan dapat dipercaya

Memastikan setiap tindakan dapat dilacak ke entitas yang bertanggung jawab, mendukung non-repudiation dan analisis forensik jika terjadi pelanggaran.

Tujuan Utama Cybersecurity

Essential Information and Network Security Objectives

Diskusi

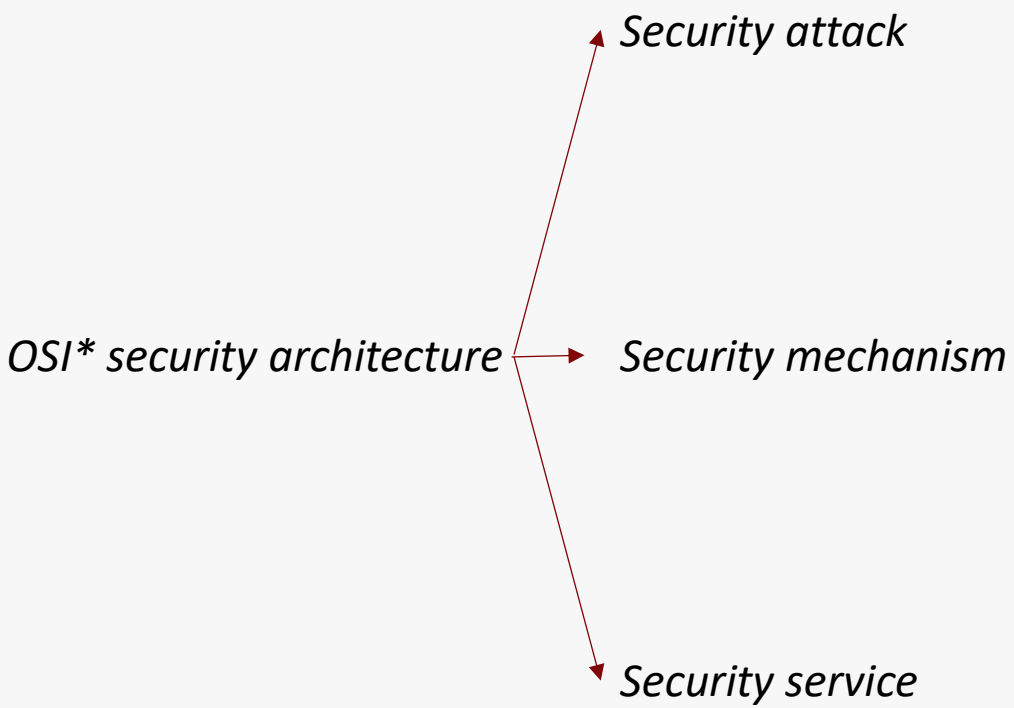
Banyak pengguna dan administrator keamanan melihat langkah-langkah keamanan yang terlalu ketat dan kompleks sebagai hambatan bagi efisiensi dan kemudahan penggunaan. Bagaimana cara mencapai keseimbangan antara keamanan yang ketat dan kemudahan operasional?

Penyerang hanya perlu menemukan satu kelemahan sementara desainer harus menghilangkan semua kelemahan, apakah ada pendekatan strategis untuk menyeimbangkan pertempuran ini? Apakah 100% keamanan realistis?

Mengapa banyak pengguna dan manajer sistem hanya menyadari pentingnya investasi dalam keamanan setelah terjadi kegagalan keamanan? Bagaimana pendekatan yang dapat digunakan untuk meningkatkan kesadaran mereka sebelum insiden terjadi?

Bagaimana organisasi dapat menyeimbangkan kebutuhan keamanan jangka panjang dengan tekanan untuk memenuhi kebutuhan operasional jangka pendek? Apakah ada prioritas yang harus didahulukan?

Security Attacks



Segala tindakan yang mengkompromikan keamanan informasi milik organisasi.

Sebuah proses (atau perangkat yang mengintegrasikan proses tersebut) yang dirancang untuk mendeteksi, mencegah, atau memulihkan dari serangan keamanan.

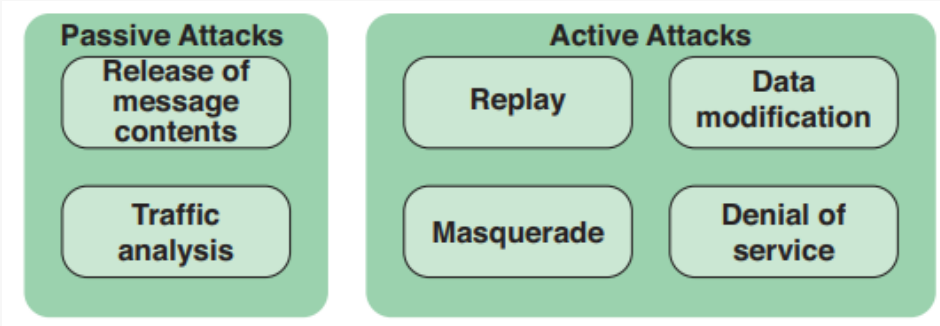
Layanan pemrosesan atau komunikasi yang meningkatkan keamanan sistem pemrosesan data dan transfer informasi, menggunakan mekanisme keamanan untuk menangkal serangan keamanan.

