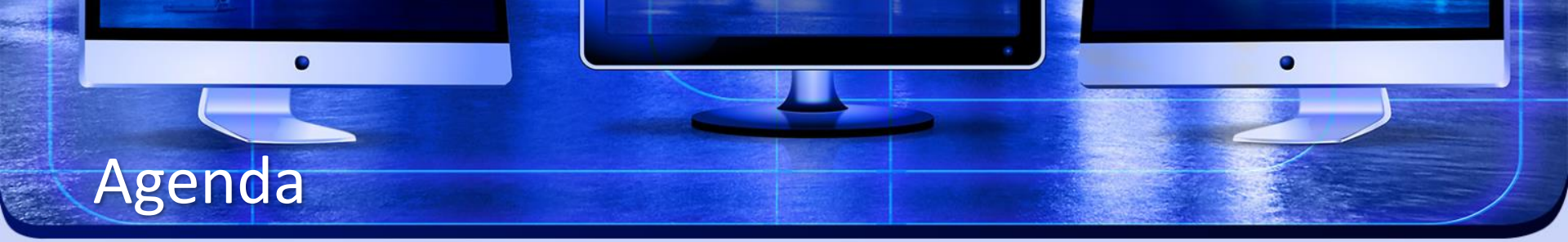
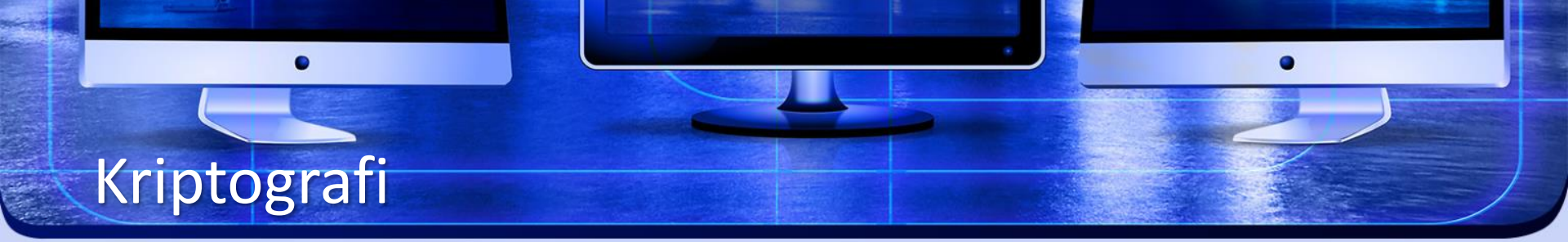
# Aspek Keamanan Dan Kerahasiaan SI

HARFEBI FRYONANDA, S.Kom, M.Kom



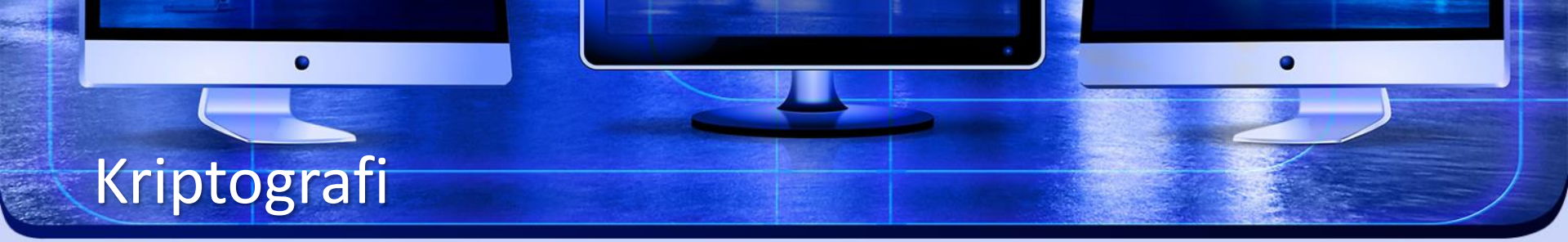
# Agenda

- Kriptografi
- Steganografi
- Enkripsi
- Kunci Private dan Public
- Kombinasi Kunci Private dan Public



