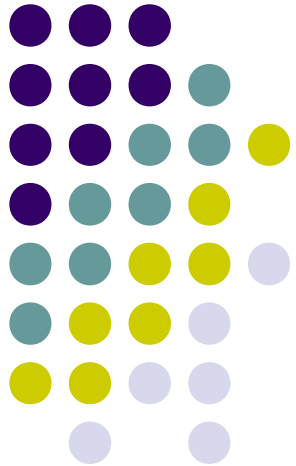
Mã hóa dữ liệu
(Cryptography)

Võ Viết Minh Nhật
Nguyễn Ngọc Thủy
Khoa CNTT – ĐHKH Huế

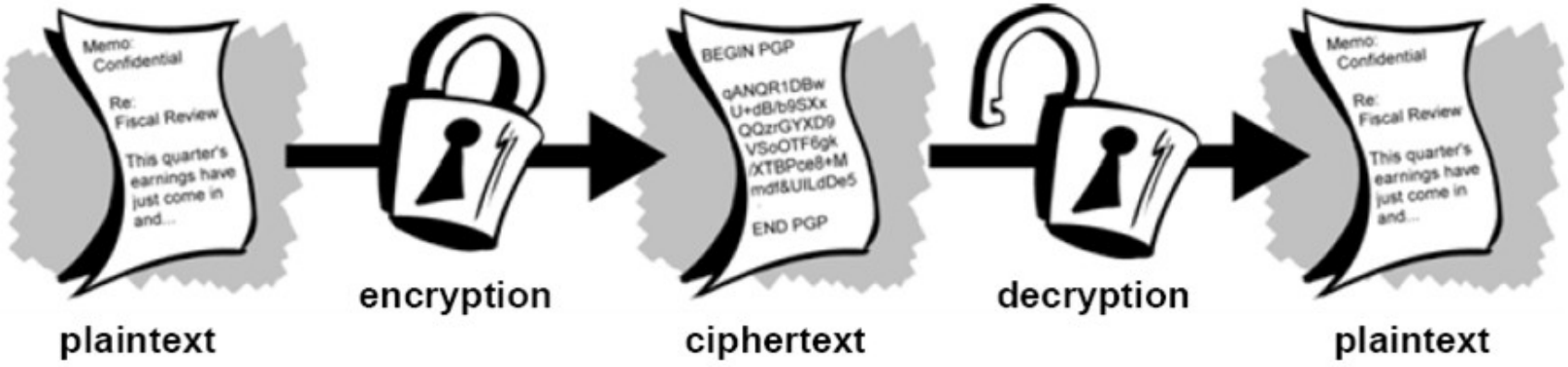


Nội dung trình bày

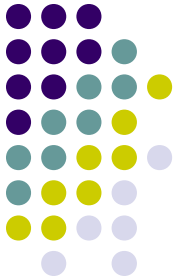
- Giới thiệu: Mã hóa và giải mã
- Các phương thức mã hóa
  - Mã hóa truyền thống
  - Mã hóa khóa công khai (public-key)
  - Mã hóa lai (hybrid)
  - Chữ ký số
- Kết luận

Giới thiệu: Mã hóa và giải mã

- Định nghĩa:
  - Mã hóa là khoa học dùng toán học để mã hóa và giải mã dữ liệu.
  - Mã hóa cho phép lưu trữ hay truyền thông tin một cách an toàn trên những mạng không an toàn (Internet) mà không bị đọc trộm.



