



KRIPTOGRAFI DAN STEGANOGRAFI

Program Studi Informatika

**Sesi 6 – Implementasi Kriptografi untuk Perlindungan
Data Pribadi**

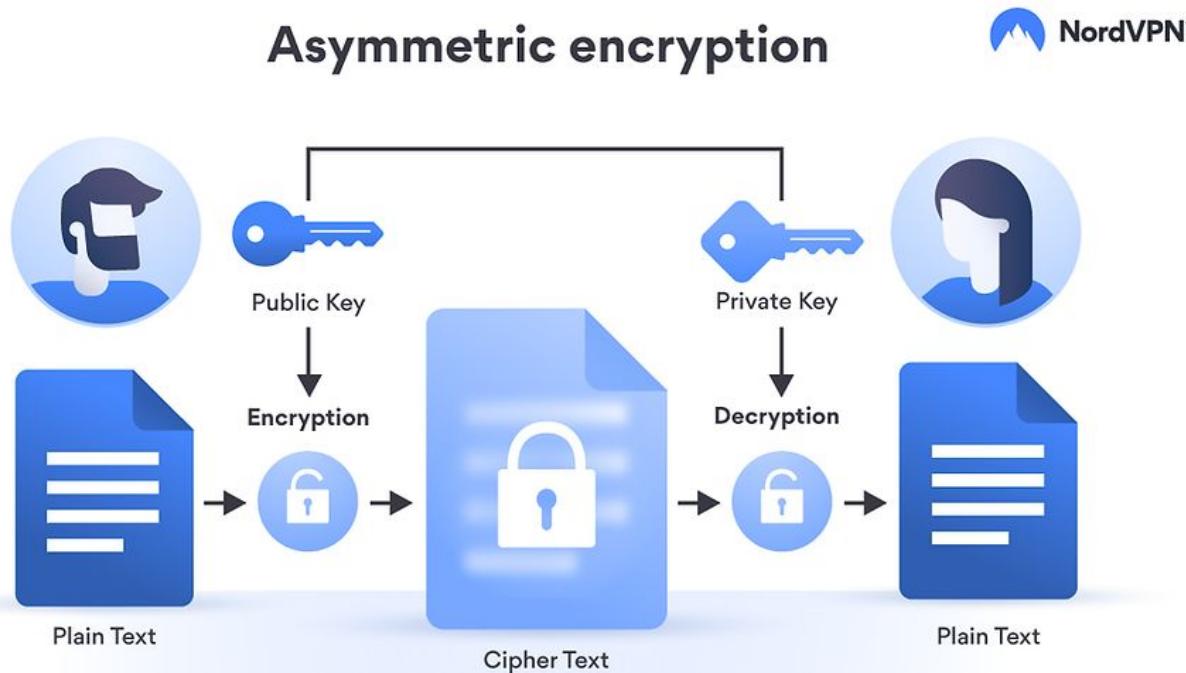
Abdul Azzam Ajhari, S.Kom.,
M.Kom.



Refreshment Sesi 5



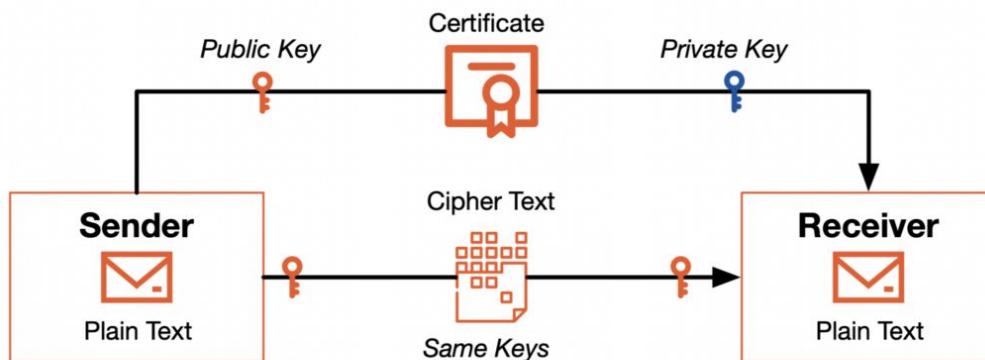
Kriptografi asimetris juga disebut sebagai kriptografi kunci publik. Ini adalah metode kriptografi paling populer yang digunakan untuk mengenkripsi dan mendekripsi pesan untuk menyediakan keamanan data di sebagian besar jaringan komunikasi. Sepasang kunci yang berbeda digunakan: kunci publik dan kunci privat.





