

# DASAR-DASAR KEAMANAN SISTEM INFORMASI

Kriptografi, Steganografi



Gentisya Tri Mardiani, S.Kom., M.Kom



The background of the slide features a blue gradient with a pattern of binary code (0s and 1s). Several puzzle pieces are scattered across the top, some of which are highlighted with a bright blue glow. The word "KRIPTOGRAFI" is centered in a large, bold, black font.

# KRIPTOGRAFI

- Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman.
- Para pelaku atau praktisi kriptografi disebut *cryptographers*.
- Sebuah algoritma kriptografik (*cryptographic algorithm*), disebut ***cipher***, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi.





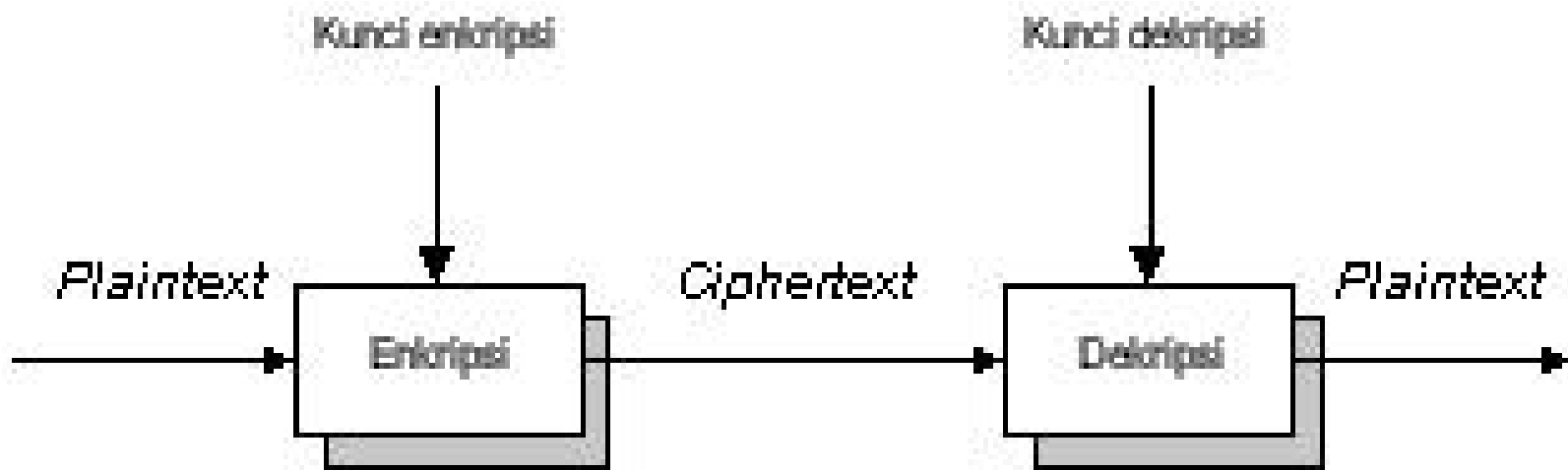
- **Enkripsi (*encryption*)**

Proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext*) menjadi pesan yang tersembunyi (*ciphertext*).

- **Dekripsi (*decryption*)**

Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*.





