CRYPTOGRAPHY

Lesson # 5

Introduction of Cryptography

- The method of hiding plaintext in such a way as to hide its substance is called encryption.
- Encrypting plaintext results in unreadable gibberish called cipher text

Origin

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the “shift by 3” rule could decipher his messages.

Caesar's Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get

DEFGHIJKLMNOPQRSTUVWXYZABC

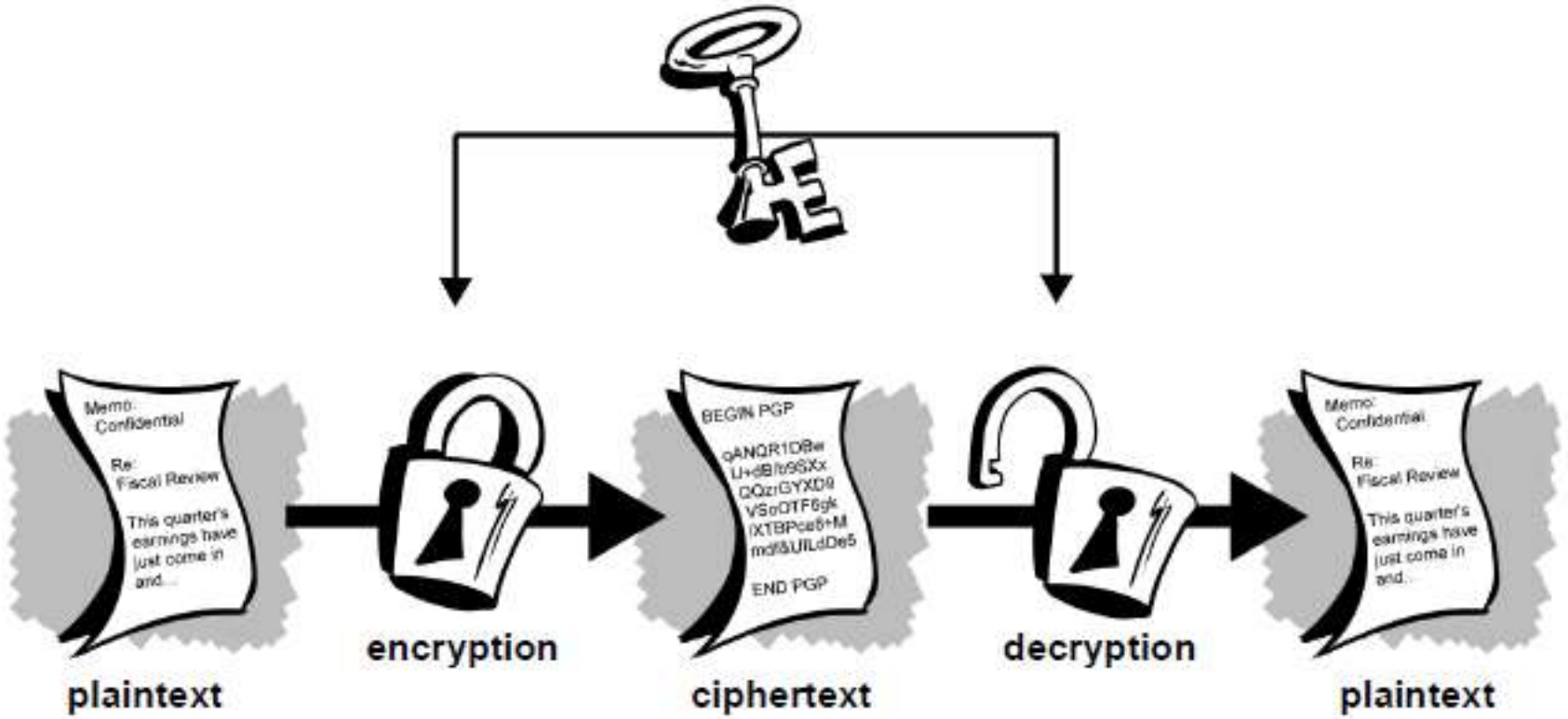
where D=A, E=B, F=C, and so on.