Kriptografi Asymmetric in Daily Life

Using Asymmetric Encryption to Establish Connection



Using the Symmetric Encryption to Transmit Data

Sumber gambar: Tetrat

Dokumen valid, Sertifikat yang digunakan terpercaya

Meterai Elektronik 10000 G1 2023

Informasi Verifikasi

- ✓ Dokumen belum dimodifikasi sejak diberikan tandatangan elektronik
- ✓ Waktu penandatanganan didapatkan dari Timestamp Authority (TSA)
- ✓ Sertifikat yang digunakan untuk penandatangan dokumen adalah valid
- ✓ Long-Term Validation

Informasi Tandatangan



Waktu Penandatanganan : 2024-05-06 13:07:21

Lokasi : JAKARTA

Alasan : [BG3EUSYWR10H0MQ80000A9] 3

Penandatangan : Meterai Elektronik 10000 G1 2023

Penanda Waktu : Meterai Elektronik TSA



PUBLIC KEY INFRASTRUCTURE



www.thecyphere.com

info@thecyphere.com



Implementasi Kriptografi untuk Pelindungan Data Pribadi

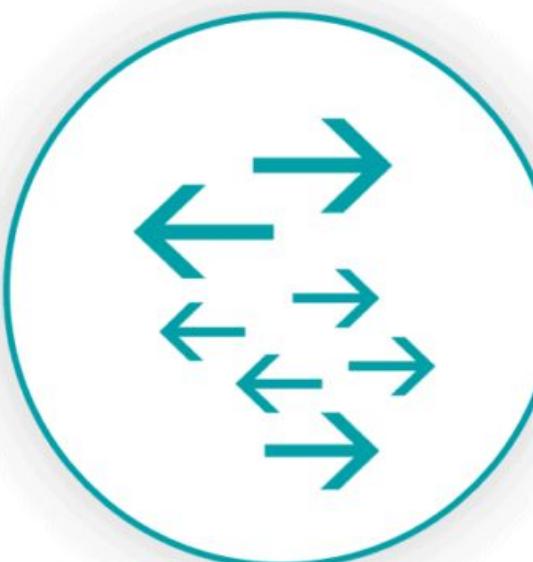