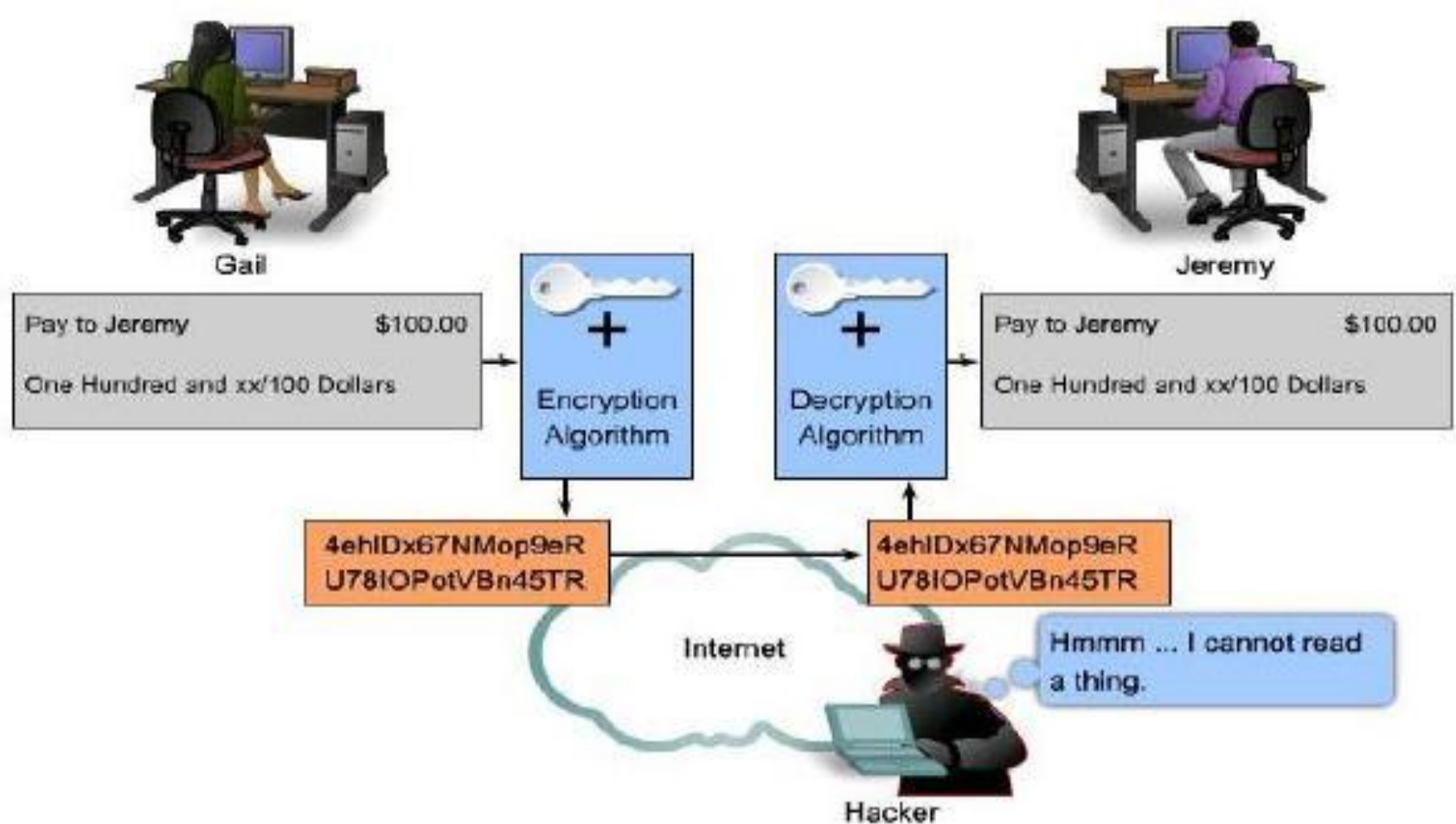


The background of the slide features a blue gradient with a pattern of binary code (0s and 1s). Several puzzle pieces are scattered across the top half of the image, some of which are interlocked. The puzzle pieces have a light blue color and a subtle texture. The title text is overlaid on this background.

# Prinsip yang mendasari KRIPTOGRAFI

- Confidentiality (kerahasiaan)
- Integrity (keutuhan)
- Authentication (otentikasi)
- Non- repudiation (anti penyangkalan)









# Algoritma Kriptografi

- Keamanan sistem yang digunakan kemudian tidak bergantung kepada pengetahuan algoritma yang digunakan, melainkan bergantung kepada kunci yang digunakan.





- Misalnya:

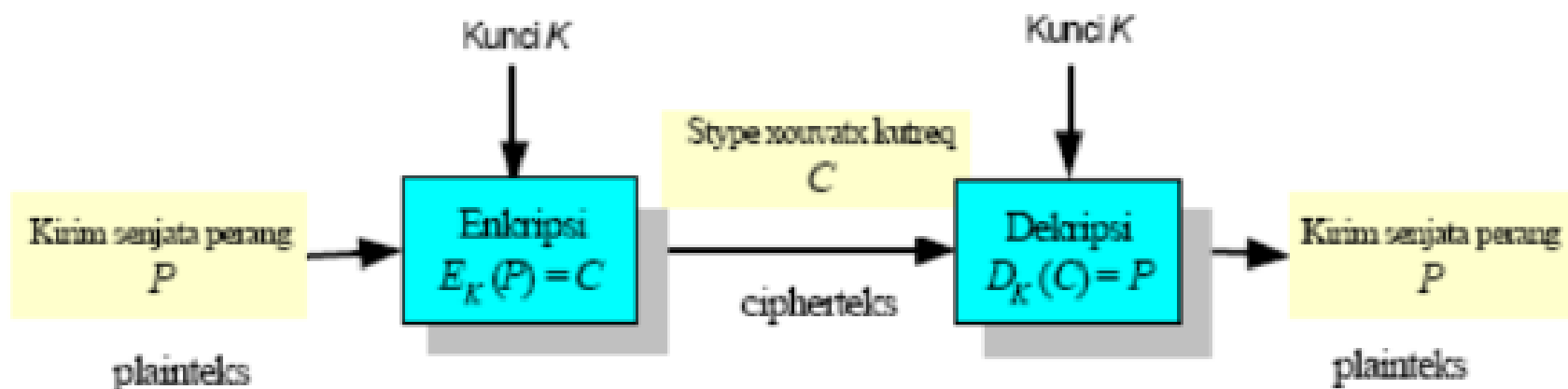
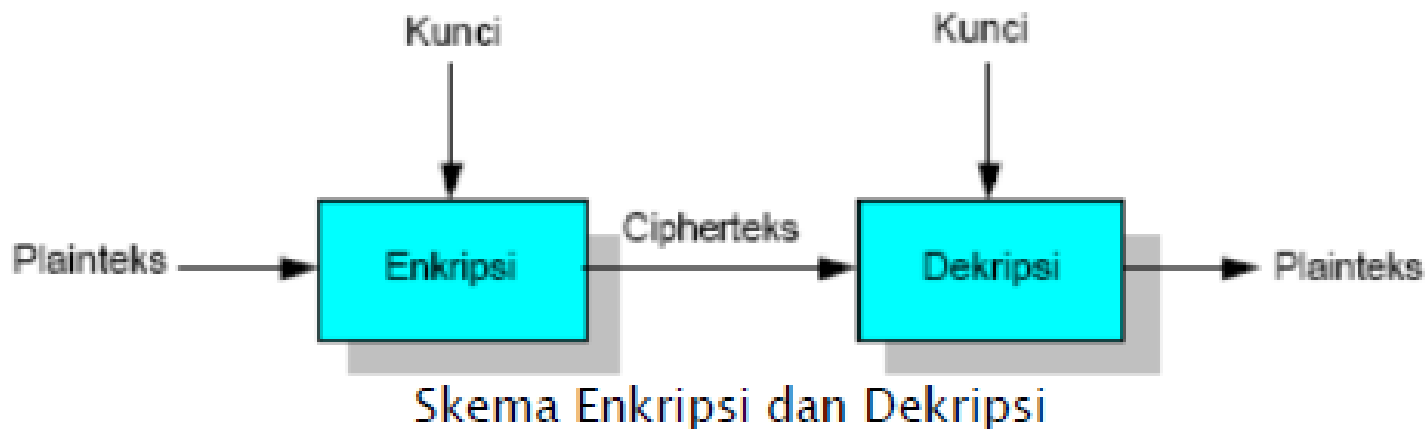
dengan menggunakan kunci K, maka fungsi enkripsi dan dekripsi dapat ditulis:

$$EK(P) = C \text{ dan } DK(C) = P$$

enkripsi E menggunakan kunci K terhadap plainteks P menghasilkan ciperteks, dekripsi D sebaliknya.



# Proses Enkripsi dan Dekripsi



Contoh Enkripsi dan Dekripsi Pesan





# Jenis Algoritma Kriptografi

Berdasarkan jenis kunci yang digunakan dapat dibedakan menjadi dua jenis yaitu :

- **Algoritma *simetris***

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

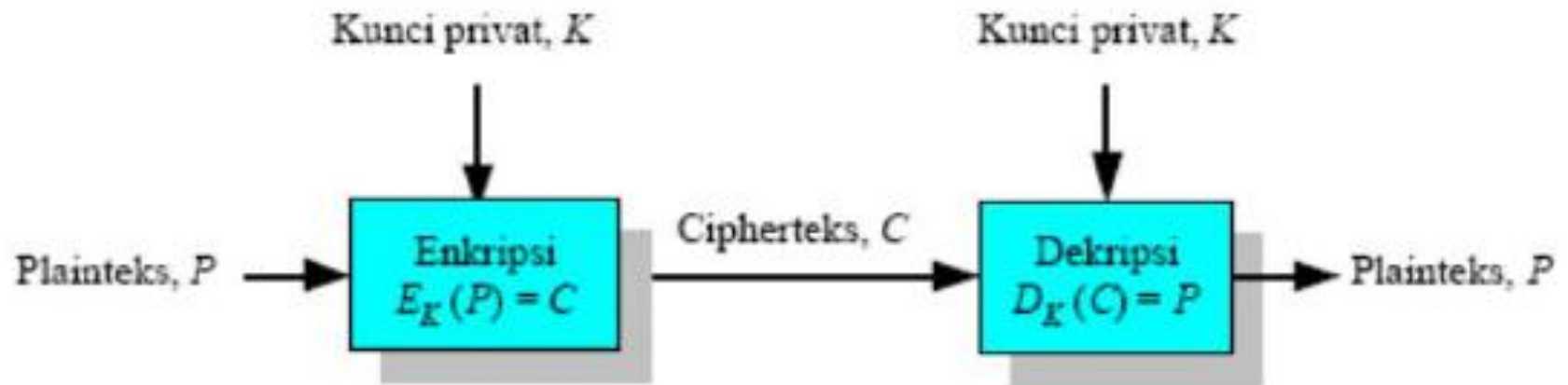
- **Algoritma *asimetris***

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



# Algoritma Simetris

- Algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya.