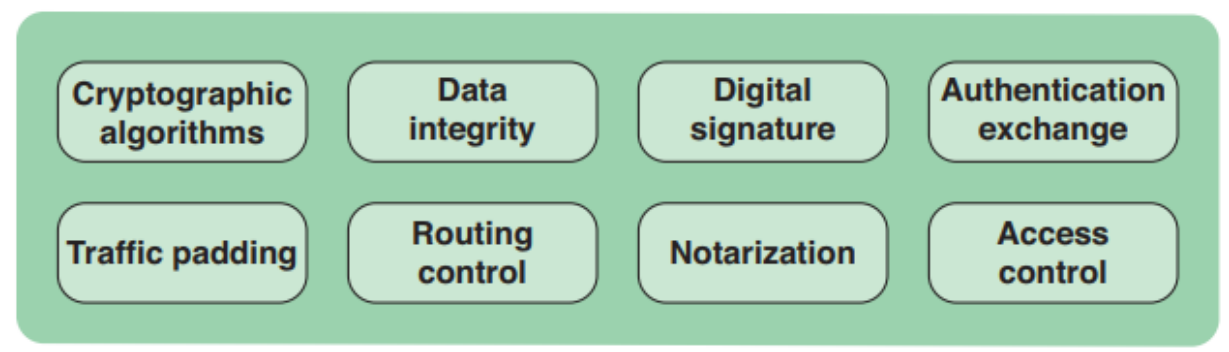
*Security Architecture for Open Systems Interconnection [OSI]

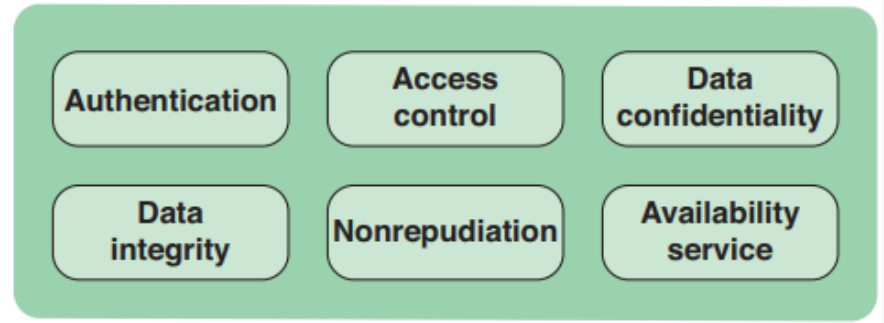
Security Attacks

OSI security architecture*

- *Security attack*
- *Security mechanism*
- *Security service*







*Security Architecture for Open Systems Interconnection [OSI]

Passive Attacks

Jenis serangan yang melibatkan penyadapan atau pemantauan transmisi dengan tujuan memperoleh informasi tanpa mengubah data

Release of Message Contents

Penyadapan komunikasi, seperti percakapan telepon, pesan email, atau file yang ditransfer

Traffic Analysis

Observasi pola lalu lintas data tanpa mengakses kontennya, seperti frekuensi, lokasi, dan panjang pesan, untuk menebak sifat komunikasi.

- Sulit dideteksi karena tidak mengubah data.
- Pencegahan lebih efektif daripada deteksi, sering menggunakan enkripsi untuk melindungi konten dan pola komunikasi

Edward Snowden was NSA Prism leak source - Guardian

10 June 2013 · 1404 Comments

https://www.bbc.com/news/world-us-canada-22836378?filter=none

Ed Snowden explains why he became a whistleblower (Video courtesy of The Guardian, Glenn Greenwald and Laura Poitras)

A former CIA technical worker has been identified by the UK's Guardian newspaper as the source of leaks about US surveillance programmes.

Edward Snowden, 29, **is described by the paper** as an ex-CIA technical assistant, currently employed by defence contractor Booz Allen Hamilton.

The Guardian said his identity was being revealed at his own request.