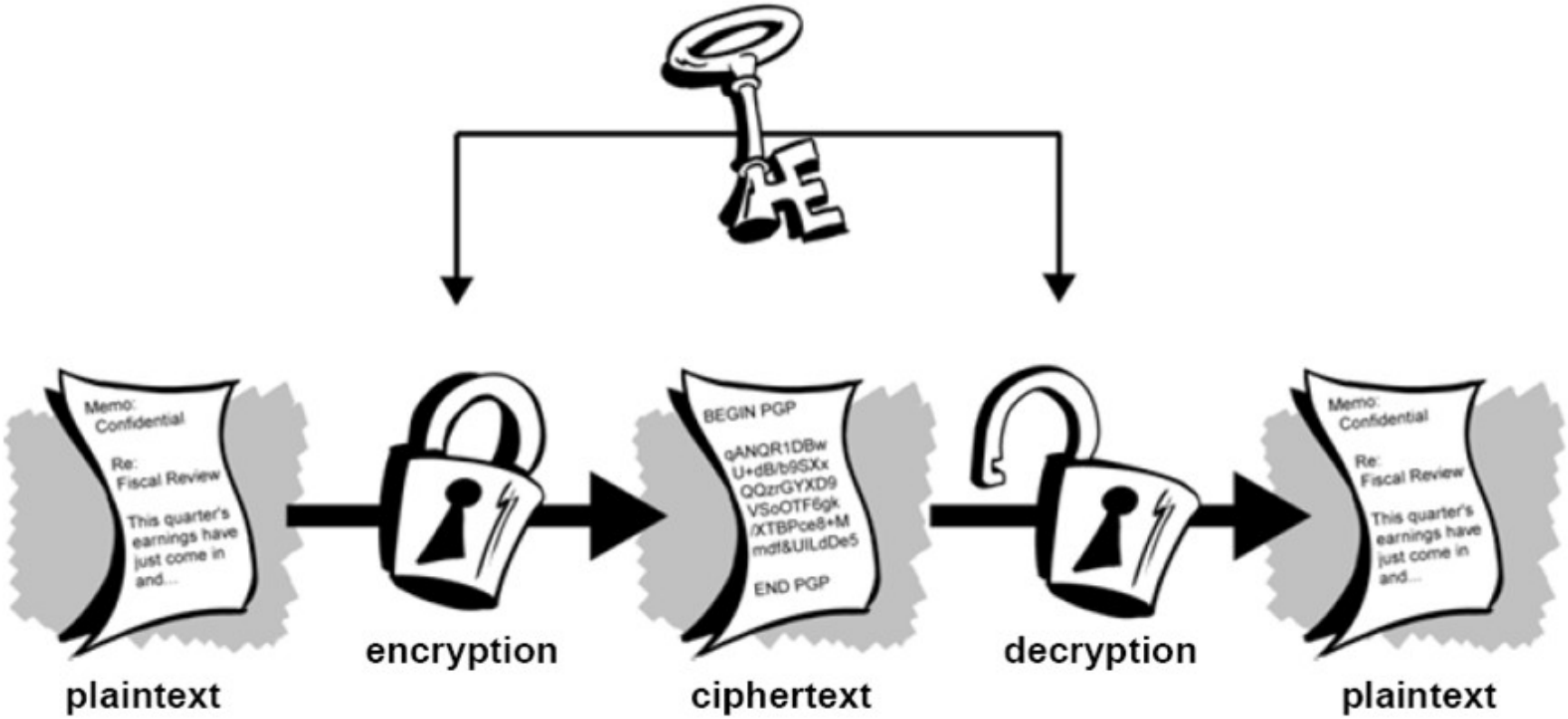
Giới thiệu (2)



- Độ khó của mã hóa:
  - được đo bằng thời gian và vật chất được yêu cầu để giải mã.
  - Độ khó = khả năng của máy tính hiện nay + Thời gian hợp lý
- Giải thuật mã hóa:
  - là một hàm toán học được sử dụng trong mã hóa và giải mã.
- Mã hóa / giải mã được thực hiện với một khóa (key)
  - Key = một từ, số, câu, ...
  - Cùng một thông tin được mã hóa với các khóa khác nhau sẽ cho ra các kết quả mã hóa khác nhau
  - Tính an toàn của thông tin phu thuộc vào độ khó của giải thuật và độ bí mật của khóa.
- Hệ thống mã hóa (cryptosystem) = giải thuật + khóa + qui trình

Mã hóa khóa bí mật

- Mã hóa khóa bí mật hay khóa đối xứng (cùng một khóa dùng để mã hóa và giải mã)