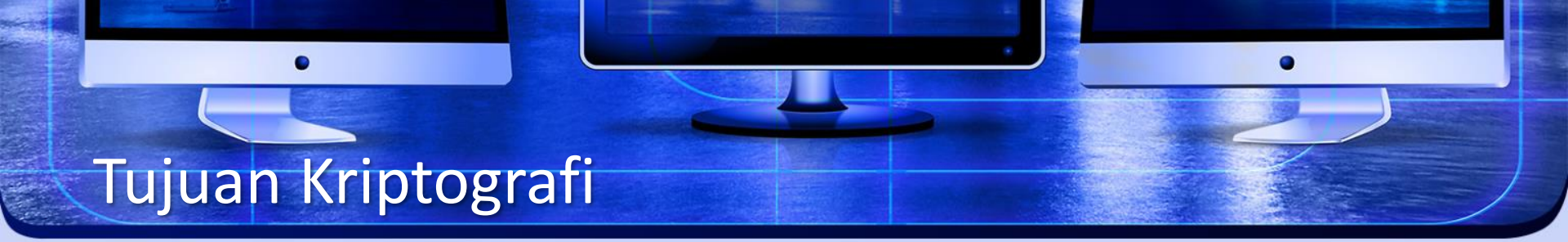
# Kriptografi

- Merupakan ilmu dan seni untuk menjaga pesan agar aman
- “Crypto” berarti “secret” (rahasia) dan “graphy” berarti “writing” (tulisan).
- Para pelaku atau praktisi kriptografi disebut cryptographers.
- Sebuah algoritma kriptografik (cryptographic algorithm), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi.



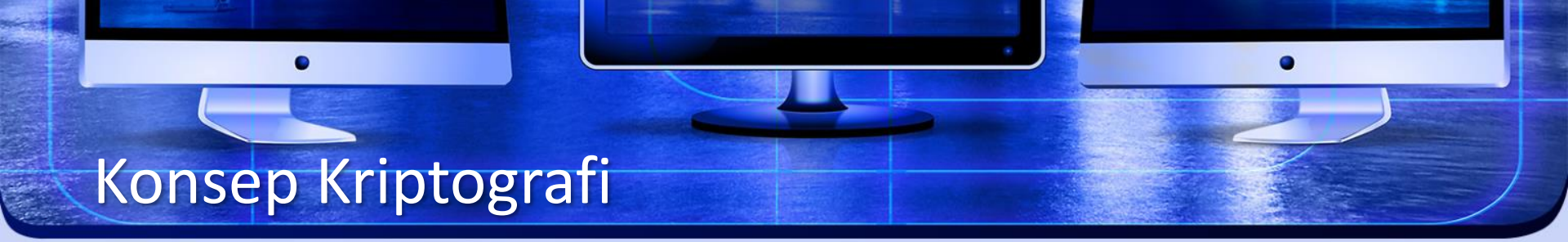
# Kriptografi

- Sampai akhir tahun 1970, hanya ada system kriptografi kunci-simetri.
- Satu masalah besar dalam sistem kriptografi: bagaimana mengirimkan kunci rahasia kepada penerima?
- Mengirim kunci rahasia pada saluran public (telepon, internet, pos) sangat tidak aman.
- Oleh karena itu, kunci harus dikirim melalui saluran kedua yang benar-benar aman.
- Saluran kedua tersebut umumnya lambat dan mahal.