The recent revelations are that US agencies gathered millions of phone

Facebook data scandal: Social network fined $5bn over 'inappropriate' sharing of users' personal information

Federal Trade Commission investigated allegations company shared information with Cambridge Analytica

Adam Forrest • Friday 12 July 2019 21:48 BST • Comments

The Facebook logo is displayed during the F8 Facebook Developers conference on April 30, 2019 in San Jose, California *(Justin Sullivan/Getty Images)*

The latest headlines from our reporters across the US sent straight to your inbox each weekday

Email

SIGN UP

I would like to be emailed about offers, events and updates from The Independent. Read our privacy policy

The US Federal Trade Commission (FTC) has approved a roughly $5bn (£4bn) settlement with Facebook over its investigation into the social media company's handling of user data, according to reports.

The FTC has been investigating allegations Facebook inappropriately shared information belonging to 87 million users with the now-defunct British political consulting firm Cambridge Analytica.

The probe has focused on whether the sharing of data and other disputes violated a 2011 consent agreement between Facebook and the agency

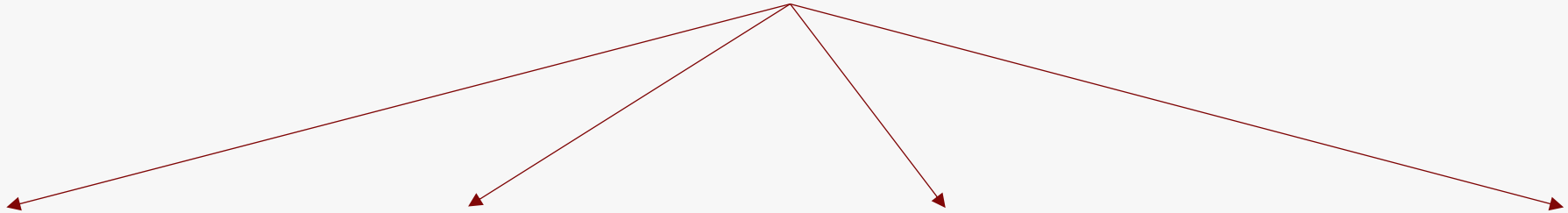
Join The Independent's free WhatsApp Channel

Breaking news updates, daily headlines and more

https://www.independent.co.uk/news/world/americas/facebook-data-privacy-scandal-settlement-cambridge-analytica-court-a9003106.html

Active Attacks

Jenis serangan yang melibatkan modifikasi data atau pembuatan data palsu untuk merusak sistem



Masquerade

Penyerang berpura-pura menjadi entitas lain untuk mendapatkan akses yang tidak sah. Contohnya penyerang menyamar sebagai klien ke server atau sebaliknya.

Replay

Penyerang mengambil data lalu mengirimnya ulang untuk membuat efek tidak sah, tanpa mengganggu aliran informasi asli.

Data Modification

Sebagian data sah diubah, ditunda, atau disusun ulang untuk menghasilkan efek tidak sah

Denial-of-Service (DoS)

Penyerang mencegah akses normal ke layanan dengan: 1)Membanjiri server dengan lalu lintas data. 2)Mengonsumsi sumber daya komputasi secara besar-besaran.

- Berbeda dengan serangan pasif, serangan aktif sulit dicegah sepenuhnya
- Fokus pencegahan adalah pada deteksi dini dan pemulihan dari gangguan atau keterlambatan.

Topics Spotlight: Building a Winning Team Ev

What is Stuxnet?

Stuxnet is a powerful computer worm designed by U.S. and Israeli intelligence that to disable a key part of the Iranian nuclear program. Targeted at an air-gapped facility, it unexpectedly spread to outside computer systems, raising a number of questions about its design and purpose.

Stuxnet exploited multiple previously unknown Windows **zero days**. That description should probably make it clear that Stuxnet was a part of a high-level sabotage operation waged by nation-states against their adversaries.

https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html?utm_source=chatgpt.com

Who created Stuxnet?

It's now widely accepted that Stuxnet was created by the intelligence agencies of the United States and Israel. Stuxnet was first identified by the infosec community in 2010, but development on it probably began in 2005. The U.S. and Israeli governments intended Stuxnet as a tool to **derail, or at least delay, the Iranian program to develop nuclear weapons**. The Bush and Obama administrations believed that if Iran were on the verge of developing atomic weapons, Israel would launch airstrikes against Iranian nuclear facilities in a move that could have set off a regional war. Operation Olympic Games was seen as a nonviolent alternative.