THE THREE STATES OF DATA

AT REST



IN TRANSIT

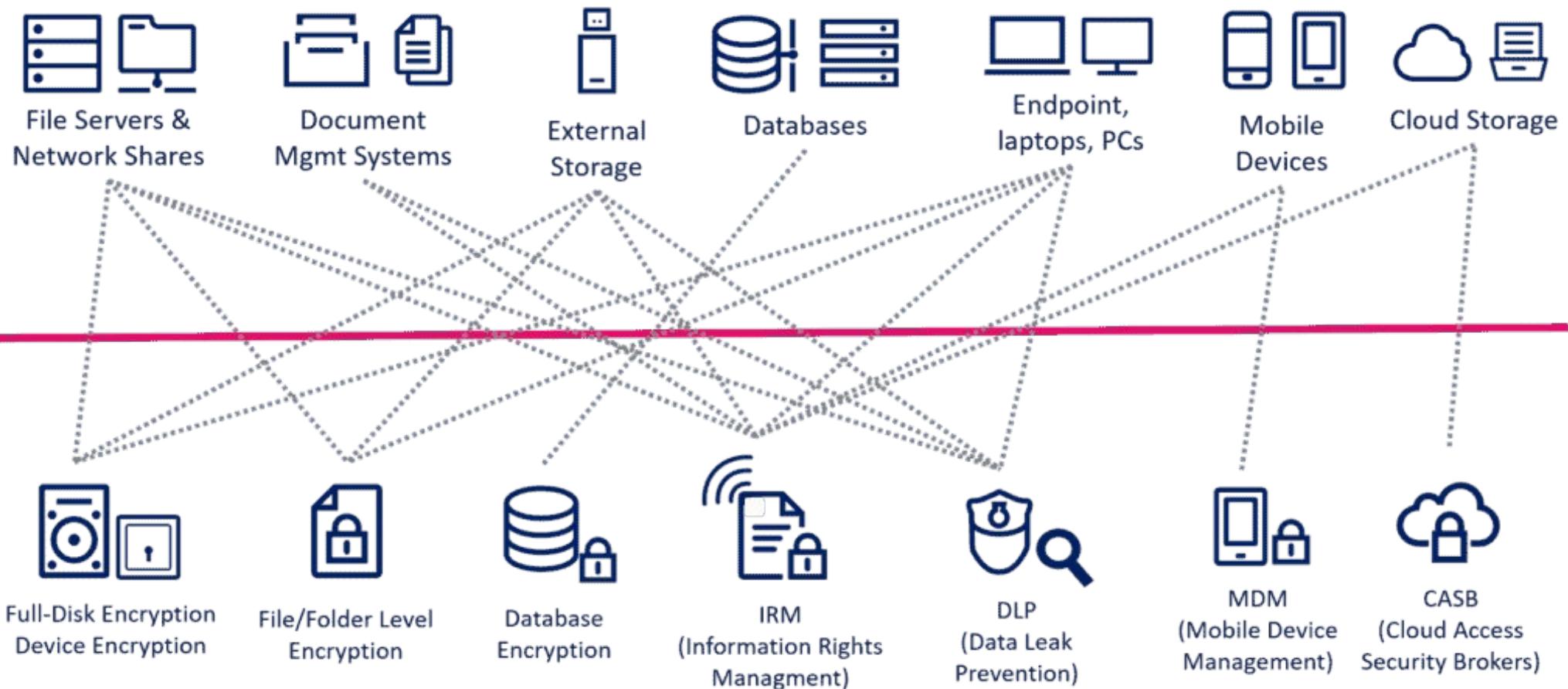


IN USE



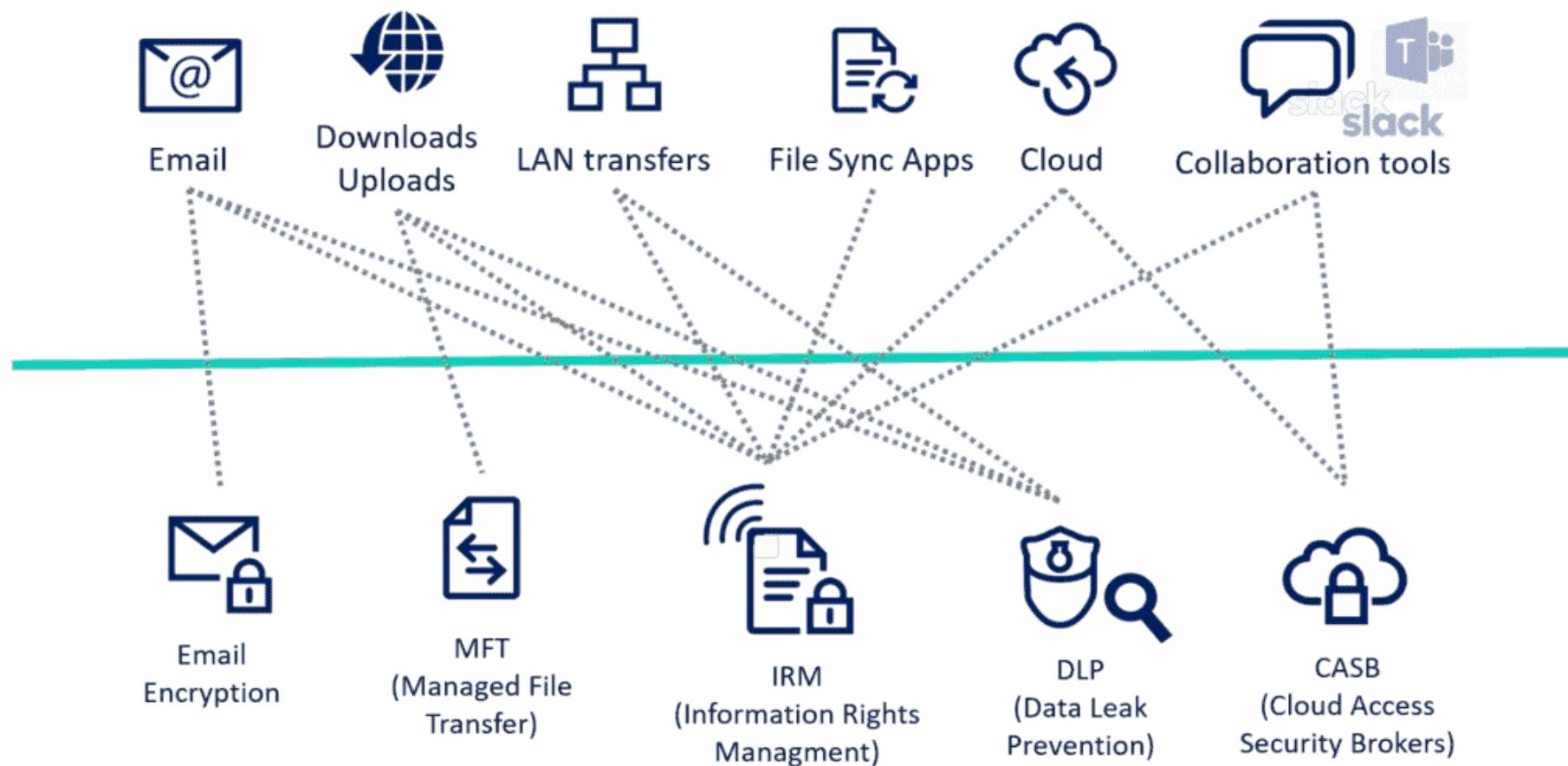


PROTECTING DATA AT REST





PROTECTING DATA IN TRANSIT





PROTECTING DATA IN USE



Office apps, PDFs, etc.



Databases, Corporate Apps



Cloud Apps



Mobile Apps



IdM
(Identity and Access Management)



RBAC & Conditional Access
(Role Based Access)



IRM
(Information Rights Management)