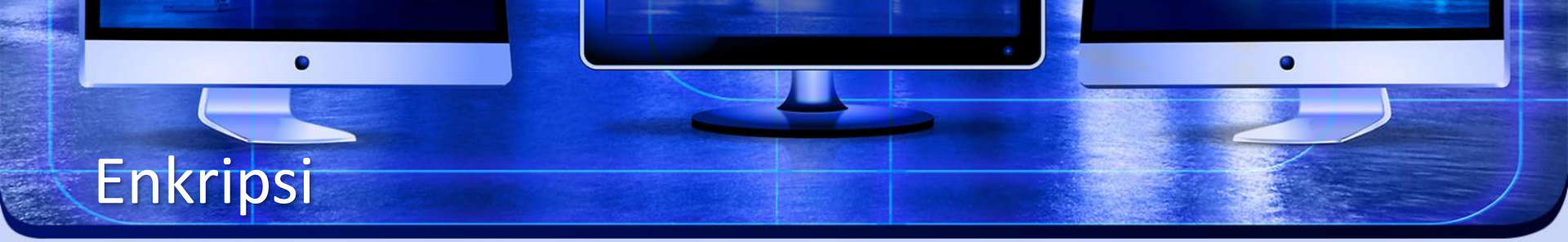
# Tujuan Kriptografi

- Secrecy
- Integrity
- Authentication
- Non-Repudiation



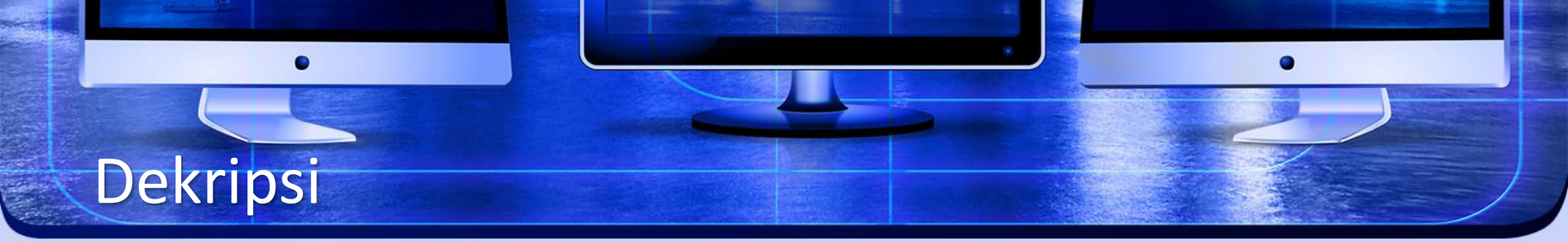
# Konsep Kriptografi

- Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi.



# Enkripsi

- Proses informasi/data yang akan dikirim diubah menjadi bentuk yang tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu

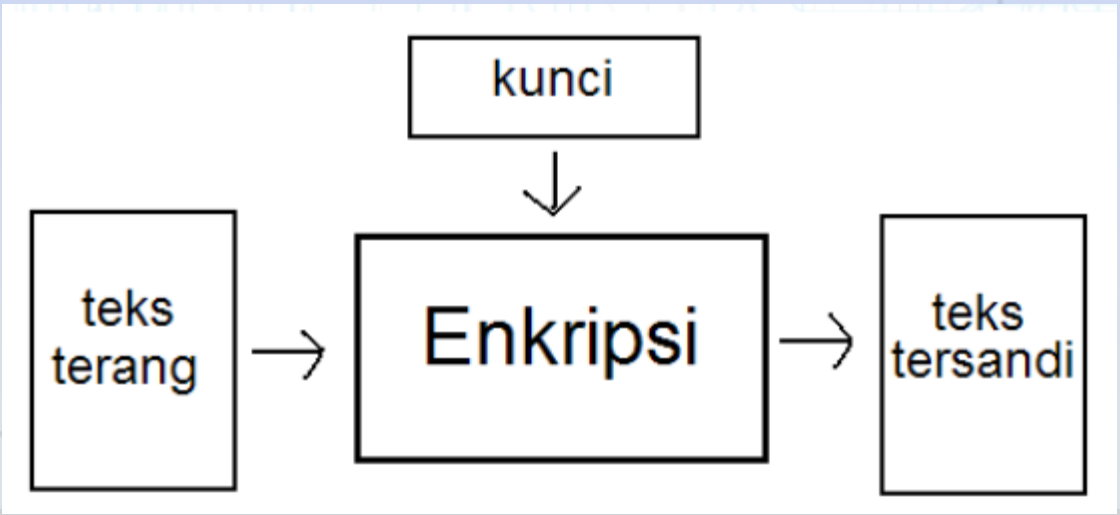


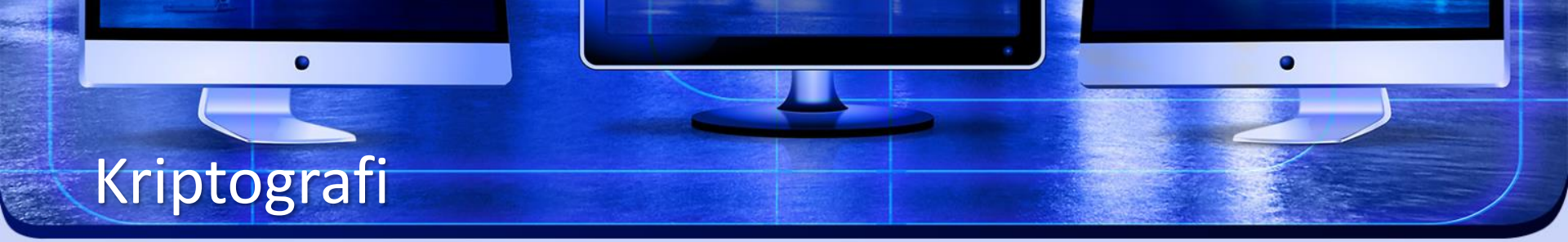
# Dekripsi

- Mengubah kembali bentuk tersamar tersebut menjadi informasi awal

# Kriptografi

- Kriptografi terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi.