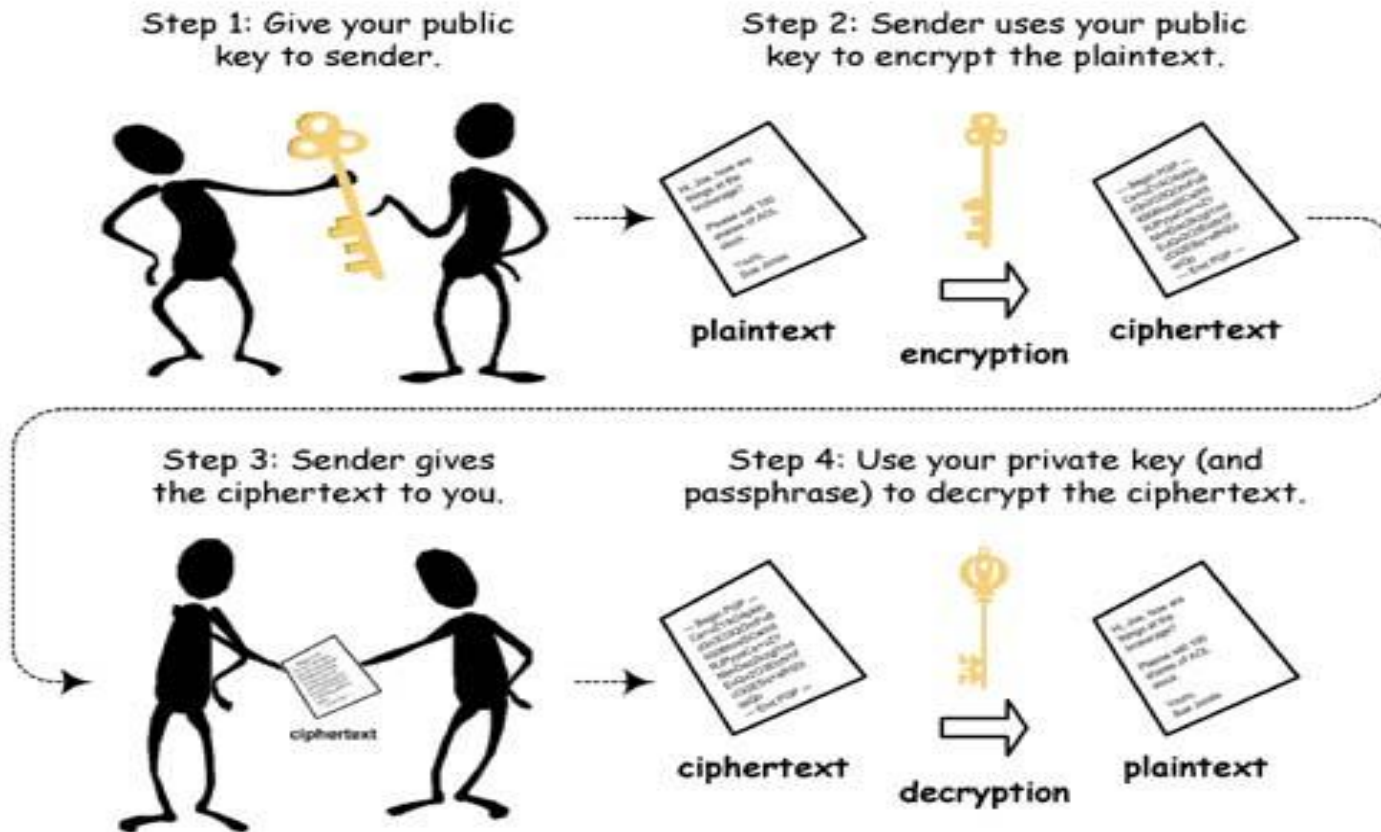
The background of the slide features a blue gradient with a pattern of binary code (0s and 1s). Overlaid on this are several puzzle pieces. Some pieces are solid blue, while others are white with blue outlines and contain binary code. The puzzle pieces are arranged in a way that suggests they are part of a larger, incomplete picture.

# Algoritma Simetris

- Istilah lain: *private-key cryptography, secret-key cryptography, conventional cryptography*
- Keamanan sistem kriptografi terletak pada kerahasiaan kuncinya.
- Pengirim dan penerima pesan sudah berbagi kunci yang sama sebelum bertukar pesan



# Algoritma Simetris





The background of the slide features a blue gradient with a pattern of binary code (0s and 1s). Several puzzle pieces are scattered across the top, some of which are highlighted with a bright blue glow. The title 'Algoritma Simetris' is centered in a large, black, sans-serif font.

# Algoritma Simetris

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



The background of the slide features a blue gradient with a pattern of binary code (0s and 1s). Several puzzle pieces are scattered across the top half of the image, some of which are highlighted with a bright blue glow. The title 'Algoritma Simetris' is centered in a large, black, sans-serif font.

# Algoritma Simetris

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





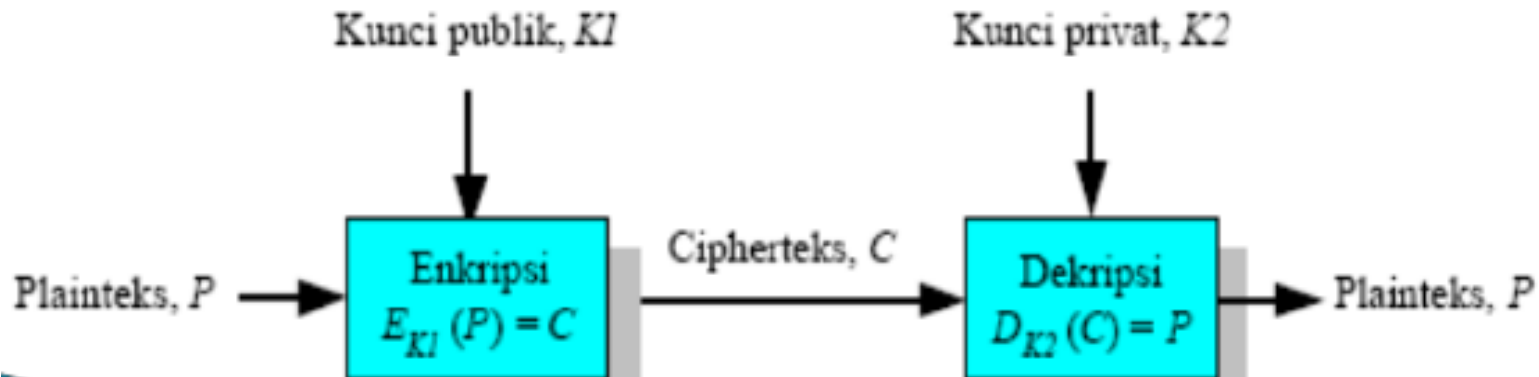
# Contoh Algoritma Simetris

- Algoritma Simetris
  - a. Blok Chiper :
    - Data Encryption Standard (DES)
    - RC2, RC4, RC5, RC6
    - International Data Encryption Algorithm (IDEA)
    - Advanced Encryption Standard (AES)
  - b. Stream Chiper :
    - One Time Pad (OTP), A5 dsb