Stuxnet

computer worm

https://www.britannica.com/technology/Stuxnet

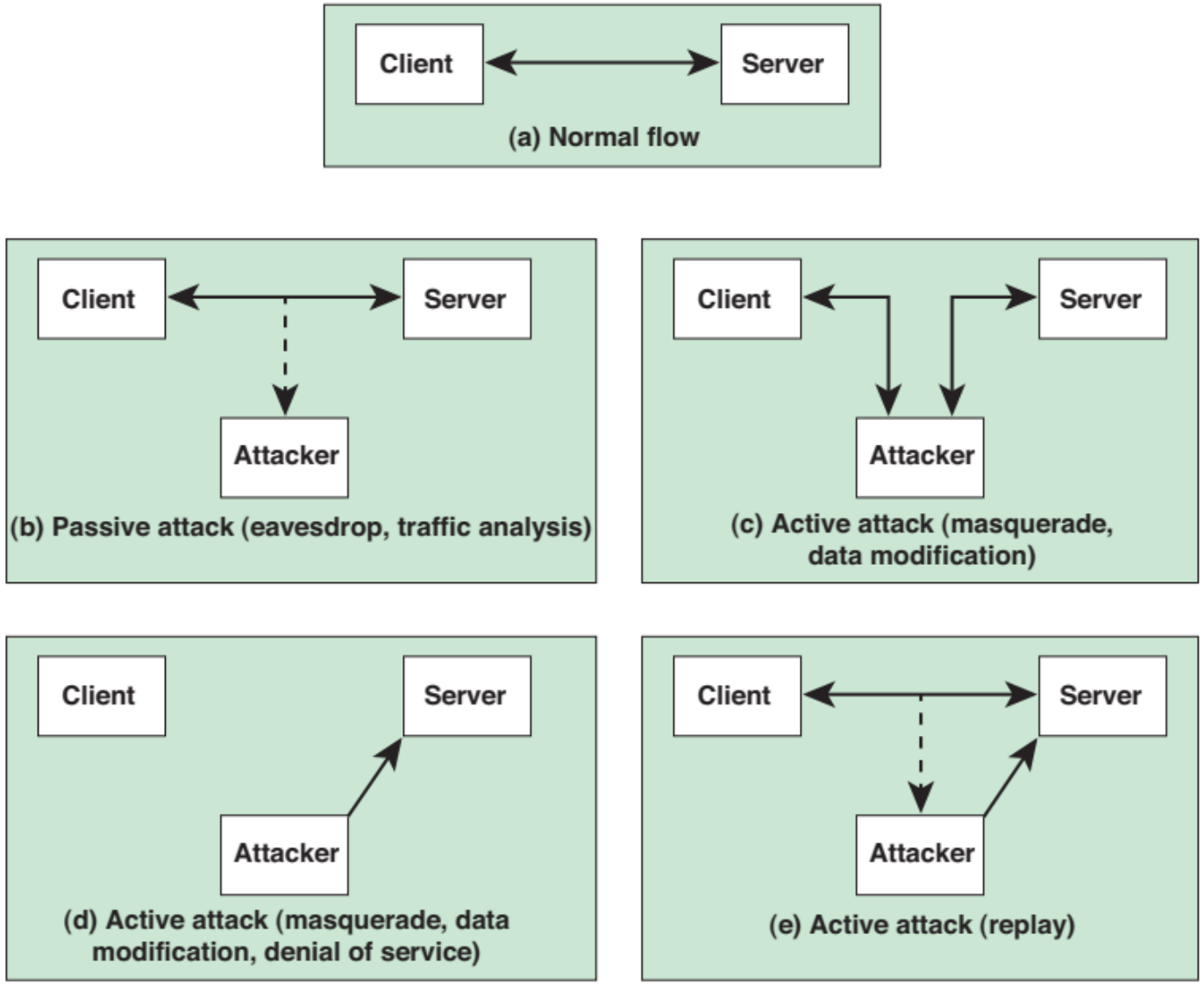
Ask the Chatbot a Question More Actions

Written and fact-checked by The Editors of Encyclopaedia Britannica
Last Updated: Dec 20, 2024 • Article History

Stuxnet, a computer worm, discovered in June 2010, that was specifically written to take over certain programmable industrial control systems and cause the equipment run by those systems to malfunction, all the while feeding false data to the systems monitors indicating the equipment to be running as intended.

As analyzed by computer security experts around the world, Stuxnet targeted certain "supervisory control and data acquisition" (SCADA) systems manufactured by the German electrical company Siemens AG that control machinery employed in power plants and similar installations. More specifically, the worm targeted only Siemens SCADA systems that were used in conjunction with frequency-converter drives, device

Security Attacks



Security Services

kemampuan yang mendukung satu atau lebih persyaratan keamanan (kerahasiaan, integritas, ketersediaan, autentikasi, dan akuntabilitas). Layanan ini menerapkan kebijakan keamanan melalui mekanisme keamanan (Security mechanism)

Service	Description
Authentication	A person's identity is determined before access is granted.
Access Control	Persons are allowed or denied access to resources for specific purposes.
Data Confidentiality	Information is only available to persons intended to use or see it.
Data Integrity	Information is modified only in appropriate ways by persons authorized to change it.
Nonrepudiation	A person cannot perform an action and then later deny performing the action.
Availability	Apps, services, and hardware are ready when needed and perform acceptably.

