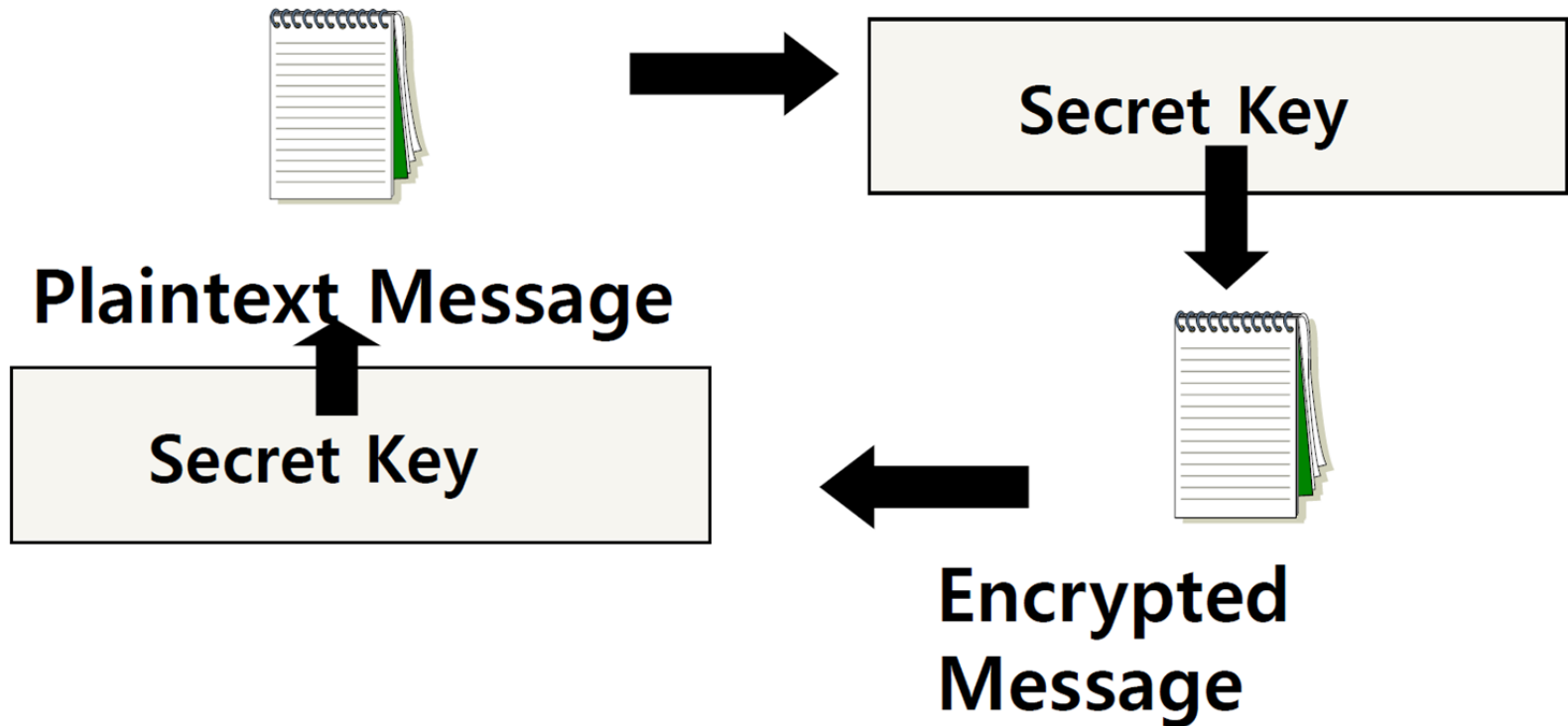# Signatures

CS 35L
Section 7: Thursday

Spring 2020

Slides adapted from Tyler Davis
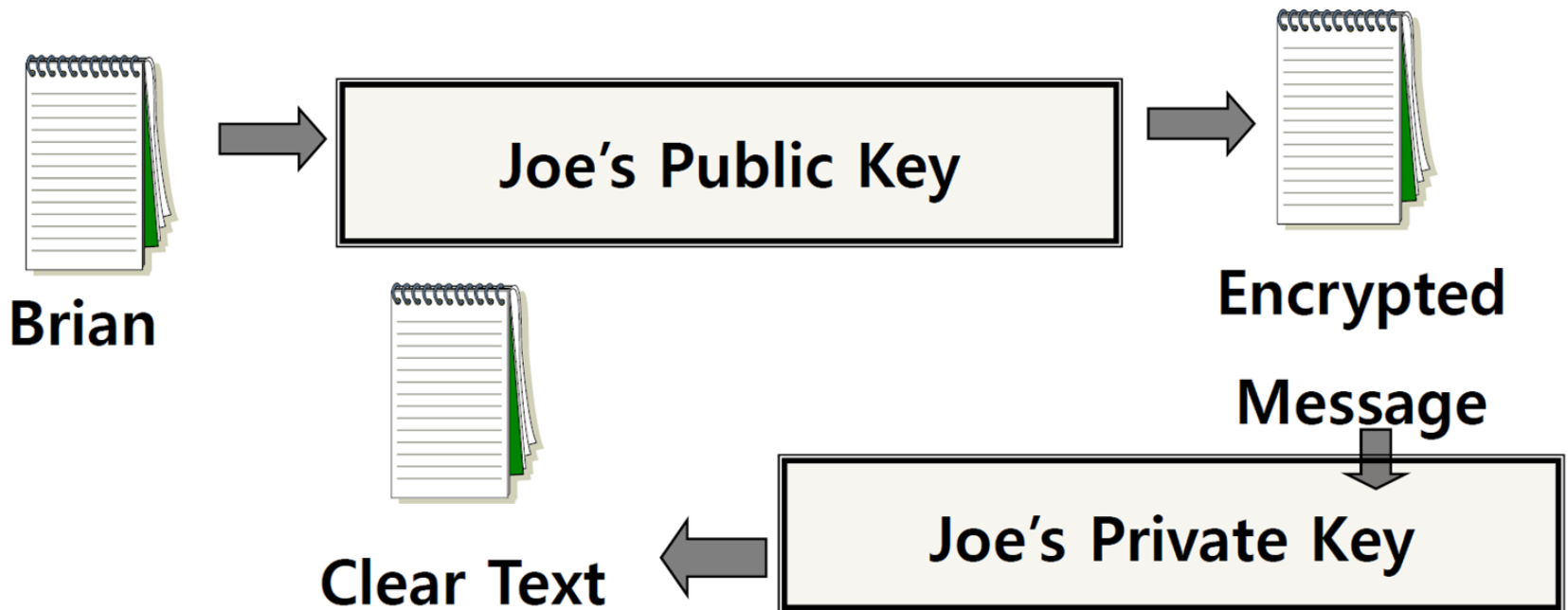
Secret Key (symmetric) Cryptography

- A single key is used to both encrypt and decrypt a message

Plaintext Message

Secret Key

Secret Key

Encrypted Message

Public Key (asymmetric) Cryptography

- Two keys are used: a public and a private key. If a message is encrypted with one key, it has to be decrypted with the other.

Digital Signature

- An electronic stamp or seal
  - almost exactly like a written signature, except more guarantees!
- Is appended to a document
  - Or sent separately (detached signature)
- Ensures data integrity
  - document was not changed during transmission

# Steps for Generating a Digital Signature

SENDER:

1) Generate a *Message Digest*
   - The message digest is generated using a set of hashing algorithms
   - A message digest is a 'summary' of the message we are going to transmit
   - Even the slightest change in the message produces a different digest
2) Create a Digital Signature
   - The message digest is encrypted using the sender's *private* key. The resulting encrypted message digest is the *digital signature*
3) Attach digital signature to message and send to receiver

Steps for Generating a Digital Signature

RECEIVER:

1) Recover the *Message Digest*
   – Decrypt the digital signature using the sender's public key to obtain the message digest generated by the sender
2) Generate the Message Digest
   – Use the same message digest algorithm used by the sender to generate a message digest of the received message
3) Compare digests (the one sent by the sender as a digital signature, and the one generated by the receiver)
   – If they are not *exactly the same* => the message has been tampered with by a third party
   – We can be sure that the digital signature was sent by the sender (and not by a malicious user) because *only* the sender's public key can decrypt the digital signature and that public key is proven to be the sender's through the certificate.
   – If decrypting using the public key renders a faulty message digest, this means that either the message or the message digest are not exactly what the sender sent.