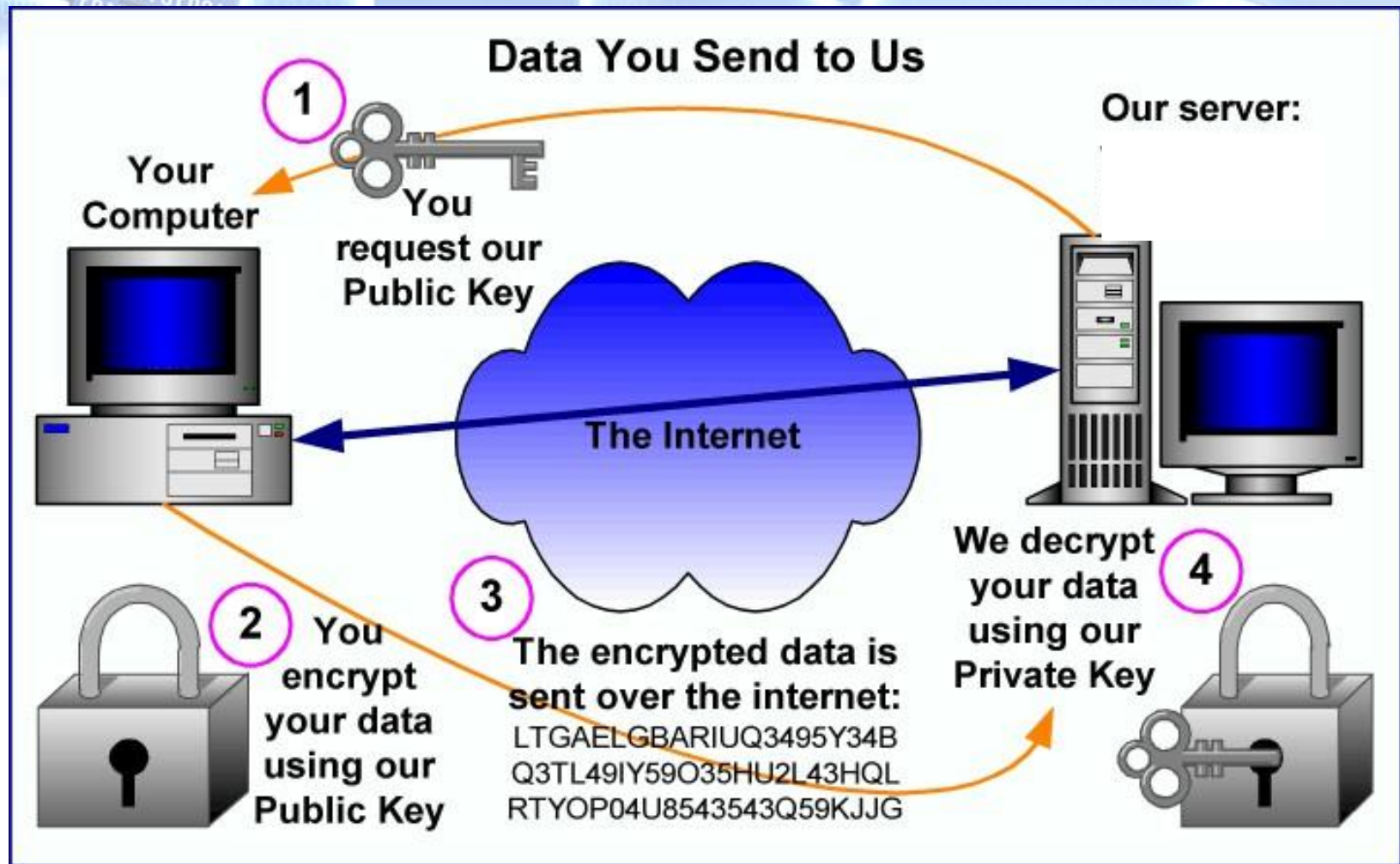
# Algoritma Asimetris

- Terdapat dua kunci yang digunakan
  - Kunci enkripsi: tidak rahasia dan dapat diketahui (kunci publik)
  - Kunci dekripsi: kunci rahasia hanya diketahui oleh penerima pesan (kunci private)
- Setiap entitas yang berkomunikasi mempunyai sepasan kunci (kunci privat dan publik)





# Algoritma Asimetris







# Algoritma Asimetris

- Kelebihan:
  - Hanya kunci privat yang perlu dijaga kerahasiaannya oleh setiap entitas yang berkomunikasi
  - Pasangan kunci privat/publik tidak perlu diubah, bahkan dalam periode waktu yang panjang





# Algoritma Asimetris

- Kelemahan:
  - Proses enkripsi dan dekripsi lebih lambat
  - Ukuran ciperteks lebih besar daripada plainteks
  - Ukuran kunci relatif lebih besar daripada ukuran kunci pada algoritma simetris
  - Karena kunci publik diketahui secara luas dan dapat digunakan setiap orang, maka ciperteks tidak memberikan informasi mengenai otentikasi pengirim



The background of the slide features a blue gradient with a pattern of binary code (0s and 1s). Several puzzle pieces are scattered across the top half of the image, some of which are interlocked. The puzzle pieces also contain binary code. The title 'Contoh Algoritma Asimetris' is centered over the puzzle pieces.