Security Mechanisms

Cryptographic Algorithms
Menggunakan algoritma untuk memastikan kerahasiaan dan keamanan data.

Data Integrity
Menjamin keutuhan data melalui mekanisme yang mencegah perubahan tidak sah.

Digital Signature
Menggunakan data kriptografis untuk memverifikasi sumber dan keutuhan data serta melindungi dari pemalsuan.

Authentication Exchange
Memastikan identitas entitas melalui pertukaran informasi.

Traffic Padding
Menambahkan bit pada aliran data untuk mencegah analisis lalu lintas.

Routing Control
Memilih rute data yang aman secara fisik atau logis, dengan kemampuan mengubah rute jika ada ancaman keamanan

Notarization
Melibatkan pihak ketiga terpercaya untuk memastikan sifat tertentu dari pertukaran data.

Access Control
Menegakkan hak akses terhadap sumber daya dengan berbagai mekanisme.

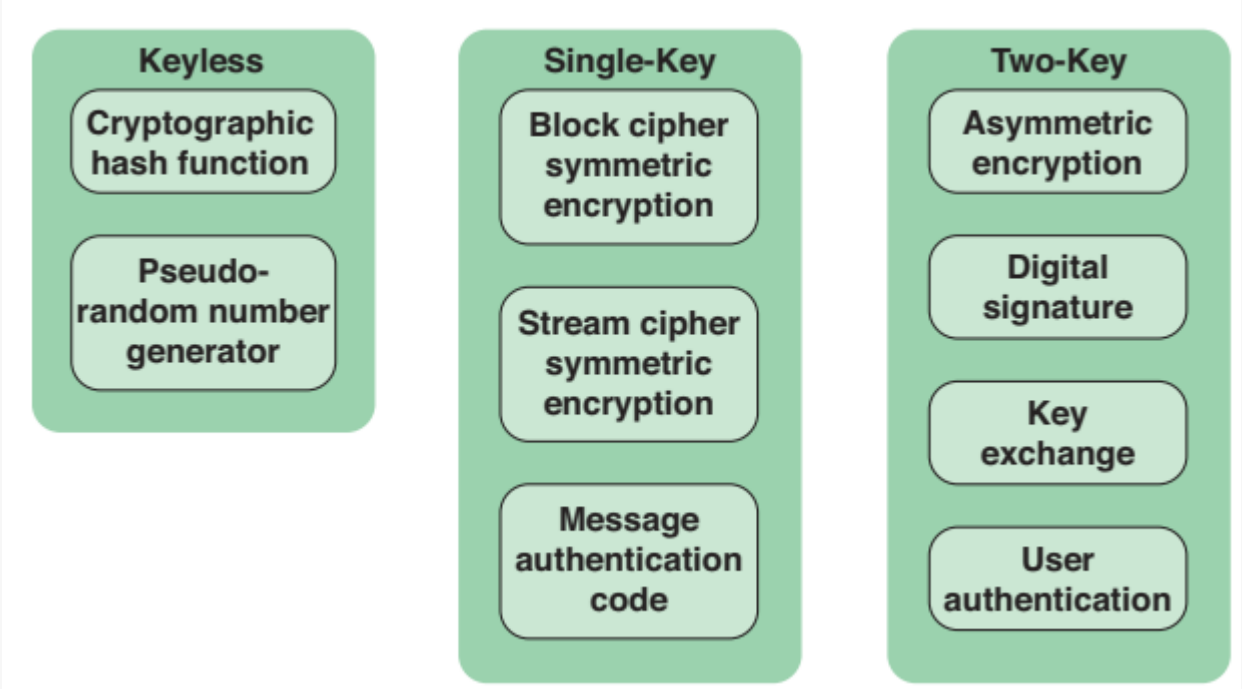
Confidential. Not to be copied / distributed

Cryptographic Algorithms

Disiplin yang mencakup prinsip, metode, dan cara untuk mengubah data agar menyembunyikan isi semantiknya, mencegah penggunaan yang tidak sah, atau modifikasi yang tidak terdeteksi.
(Service: kerahasiaan, integritas data, non-repudiation, dan autentikasi)

Sering menggunakan kunci kriptografi untuk menghasilkan keluaran berdasarkan data masukan

- Keyless: Tidak menggunakan kunci untuk transformasi kriptografi.
- Single-Key (Symmetric): Menggunakan satu kunci rahasia untuk proses enkripsi dan dekripsi.
- Two-Key (Asymmetric): Menggunakan dua kunci berbeda namun saling terkait, yaitu kunci privat dan kunci publik.