UU No 27 Tahun
2022 ttg PDP



Bersifat Umum

Nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan

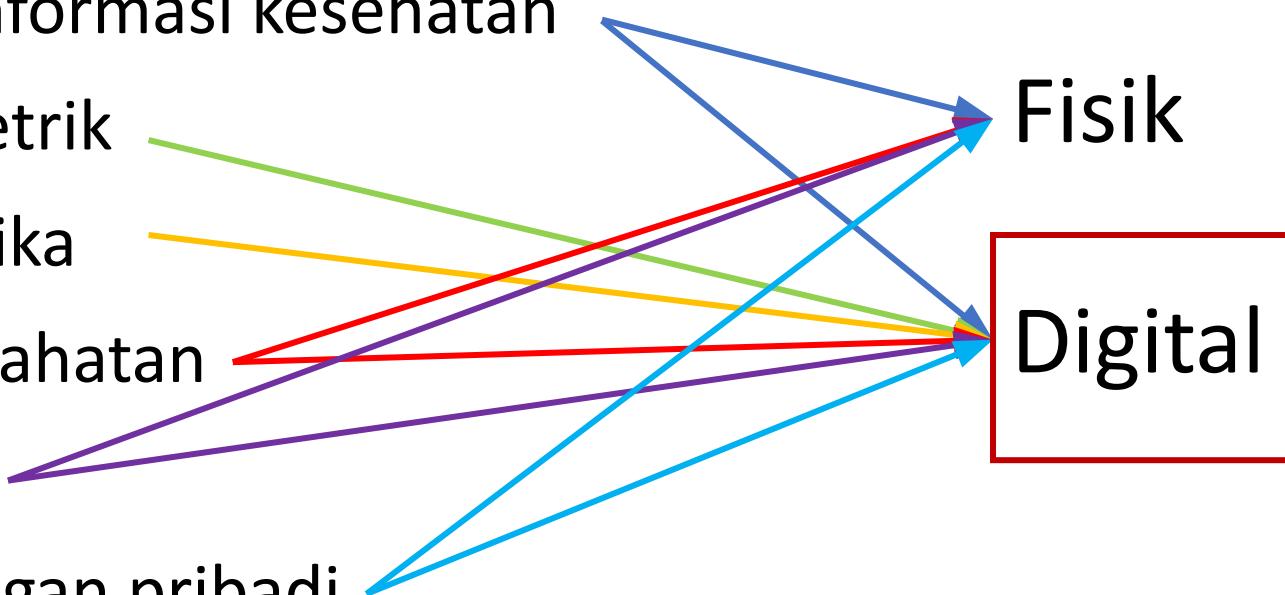
Bersifat Spesifik

Data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi



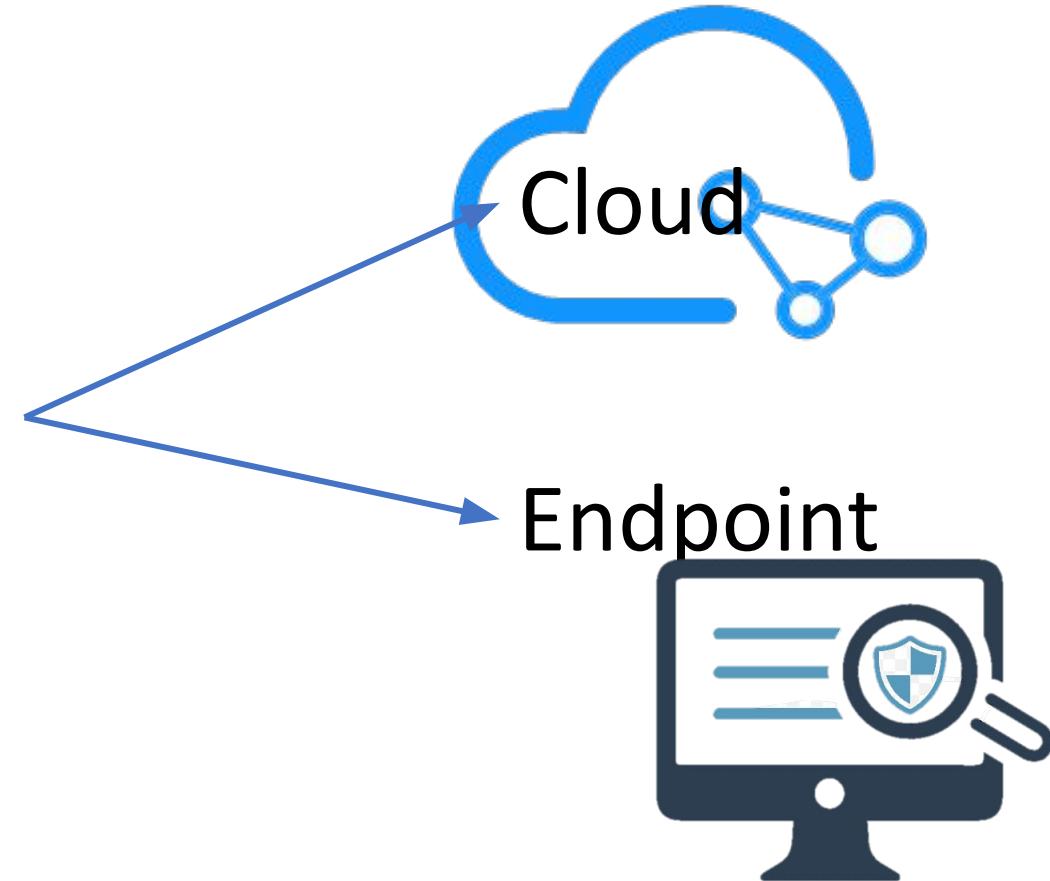
Bersifat Spesifik

