# Pengamanan Informasi

# Aspek Keamanan

- Confidentiality (Kerahasiaan)
- Integrity (Integritas)
- Availability (Ketersediaan)

# Evolusi Pengamanan Data

- **Steganography**
  - Menyamarkan data sehingga seolah-olah tidak ada
- **Cryptography**
  - Mengacak data;
    - Mengubah susunan huruf (*transposition*)
    - Menggantikan huruf dengan huruf atau kode lainnya (*substitution*)

# Steganography

- **Yunani vs Persia**
  - Pesan disembunyikan di meja yang dilapisi lilin
- **Histalaeus**
  - Pesan ditato di kepala budak yang telah digunduli
- **Digital watermarking**
  - Menandai kepemilikan gambar digital dengan menyisipkan pesan dalam bit terendah (LSB)


# THE DA VINCI CODE

A NOVEL

While in Paris on business, Harvard symbologist Robert Langdon receives an urgent late-night phone call. The elderly curator of the Louvre has been murdered inside the museum, a baffling cipher found near the body. As Langdon and a gifted French cryptologist, Sophie Neveu, sort through the bizarre riddles, they are stunned to discover a trail of clues hidden in the works of Da Vinci—clues visible for all to see and yet ingeniously disguised by the painter.

The stakes are raised when Langdon uncovers a startling link: The late curator was involved in the Priory of Sion—an actual secret society whose members included Sir Isaac Newton, Botticelli, Victor Hugo, and Da Vinci, among others. Langdon suspects they are on the hunt for a breathtaking historical secret, one that has proven through the centuries to be as enlightening as it is dangerous. In a frantic race through Paris, and beyond,

*(continued on back flap)*

*(continued from front flap)*

Langdon and Neveu find themselves matching wits with a faceless powerbroker who appears to anticipate their every move. Unless they can decipher the labyrinthine puzzle, the Priory's secret—and an explosive ancient truth—will be lost forever.

Breaking the mold of traditional suspense novels, *The Da Vinci Code* is simultaneously lightning-paced, intelligent, and intricately layered with remarkable research and detail. From the opening pages to the unpredictable and stunning conclusion, bestselling author Dan Brown proves himself a master storyteller.

**http://www.randomhouse.com/doubleday/davinci/**

# Masih Steganography ...

- Isi sebuah iklan

  *Setelah engkau rasakan nikmatnya gula, hisap aroma rokok ini sampai engkau nyaman ingin nambah.*
  (Tugas dari Nur Alimah)

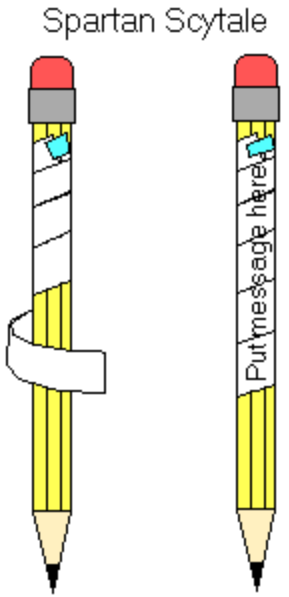
- Apa pesan sebenarnya?

# Cryptography

- Contoh transposition
  - Rail fence
  - Simple transposition:
    **pesan ditulis mendatar dikirimkan vertikal**
  - Spartan Scytale (5 BC)

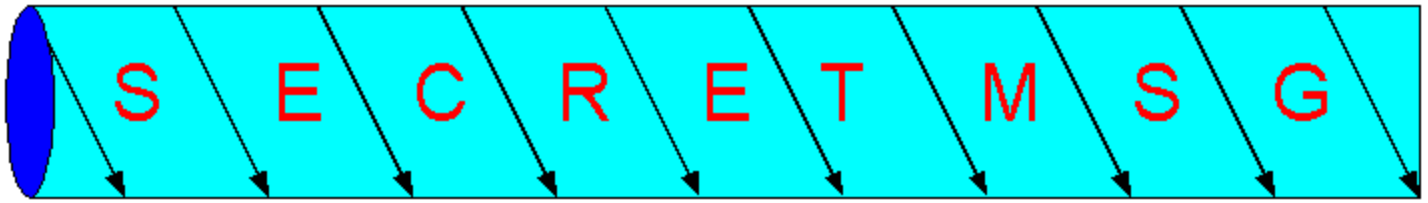
http://www.unmuseum.org/excoded.htm

```
asimplekin
doftranspo
sitionciph
erwritesth
emessagein
toarectang
lebyrowsan
dreadsitou
tbycolumns
```




http://en.wikibooks.org/wiki/Cryptography:Transposition_ciphers

http://www.ccisource.com/content/resources/articles/Jan01/symmetric.htm



# Cryptography

- Contoh substitution
  - Caesar cipher (geser 3 huruf)

```
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
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
```

```
BUDI = exgl
```