Confidential. Not to be copied / distributed

Cryptographic Algorithms

Keyless Algorithms

Menggunakan fungsi deterministik tanpa kunci untuk transformasi kriptografi.
Contoh:
Cryptographic Hash Function: Mengubah teks menjadi nilai tetap (hash value) untuk autentikasi pesan atau tanda tangan digital.
Pseudorandom Number Generator: Membuat urutan angka atau bit yang tampak acak untuk tujuan kriptografi.

Single-Key Algorithms (Symmetric Encryption)

Menggunakan satu kunci rahasia yang digunakan untuk enkripsi dan dekripsi.
Contoh:
Message Authentication Code (MAC): Menggunakan kunci rahasia dan fungsi hash untuk menjamin integritas pesan. Penerima dapat memverifikasi pesan dengan menghitung ulang MAC.

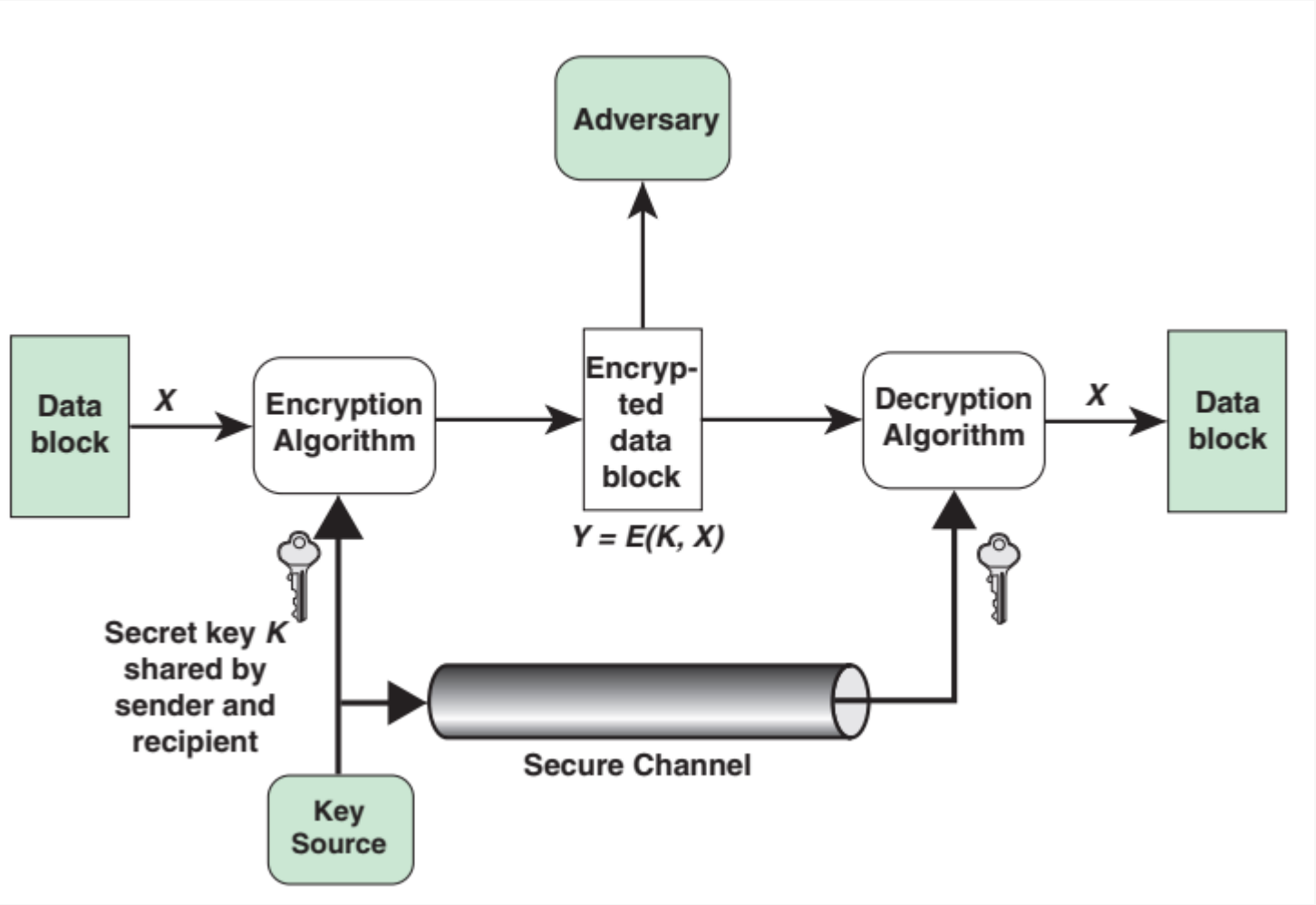
Two-Key Algorithms (Asymmetric Encryption)

Menggunakan dua kunci berbeda tetapi saling terkait:
Private Key: Hanya diketahui oleh pengguna tertentu.
Public Key: Diketahui oleh banyak pihak.