Digital Signature

Image Source : gdp.globus.org
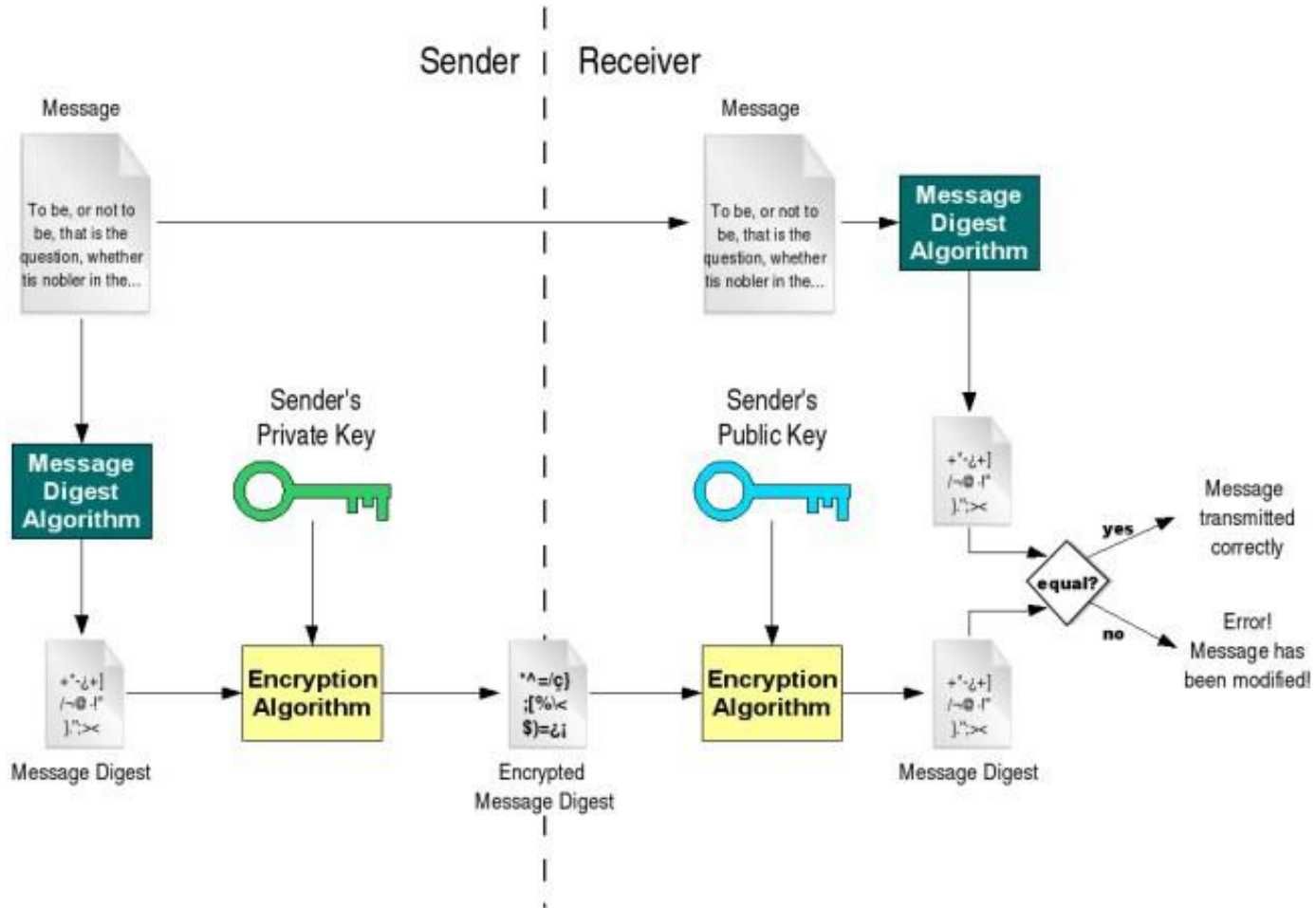
Detached Signature

- Digital signatures can either be *attached* to the message or *detached*

- A detached signature is stored and transmitted separately from the message it signs

- Commonly used to validate software distributed in compressed tar files

- You can't sign such a file internally without altering its contents, so the signature is created in a separate file