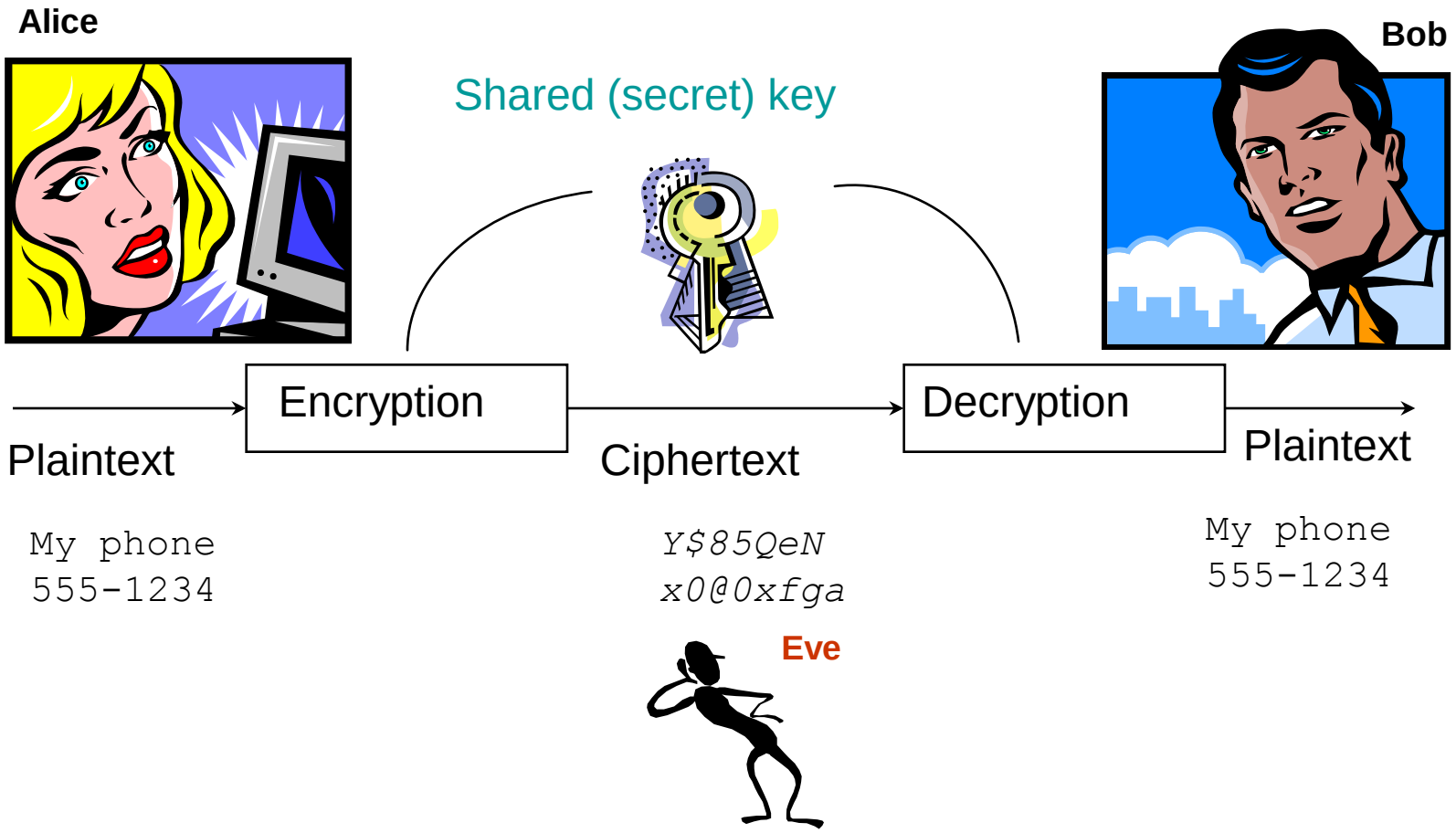
Tabel dapat digeser *n* huruf ke kiri atau ke kanan. *n* dan arah menjadi kunci