# Contoh Algoritma Asimetris

- Digital Signature Algorithm (DSA)
- RSA
- Diffie Hellman
- Elliptic Curve Cryptography (ECC)
- Quantum, dsb





# Fungsi Hash

- Fungsi Hash merupakan fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap.
- Fungsi hash biasanya digunakan jika membuat sidik jari dari suatu pesan, yang merupakan tanda bahwa pesan tersebut benar berasal dari pengirim asli.





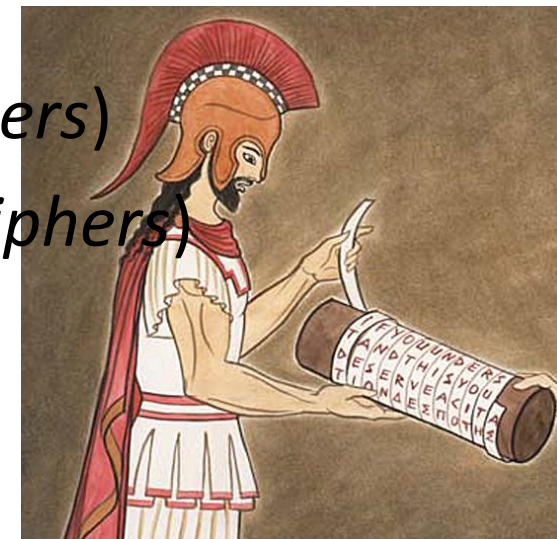
# Contoh Fungsi Hash

- Fungsi hash sering disebut one way function, message-digest, fingerprint, fungsi kompresi, dan message authentication code (MAC)
- MD5, SHA, dsb



# KRIPTOGRAFI KLASIK

- Algoritma kriptografi klasik berbasis karakter
- Menggunakan pena dan kertas saja, belum ada komputer
- Termasuk ke dalam kriptografi kunci-simetri
- Algoritma kriptografi klasik:
  - *Cipher Substitusi (Substitution Ciphers)*
  - *Cipher Transposisi (Transposition Ciphers)*





# 1. Cipher Substitusi - Caesar Cipher

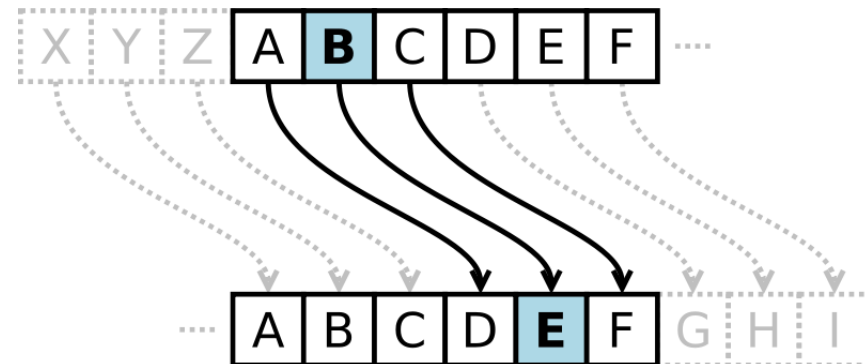
- Tiap huruf alfabet digeser 3 huruf ke kanan

$p_i$  : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
 $c_i$  : **D E F G H I J K L M N O P Q R S T U V W X Y Z A B C**


- Contoh:

Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBD REHOLA**





- 
- Dalam praktek, cipherteks dikelompokkan ke dalam kelompok n-huruf, misalnya kelompok 4-huruf:

DZDV LDVW HULA GDQW HPDQ QBDR EHOL A

- Atau membuang semua spasi:  
DZDVLDVWHULAGDQWHPDQQBDREHOLA
- Tujuannya agar kriptanalisis menjadi lebih sulit



The background of the slide features a blue gradient with a pattern of binary code (0s and 1s). Several interlocking puzzle pieces are scattered across the top, some of which also contain binary code. The title 'ROT13' is prominently displayed in the center of the puzzle pieces.

# ROT13

- Substitution cipher yang masih umum digunakan di sistem UNIX
- Sebuah huruf digantikan dengan huruf yang letaknya 13 posisi darinya. Sebagai contoh, huruf “A” digantikan dengan huruf “N”, huruf “B” digantikan dengan huruf “O”, dan seterusnya.



The background of the slide features a blue gradient with a pattern of binary code (0s and 1s). Overlaid on this are several puzzle pieces. Some pieces are solid blue, while others are white with black outlines and contain binary code. The puzzle pieces are arranged in a way that suggests they are being assembled or rearranged, which visually represents the concept of transposition or permutation.

## 2 Ciper Transposisi

- Cipherteks diperoleh dengan mengubah posisi huruf di dalam plainteks.
- Algoritma ini melakukan *transpose* terhadap rangkaian huruf di dalam plainteks.
- Nama lain untuk metode ini adalah **permutasi**, karena *transpose* setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.