"SECRET" encrypts as "VHFUHW

Examples

CONVENTIONAL CRYPTOGRAPHY

Conventional cryptography



Conventional cryptography

- It is very fast. It is especially useful for encrypting data that is not going anywhere.

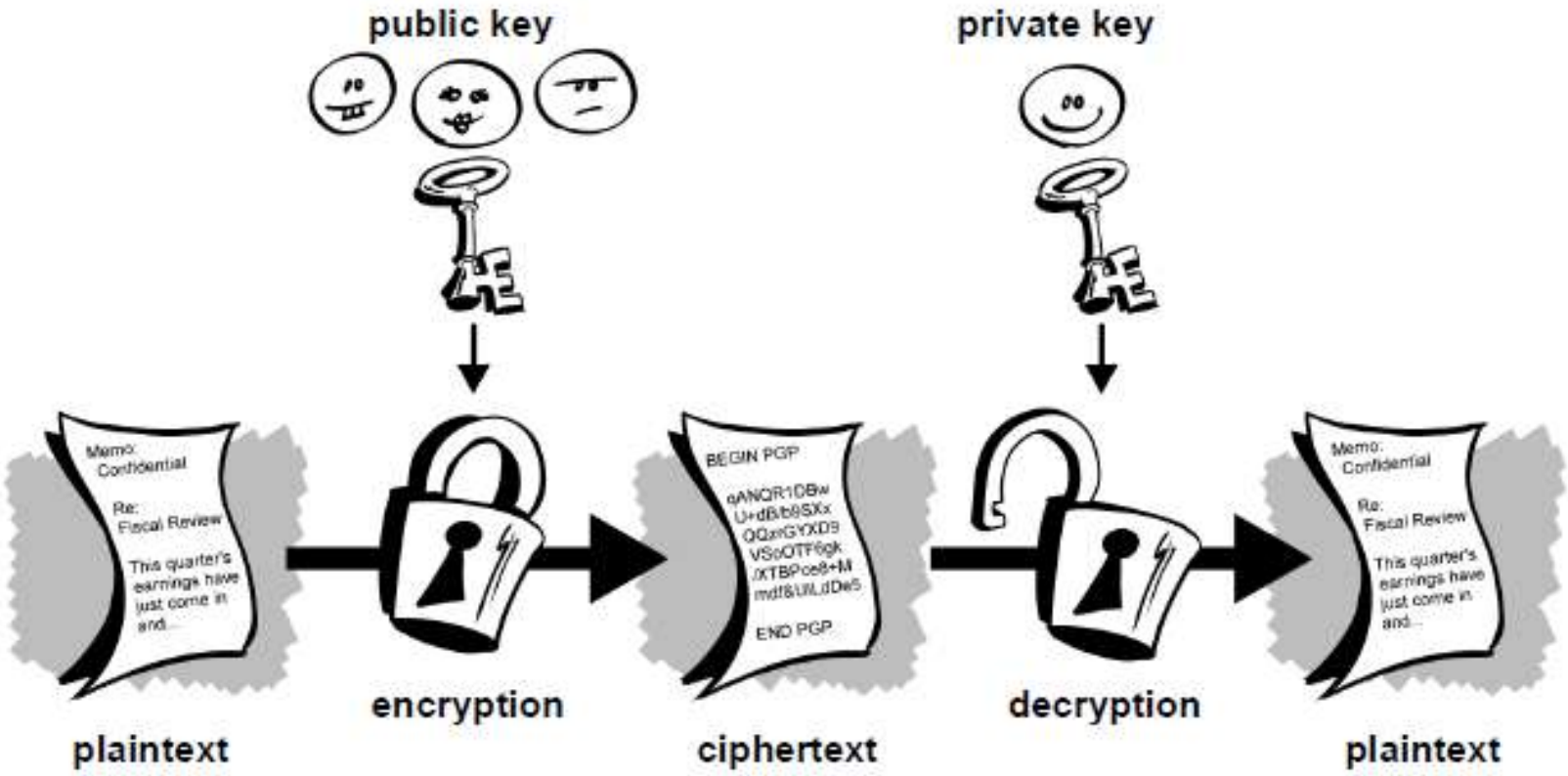
BUT

Key Management

- Both ends must agree upon a key and keep it secret between themselves.
- Being on different physical locations, they must trust a courier (secure communication medium) to prevent the disclosure of the secret key.
- Anyone who overhears or intercepts the key in transit can later read, modify, and forge all information encrypted or authenticated with that key