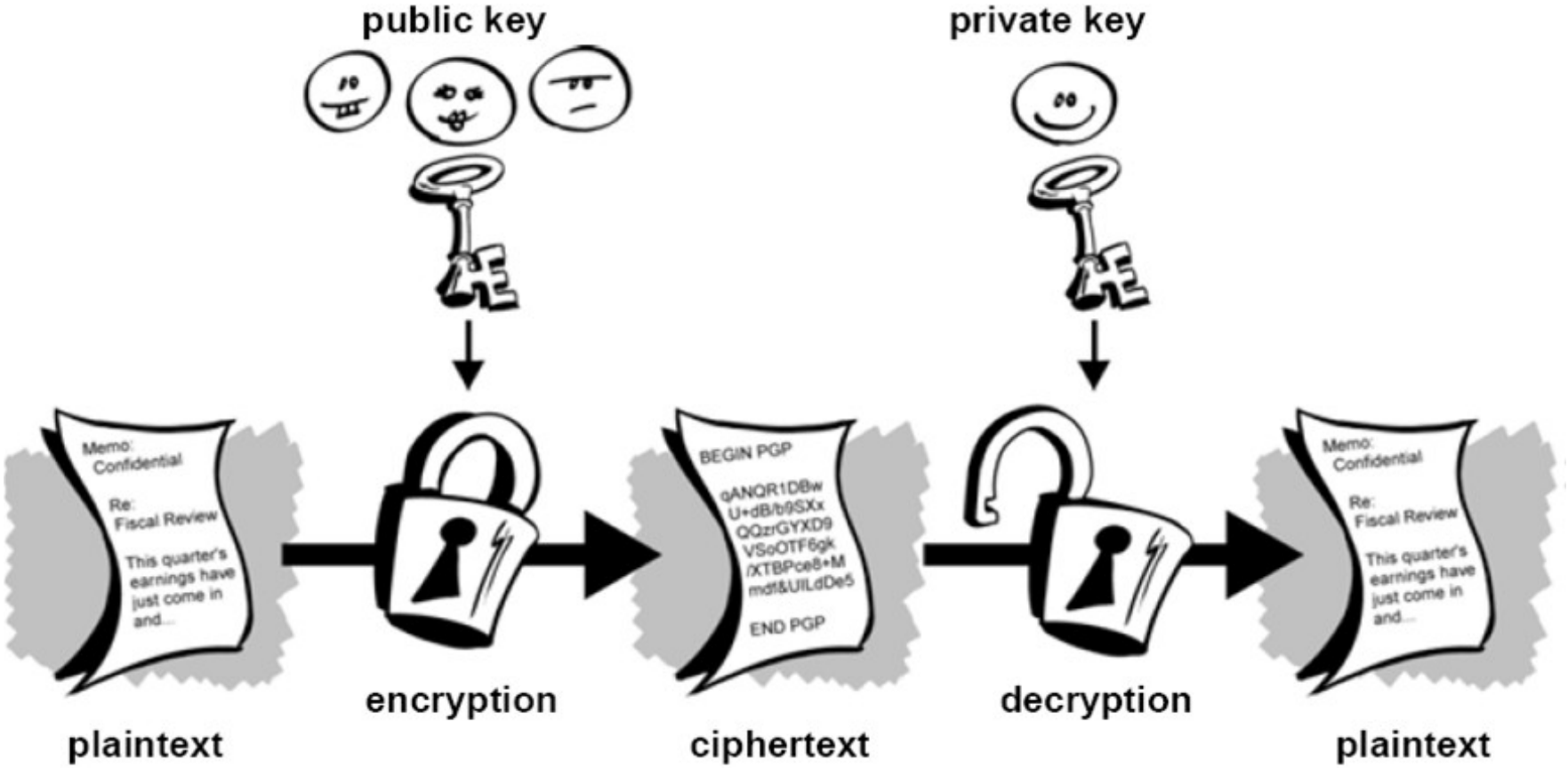


Mã hóa khóa bí mật

- Ví dụ: Mã hóa Caesar
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - DEFGHIJKLMNOPQRSTUVWXYZACB (dịch 3)
  - SECRET => VHFUHW
- Nhanh, nhưng không thích hợp trong việc truyền khóa.
- Người gởi và nhận phải cùng biết và giữ bí mật về khóa

Mã hóa khóa công khai

- Sử dụng một khóa công khai cho mã hóa và một khóa bí mật cho giải mã.