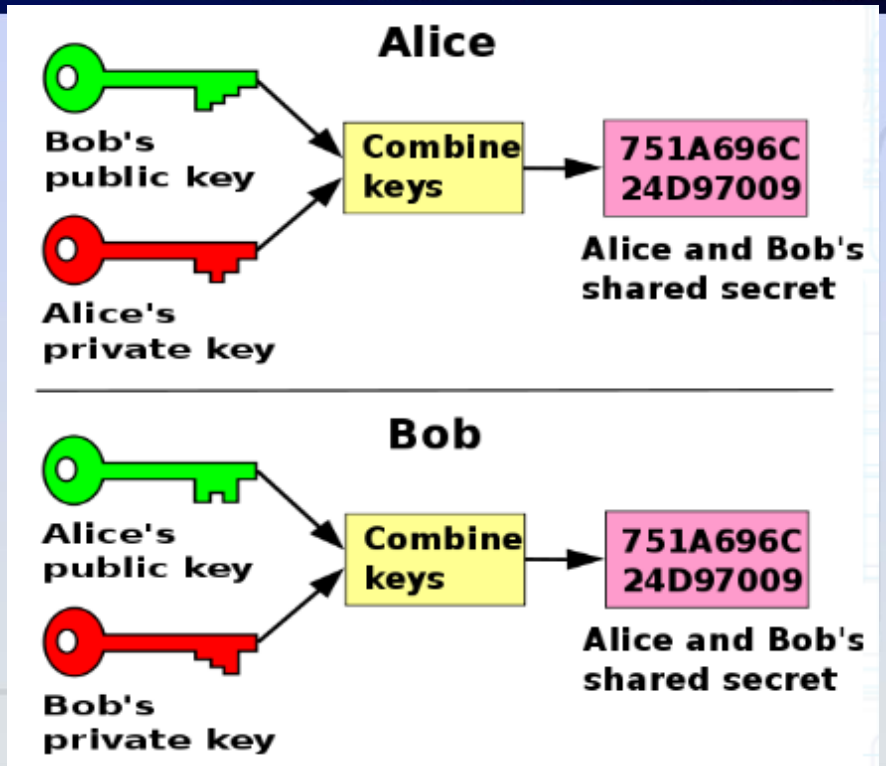


# Kriptografi

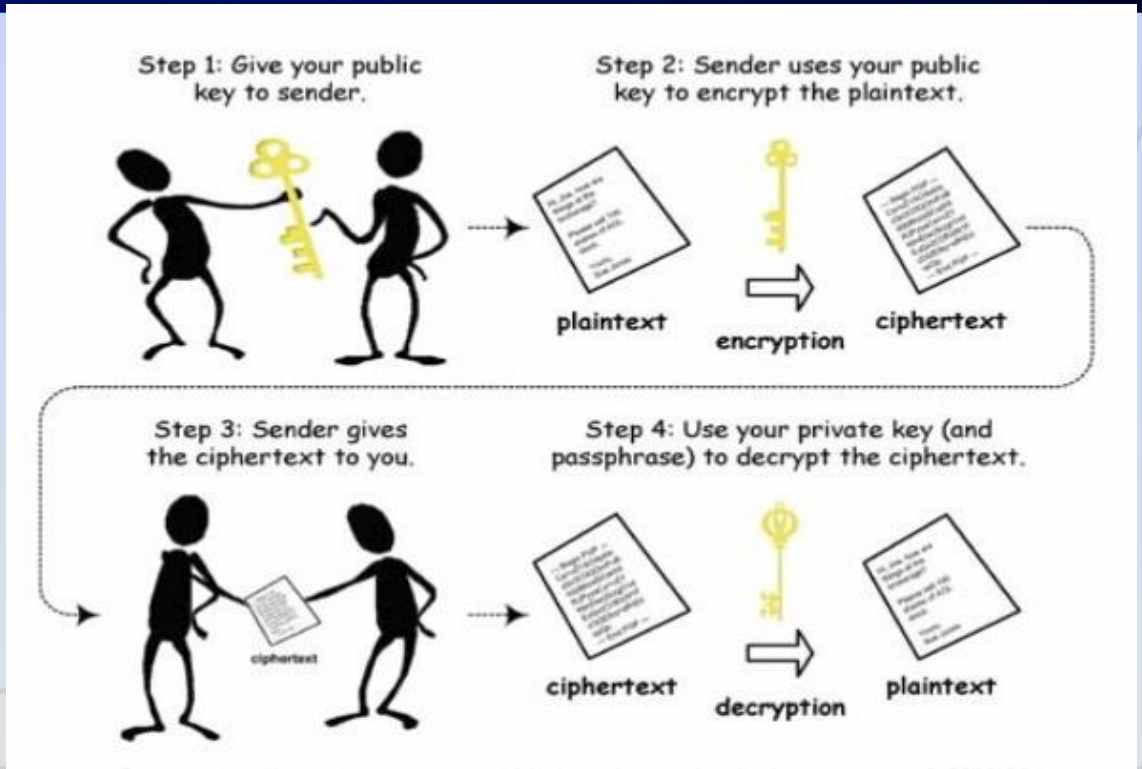
- Algoritma kriptografi berdasarkan jenis kunci yang digunakan dapat dibedakan menjadi dua jenis :