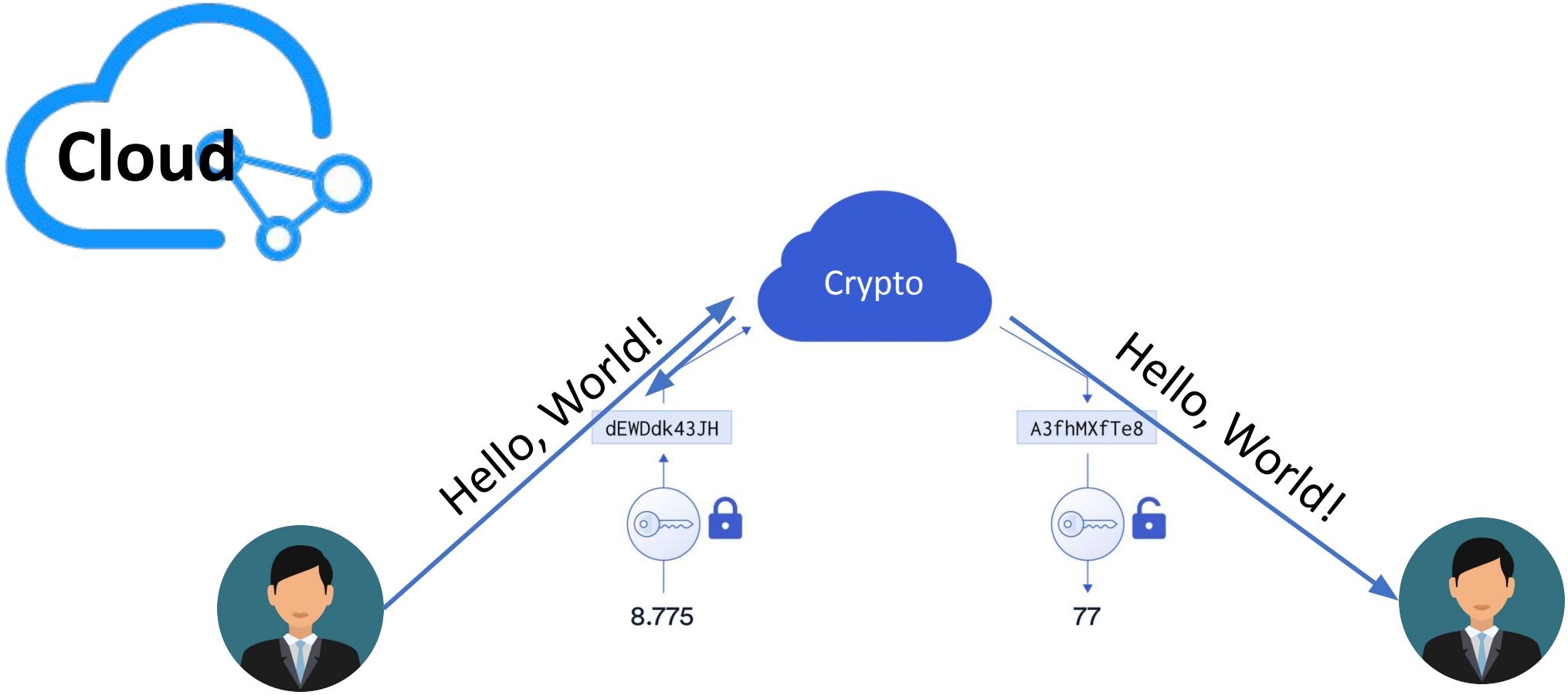
1. Data dan informasi kesehatan
2. Data biometrik
3. Data genetika
4. Catatan kejahatan
5. Data anak
6. Data keuangan pribadi





Digital Cryptography







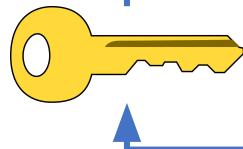
Endpoint



Hello, World!



yOuZwqrKS+INza/EH+NKUg==



Hello, World!