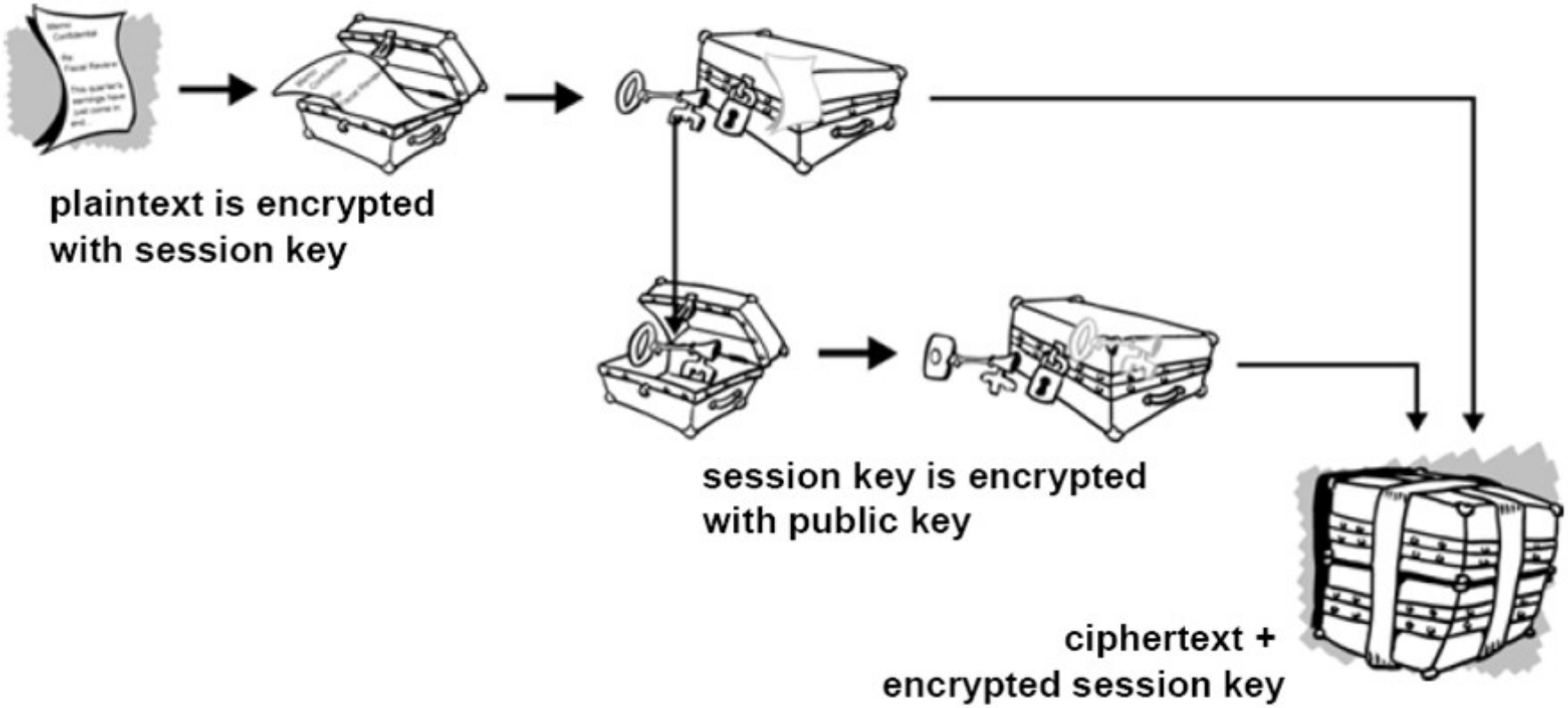


Mã hóa khóa công khai (1)