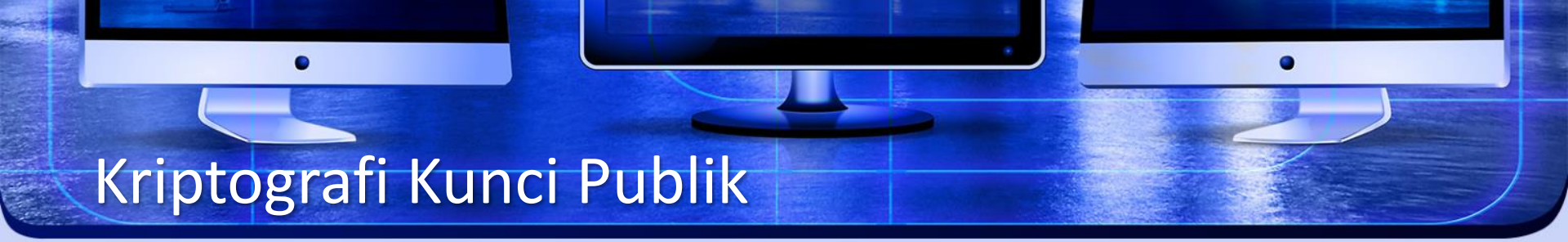
1. Algoritma Simetris
2. Algoritma Asimetris (Kunci Publik – Privat)

# Kriptografi Kunci Publik



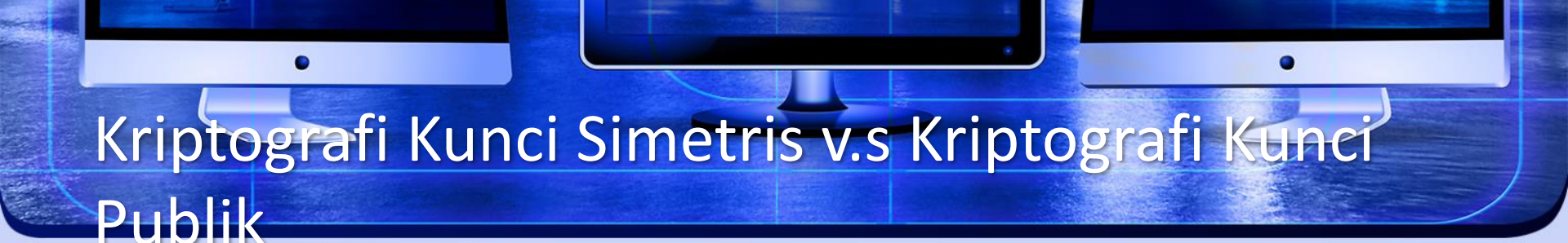
# Kriptografi Kunci Publik





# Kriptografi Kunci Publik

- Kunci enkripsi dapat dikirim melalui saluran yang tidak perlu aman (unsecure channel).
- Saluran yang tidak perlu aman ini mungkin sama dengan saluran yang digunakan untuk mengirim cipherteks.



# Kriptografi Kunci Simetris v.s Kriptografi Kunci Publik

- Analogi kriptografi kunci-simetri dan kriptografi kunci-publik dengan kotak surat yang dapat dikunci dengan gembok.
- Kriptografi kunci-simetri: Alice dan Bob memiliki kunci gembok yang sama
- Kriptografi kunci-publik: Bob mengirimi Alice gembok dalam keadaan tidak terkunci (gembok = kunci publik Bob, kunci gembok = kunci privat Bob).

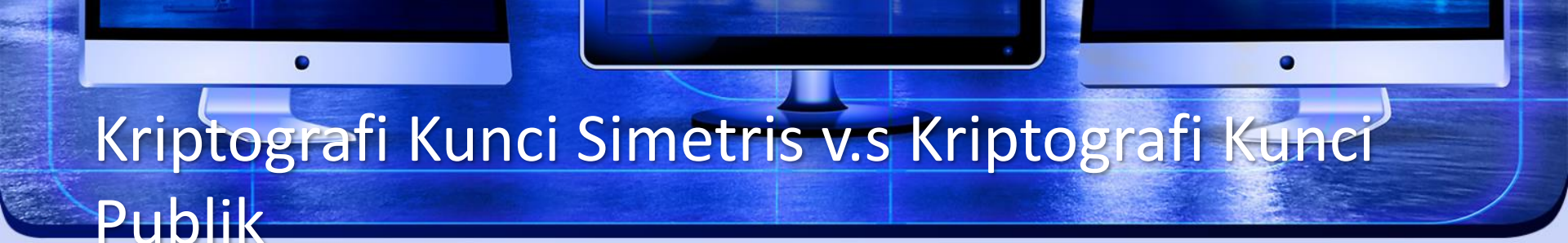
# Kriptografi Kunci Simetris v.s Kriptografi Kunci Publik