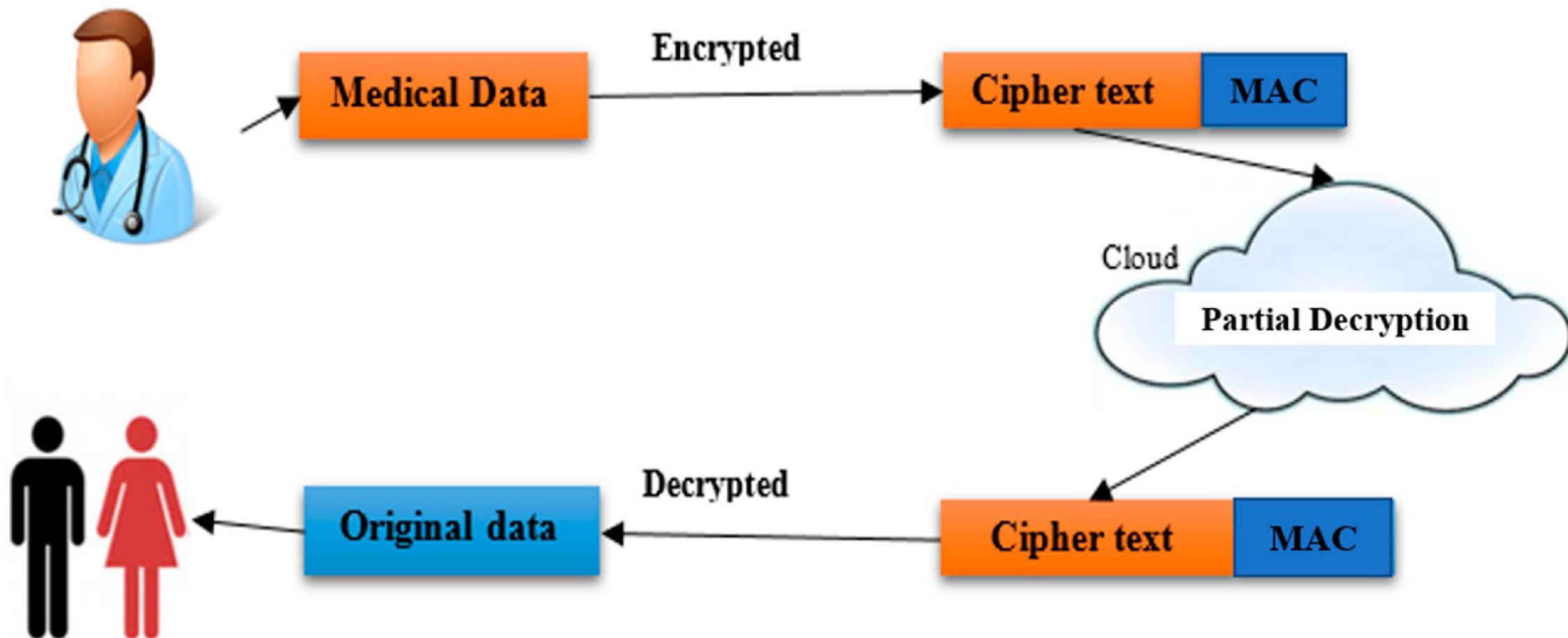
Same key



No	Cloud	Endpoint
1.	Protects data while it's stored on cloud servers	Protects data on the user's device before it is uploaded to the cloud.
2.	Allows for secure data sharing across different locations.	Provides an additional layer of security by encrypting sensitive information locally.
3.	Managed by the cloud provider, who handles key generation and management.	Can be more user-managed, depending on the device and application.



Dual Authentication-Based Encryption with a Delegation System to Protect Medical Data in Cloud Computing





- Computer Security Principles and Practice Third Edition, William Stallings and Lawrie Brown, Pearson, 2012
- Introduction to computer security, Matt Bishop, Addison Wesley, 2005
- Computer Networking: A Top Down Approach 6th edition Jim Kurose, Keith Ross, and Addison-Wesley
- <https://www.ericsson.com/en/blog/2021/7/cryptography-and-privacy-protecting-private-data>
- <https://selembardigital.com/pelajari-semua-tentang-cryptocurrency-criptografi-bagaimana-cara-kerjanya/>
- [https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography/cryptographic
hash-functions](https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography/cryptographic-hash-functions)
- Katz, J., & Lindell, Y. (2007). Introduction to Modern Cryptography: Principles and Protocols. CRC Press.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson.
- National Institute of Standards and Technology (NIST) - Publications on Secure Hash Standards (SHS)