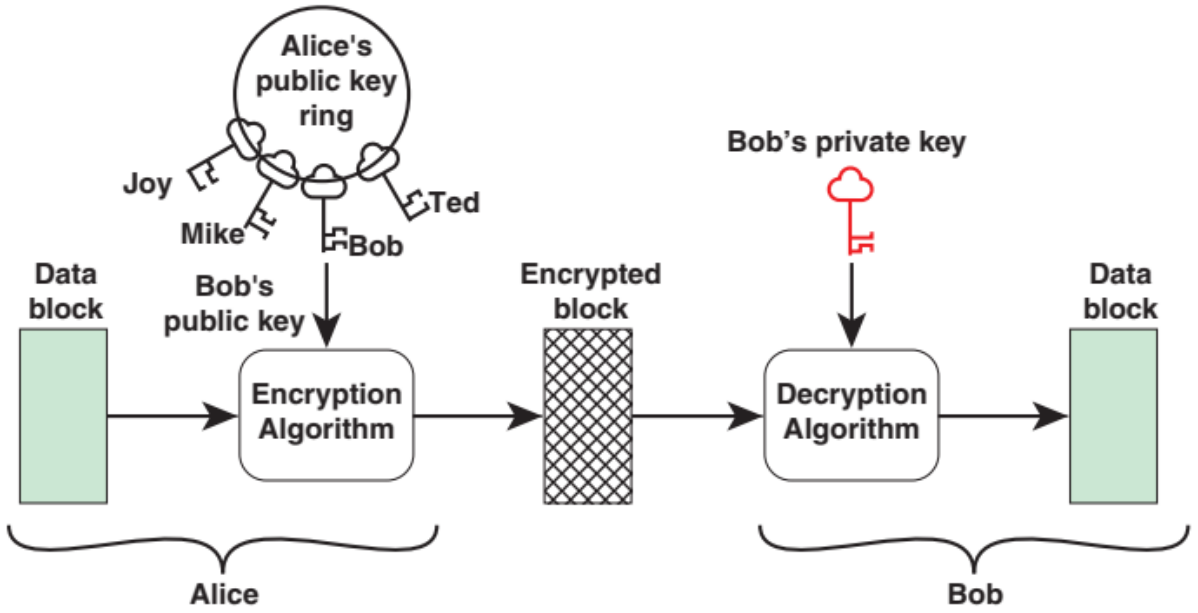
Cara Kerja:Data yang dienkripsi dengan private key dapat didekripsi dengan public key, dan sebaliknya.
Contoh:
User Authentication: Memastikan identitas pengguna dengan menggunakan kunci asimetris.