- Algoritma Simetris

Kunci yang digunakan untuk proses enkripsi dan dekripsi adalah kunci yang sama.

**Kelebihan :**

- Proses enkripsi/dekripsi membutuhkan waktu yang singkat.
- Ukuran kunci simetri relatif pendek .
- Otentikasi pengirim pesan langsung diketahui dari cipherteks yang diterima, karena kunci hanya diketahui oleh pengirim dan penerima pesan saja.



# Kriptografi Kunci Simetris v.s Kriptografi Kunci Publik

Kelemahan :

- Kunci simetri harus dikirim melalui saluran yang aman. Kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci ini.
- Kunci harus sering diubah, mungkin pada setiap sesi komunikasi

Contoh algoritma : TwoFish, Rijndael, Camellia

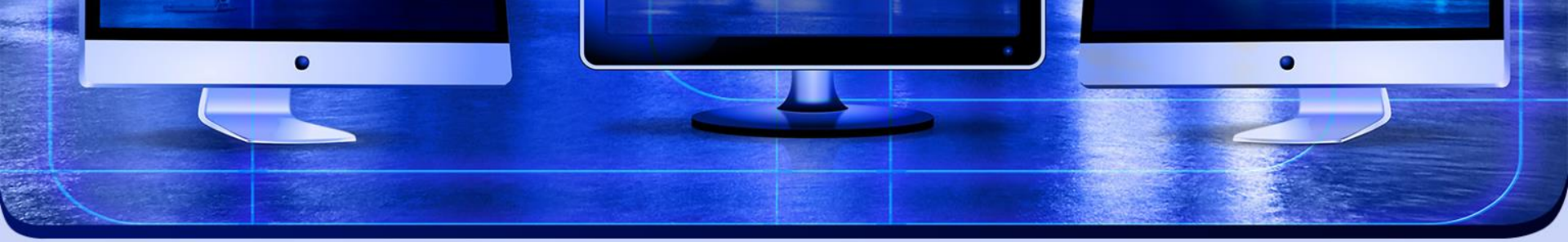
# Kriptografi Kunci Simetris v.s Kriptografi Kunci Publik

- Algoritma Asimetris

Kunci yang digunakan untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.

Kelebihan :

- Masalah keamanan pada distribusi kunci dapat lebih baik
- Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit



- Kelebihan :
  - Hanya kunci privat yang perlu dijaga kerahasiaannya oleh seiap entitas yang berkomuniaksi. Tidak ada kebutuhan mengirim kunci kunci privat sebagaimana pada system simetri.
  - Pasangan kunci publik/kunci privat tidak perlu diubah, bahkan dalam periode waktu yang panjang.

# Kriptografi Kunci Simetris v.s Kriptografi Kunci Publik

- Kelebihan :
  - Dapat digunakan untuk mengamankan pengiriman kunci simetri.
  - dapat digunakan untuk memberi tanda tangan digital pada pesan.

# Kriptografi Kunci Simetris v.s Kriptografi Kunci Publik

- Kelemahan :
  - Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris.
  - Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.
  - Ukuran cipherteks lebih besar daripada plainteks (bisa dua sampai empat kali ukuran plainteks).
  - Ukuran kunci relatif lebih besar daripada ukuran kunci simetri.

  Contoh algoritma : RSA, DSA, ElGamal