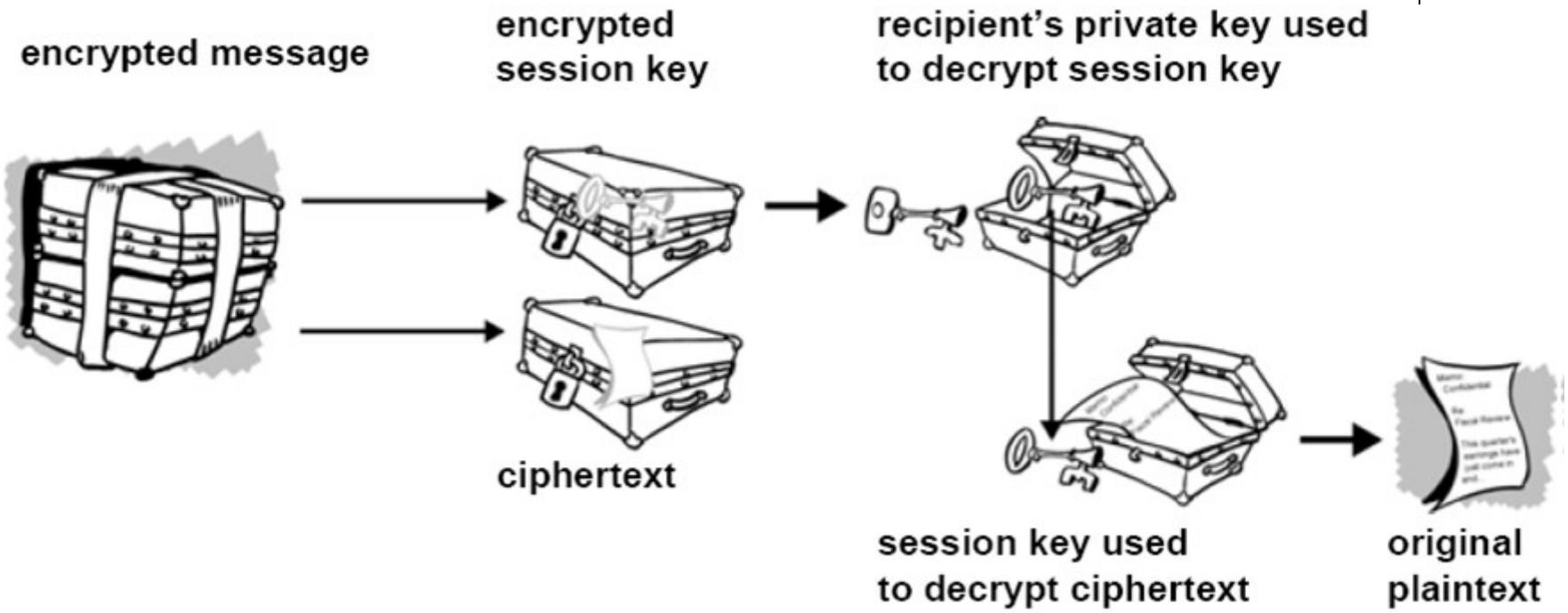
- Những người có khóa công khai có thể mã hóa thông tin, nhưng chỉ những người có khóa bí mật mới đọc được thông tin.
- Cho phép trao đổi thông tin an toàn hơn
- Người gởi và nhận có thể dùng một kênh riêng chỉ để trao đổi khóa bí mật.

Mã hóa lai

- Mã hóa lai = Mã hóa khóa bí mật + Mã hóa khóa công khai



Mã hóa lai (2)