  - Enigma (rotor)
    - Digunakan Jerman pada perang dunia ke 2

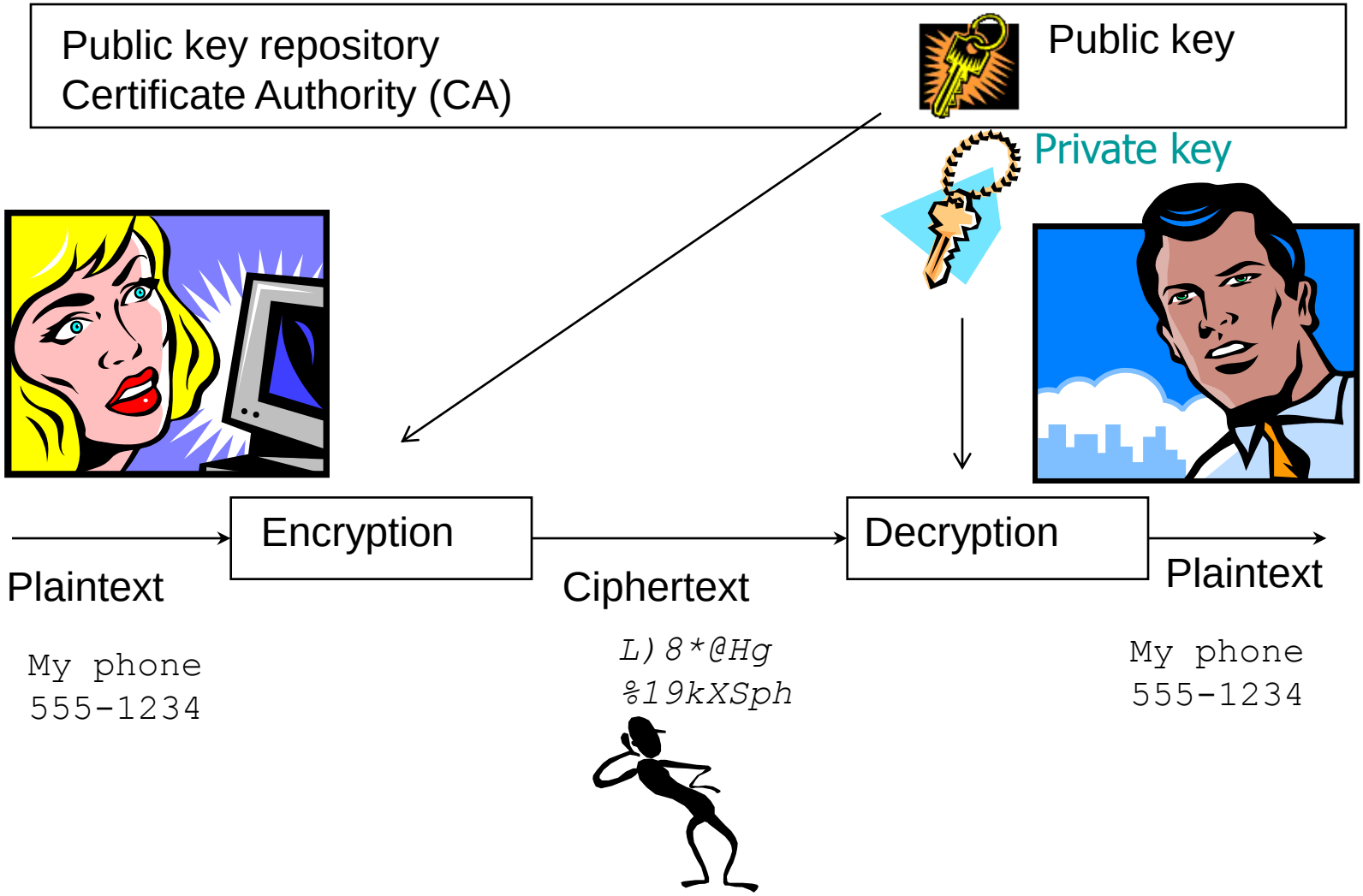
# Komponen Cryptography

- **Plain text**
  - Sumber berita/pesan/teks asli
- **Cipher text**
  - Teks yang sudah diproses (diacak, digantikan)
- **Algoritma & kunci**
  - Misal: subsitusi (algoritma) & number of shift (kunci)
  - Pemisahan alg & kunci ditemukan oleh Auguste Kerckhoffs von Niewenhof (1883)

# Private-key Cryptosystem



# Public-key Cryptosystem



# Penutup

- Masih kurang SDM Indonesia yang menguasai teknis pengamanan data
- Bergantung kepada negara lain! Sangat berbahaya