Confidential. Not to be copied / distributed

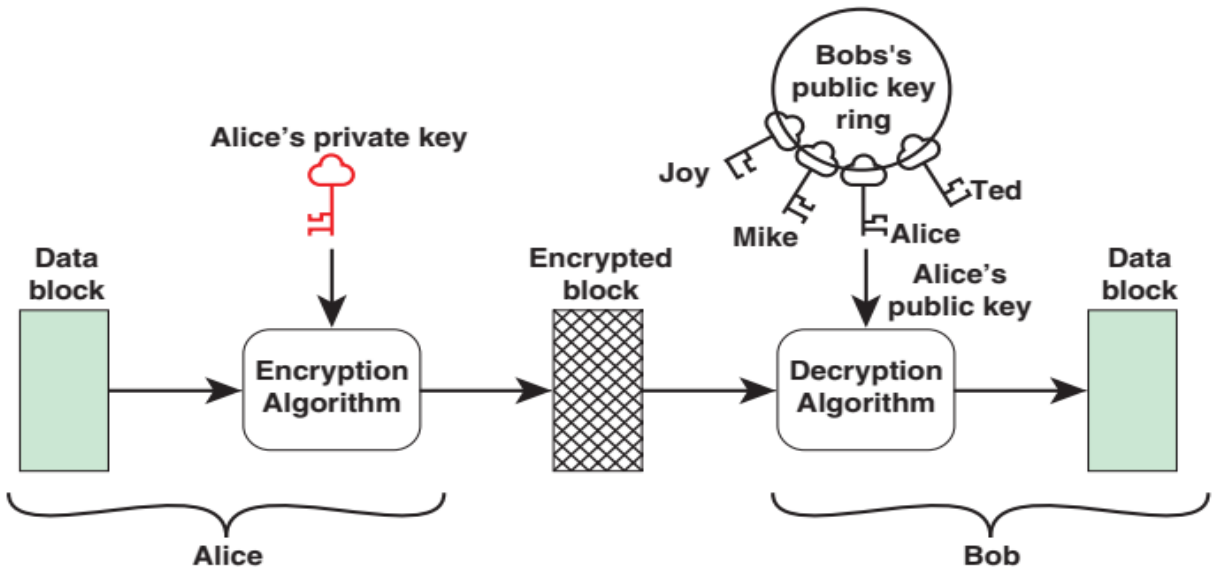
Symmetric Encryption



Asymmetric Encryption



(a) Public-key encryption/decryption (Alice encrypts block for Bob only)



(b) Public-key encryption/decryption (Alice authenticates block for any recipient)

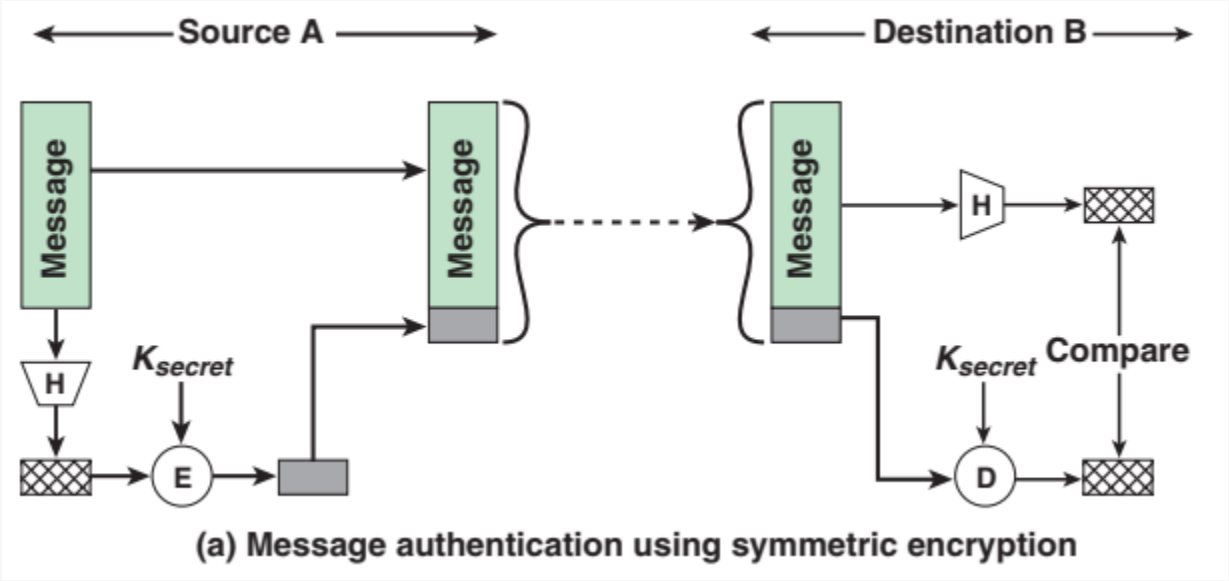
Confidential. Not to be copied / distributed

Symmetric and Asymmetric Encryption

Symmetric Encryption	Asymmetric Encryption
Needed to Work:	***Needed to Work:***
The same algorithm with the same secret key is used for encryption and decryption.	One algorithm is used for encryption and a related algorithm for decryption, with a pair of keys, known as the public key and the private key. The two keys can be used in either order, one for encryption and one for decryption.
The sender and receiver must share the algorithm and the secret key.	The sender and receiver must each have a unique public/private key pair.
Needed for Security:	***Needed for Security:***
The key must be kept secret.	The private key must be kept secret.
It must be impossible or at least impractical to decipher a message if the key is kept secret.	It must be impossible or at least impractical to decipher a message if the private key is kept secret.
Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	Knowledge of the algorithm plus the public key plus samples of ciphertext must be insufficient to determine the private key.

Cryptographic Hash Functions

Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that H(y) = h.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find $y \neq x$ with H(y) = H(x).
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).
Pseudorandomness	Output of H meets standard tests for pseudorandomness; that is, the output appears to be a random sequence of bits.



(a) Message authentication using symmetric encryption

CALVIN
INSTITUTE OF TECHNOLOGY
God's People for God's Glory

Terima Kasih
Tuhan Memberkati