# Contoh

## Plaintext:

TEKNIK DAN ILMU KOMPUTER

## Enkripsi:

TEKNIKD  
ANILMUK  
OMPUTER

## Cipherteks: (baca secara vertikal)

TAOENMKI PNLUIMTKUEDKR

TAOE NMKI PNLU IMTK UEDK R





# KRIPTOGRAFI MODERN

- Beroperasi dalam mode bit (algoritma kriptografi klasik beroperasi dalam mode karakter)
- kunci, plainteks, cipherteks, diproses dalam rangkaian bit
- operasi bit xor paling banyak digunakan





# ALGORITMA KRIPTOGRAFI MODERN

- Tetap menggunakan gagasan pada algoritma klasik: substitusi dan transposisi, tetapi lebih rumit (sangat sulit dipecahkan)
- Perkembangan algoritma kriptografi modern didorong oleh penggunaan komputer digital untuk keamanan pesan.
- Komputer digital merepresentasikan data dalam biner.





- Pesan (dalam bentuk rangkaian bit) dipecah menjadi beberapa blok

- Contoh:

Plainteks 100111010110

Bila dibagi menjadi blok 4-bit

1001    1101    0110

maka setiap blok menyatakan 0 sampai 15 :

9

13

6





Bila plainteks dibagi menjadi blok 3-bit:

100      111      010      110

maka setiap blok menyatakan 0 sampai 7 :

4      7      2      6





# Steganografi

- **Steganografi** adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain pengirim dan penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa terdapat suatu pesan rahasia.





# Steganografi

- Istilah steganografi termasuk menyembunyikan data digital dalam berkas-berkas (*file*) komputer.
- Teknik steganografi meliputi banyak metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam berkas lain yang mengandung teks, *image*, bahkan audio tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari berkas semula.



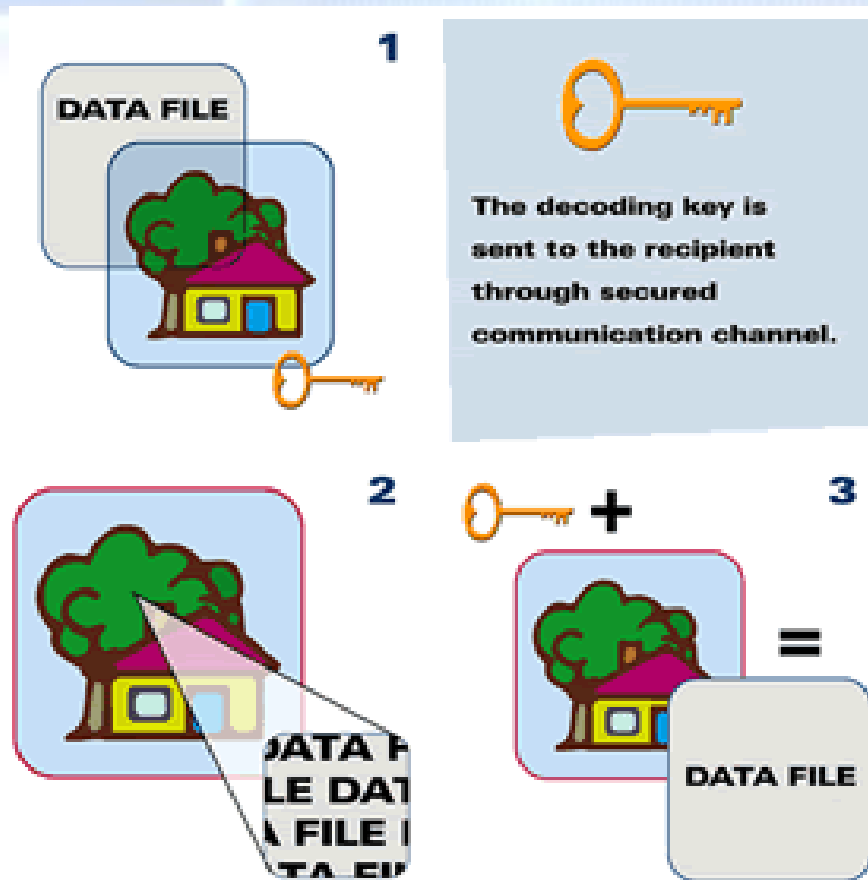
The background of the slide features a blue gradient with a pattern of binary code (0s and 1s). In the upper portion, there are several interlocking puzzle pieces. Some of these pieces are white with black binary code patterns, while others are solid blue. The word 'Steganografi' is centered over the puzzle pieces in a large, black, sans-serif font.

# Steganografi

- Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi.
- Format yang biasa digunakan di antaranya:
  - *image* : bitmap (bmp), gif, pcx, jpeg, dll.
  - audio : wav, voc, mp3, dll.
  - Format lain : teks file, html, pdf, dll.



# Steganografi





The background of the slide features a blue gradient with a pattern of binary code (0s and 1s). Several puzzle pieces are scattered across the top half of the image, some of which are highlighted with a bright blue glow. The title 'Jenis Serangan' is centered in the upper half of the slide.

