# Public and Private Key
# Encrypt/Decrypt with which Key?
# Who is Authenticated?

**Public and Private Key**
**Encrypt/Decrypt with which Key?**
**Who is Authenticated?**

When sender **encrypts with sender's private key**,
and receiver **decrypts with sender's public key**,
Then _____ is authenticated.

**Public and Private Key**
**Encrypt/Decrypt with which Key?**
**Who is Authenticated?**

When sender **encrypts with sender's private key**,
and receiver **decrypts with sender's public key**,
Then **Sender** is authenticated.

**Public and Private Key**
**Encrypt/Decrypt with which Key?**
**Who is Authenticated?**

When sender **encrypts with sender's private key**,
and receiver **decrypts with sender's public key**,
Then **Sender** is authenticated.

When sender **encrypts with receiver's public key**,
and receiver **decrypts with receiver's private key**,
Then _____ is authenticated.

**Public and Private Key**
**Encrypt/Decrypt with which Key?**
**Who is Authenticated?**

When sender **encrypts with sender's private key**,
and receiver **decrypts with sender's public key**,
Then **Sender** is authenticated.

When sender **encrypts with receiver's public key**,
and receiver **decrypts with receiver's private key**,
Then **Receiver** is authenticated.

The entity that owns the private key
is the entity that is authenticated

# Disseminating Symmetric Keys using Asymmetric Cryptography

## (also used for digital signatures)

# Disseminating Symmetric Keys using Asymmetric Cryptography

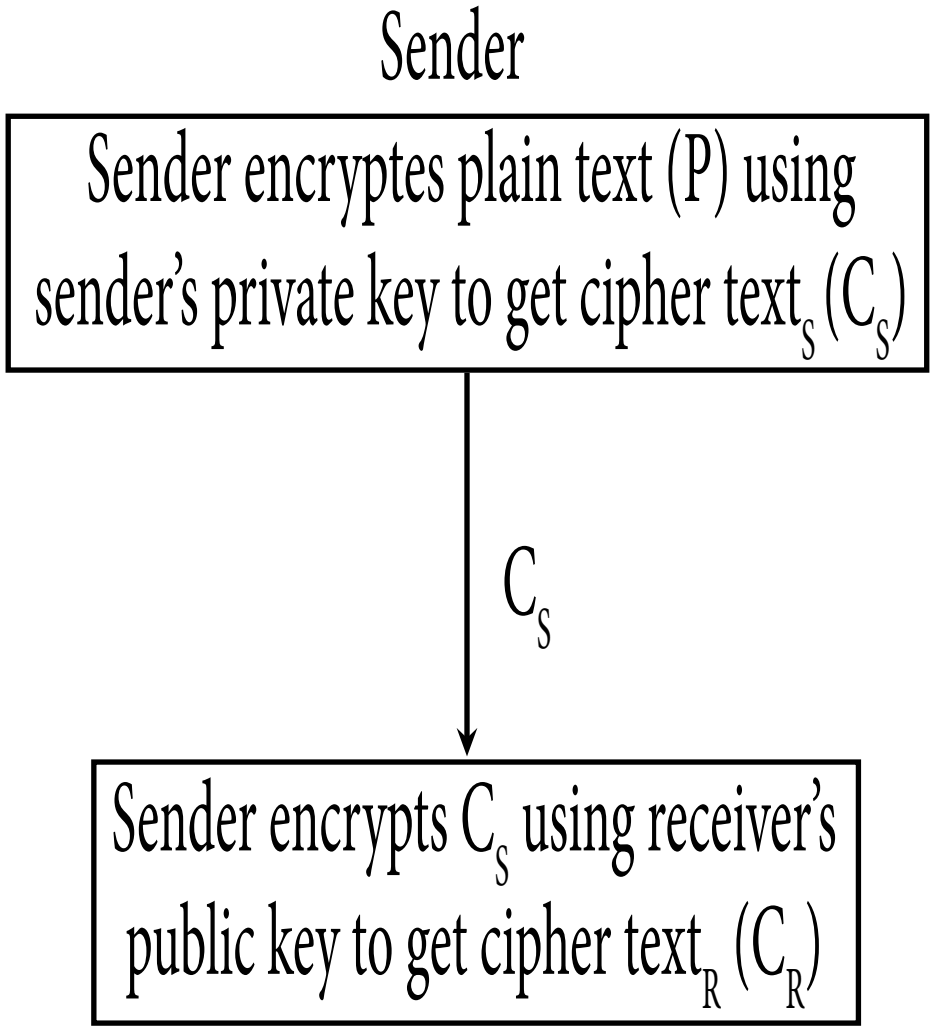
**(also used for digital signatures)**

Sender

Sender encryptes plain text (P) using sender's private key to get cipher text$_s$ ($C_s$)