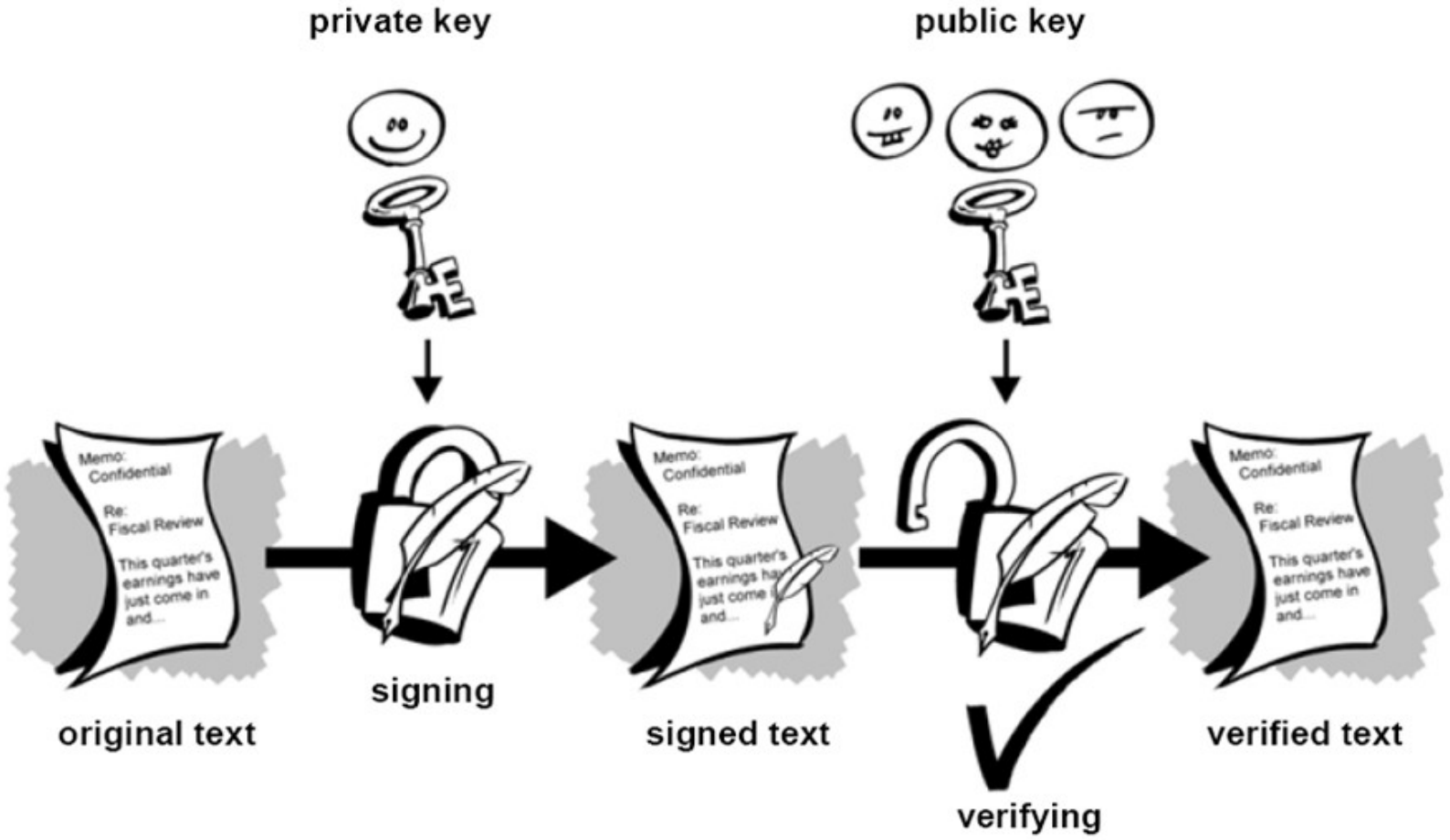


- Mã khóa lai đã kết hợp những ưu điểm của mã hóa khóa bí mật (nhanh gấp 1000 lần mã hóa khóa công khai) và của mã hóa khóa công khai (thuận tiện trong việc truyền khóa và dữ liệu)

Chữ ký số

- Mã hóa khóa công khai cung cấp một phương pháp cho việc sử dụng chữ ký số
- Chữ ký số sẽ được sử dụng như là khóa bí mật trong khi mã hóa thông tin
- Cho phép người nhận kiểm tra tính xác thực và tính nguyên vẹn của thông tin gốc
- Hơn chữ ký tay, chữ ký số ngăn chặn được việc giả mạo
- Tuy nhiên, mã hóa chữ ký số thực hiện chậm, tạo ra khối lượng dữ liệu lớn