# Jenis Serangan

- Ilmu untuk mendapatkan pesan asli yang telah disandikan tanpa memiliki kunci untuk membuka pesan rahasia disebut *kriptonalalisis*,
- Usaha untuk membongkar suatu pesan tanpa mendapatkan kunci yang sah dikenal sebagai serangan (*attack*)





# Jenis serangan

- *Chiphertext only attack*, penyerang hanya mendapatkan pesan yang sudah tersandikan saja.
  - *Known plaintext attack*, penyerang selain mendapatkan kunci, juga mendapatkan pesan asli
  - *Chosen plaintext attack*, penyerang dapat memilih penggalan mana dari pesan asli yang disandikan



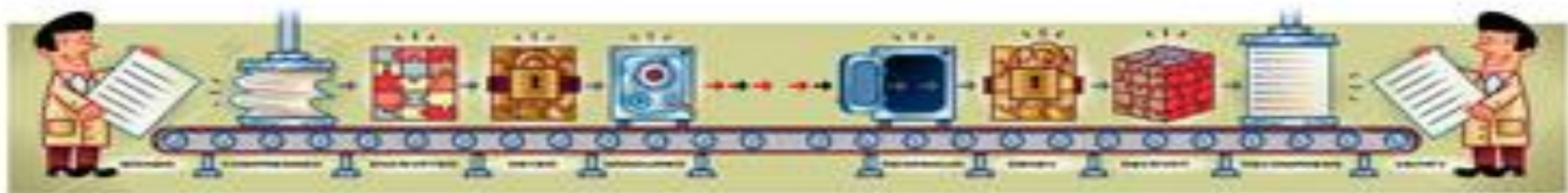
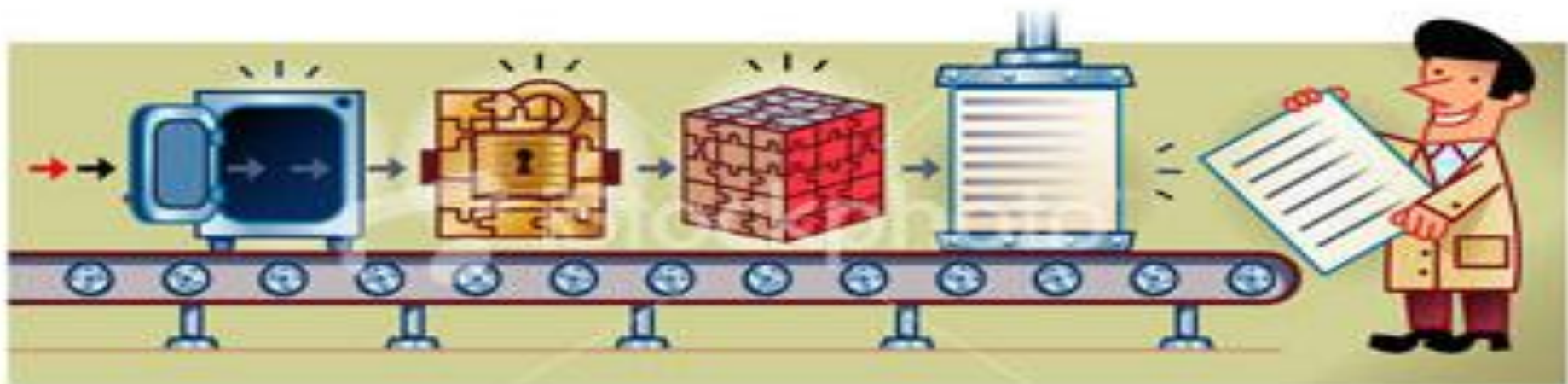
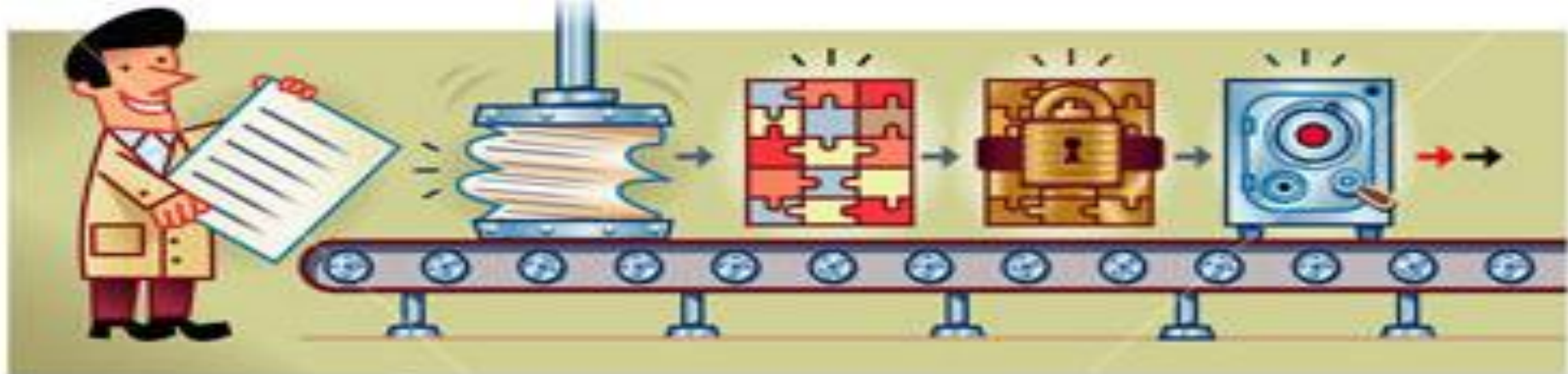


# Jenis serangan

Berdasarkan cara mendapatkan pesan dalam saluran komunikasi:

- Sniffing
- Replay attack
- Spoofing
- Man in the middle attack





See u next week..