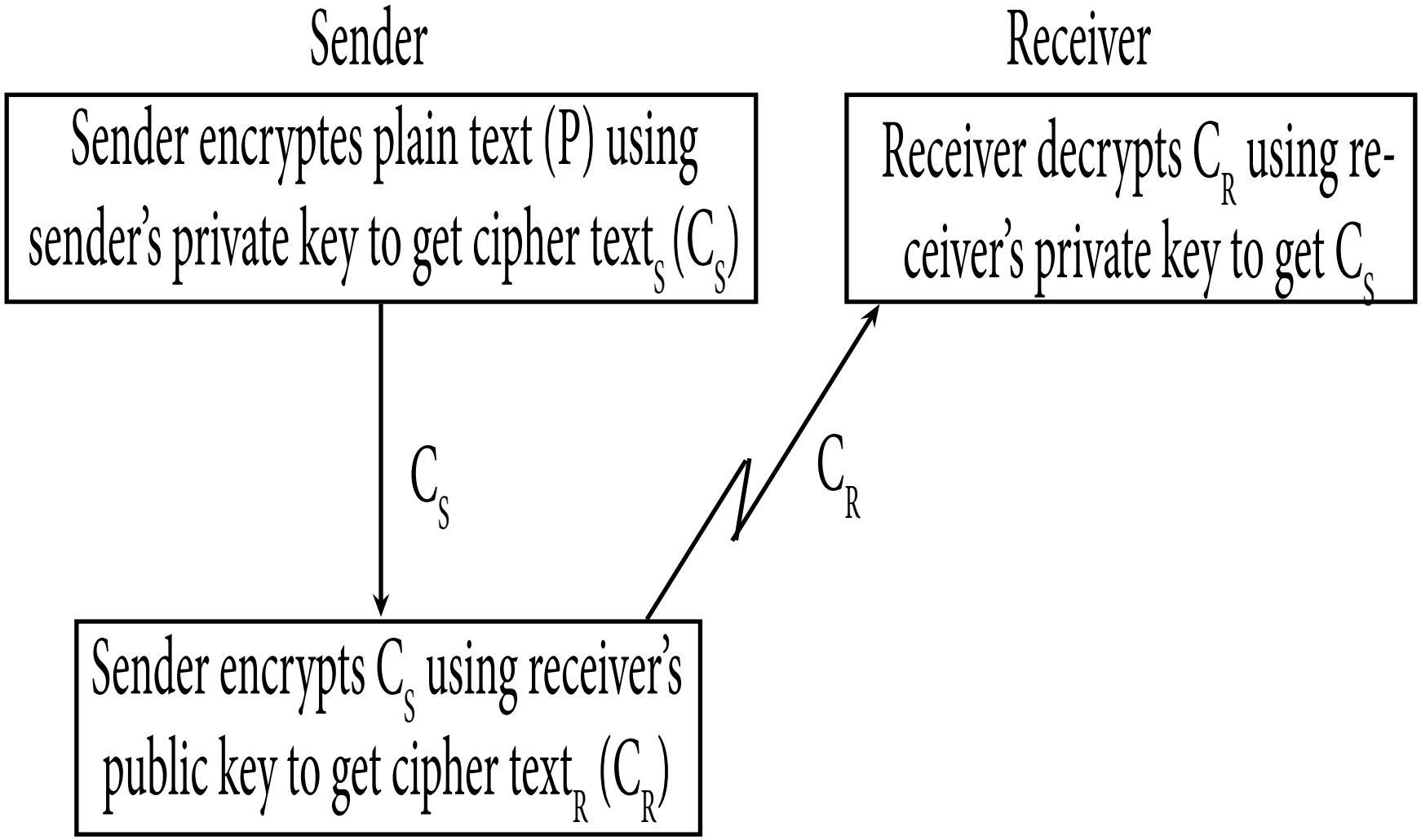
# Disseminating Symmetric Keys using Asymmetric Cryptography

**(also used for digital signatures)**



# Disseminating Symmetric Keys using Asymmetric Cryptography

**(also used for digital signatures)**



# Disseminating Symmetric Keys using Asymmetric Cryptography

**(also used for digital signatures)**