PUBLIC KEY CRYPTOGRAPHY

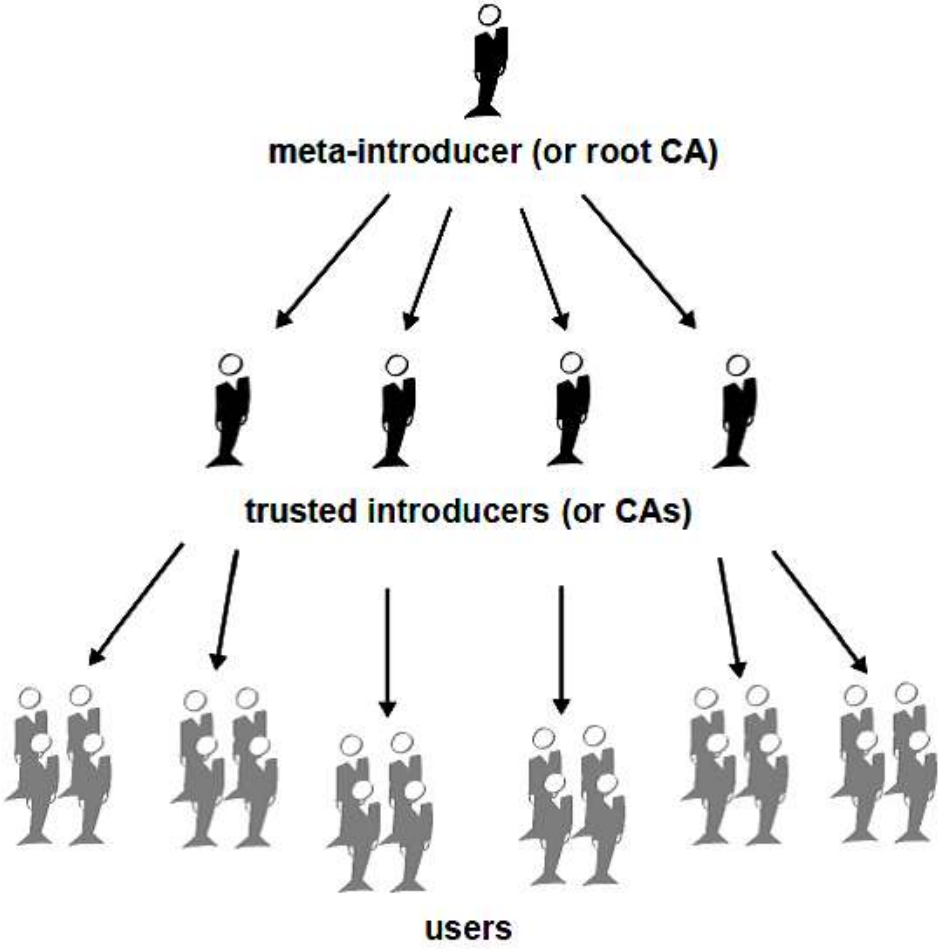
Public key cryptography



Certificate Management and Distribution

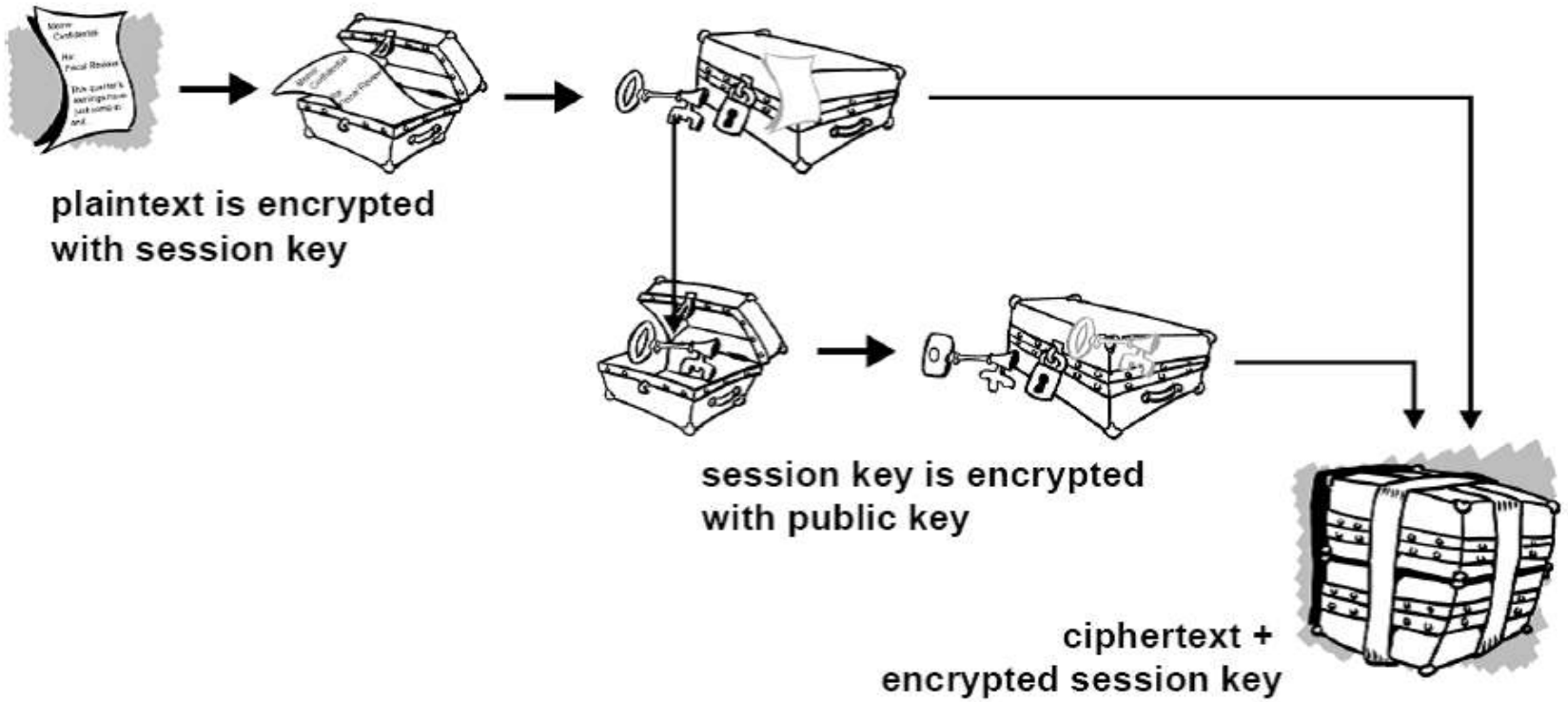
- Public Key Infrastructures
- Certification Authority, or CA
  - CA is authorized to issue certificates to its computer users. (ACA's role is analogous to a country's government's Passport Office.)

Certificate Management and Distribution



HYBRID APPROACH

Hybrid Approach



Hybrid Approach