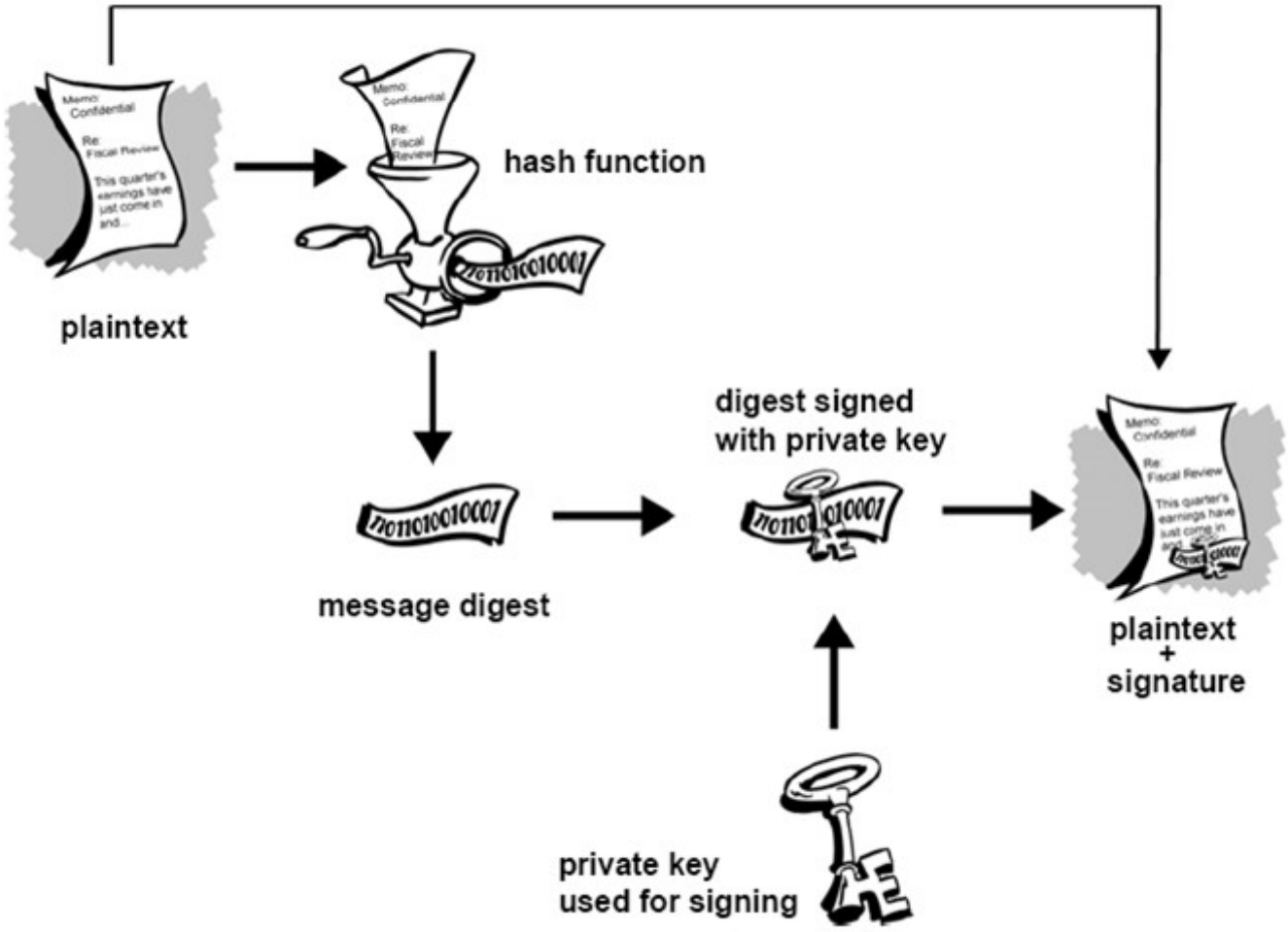
Chữ ký số (2)


private key
public key
Memo:
Confidential
Re:
Fiscal Review
This quarter's
earnings have
just come in
and...
signing
original text
signed text
verifying
verified text

Hàm băm

- Với thông tin vào có độ dài bất kỳ, hệ thống thực hiện băm ra thành những đoạn có độ dài cố định bằng nhau
- Khóa mã hóa được tạo ra dựa trên từng đoạn và khóa bí mật
- Các đoạn thông tin có thể được mã hóa hoặc không trước khi truyền qua mạng
- Chỉ người nhận có khóa mã hóa mới giải mã được các đoạn thông tin

Hàm băm (2)


plaintext
hash function
message digest
digest signed
with private key
plaintext
+
signature
private key
used for signing

Kết luận