

**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 encrypts plain text (P) using  
sender's private key to get cipher text<sub>s</sub> (C<sub>s</sub>)

# Disseminating Symmetric Keys using Asymmetric Cryptography

(also used for digital signatures)

Sender

Sender encrypts plain text (P) using  
sender's private key to get cipher text<sub>s</sub> ( $C_s$ )

$C_s$

Sender encrypts  $C_s$  using receiver's  
public key to get cipher text<sub>R</sub> ( $C_R$ )



# Disseminating Symmetric Keys using Asymmetric Cryptography

(also used for digital signatures)

Sender

Receiver

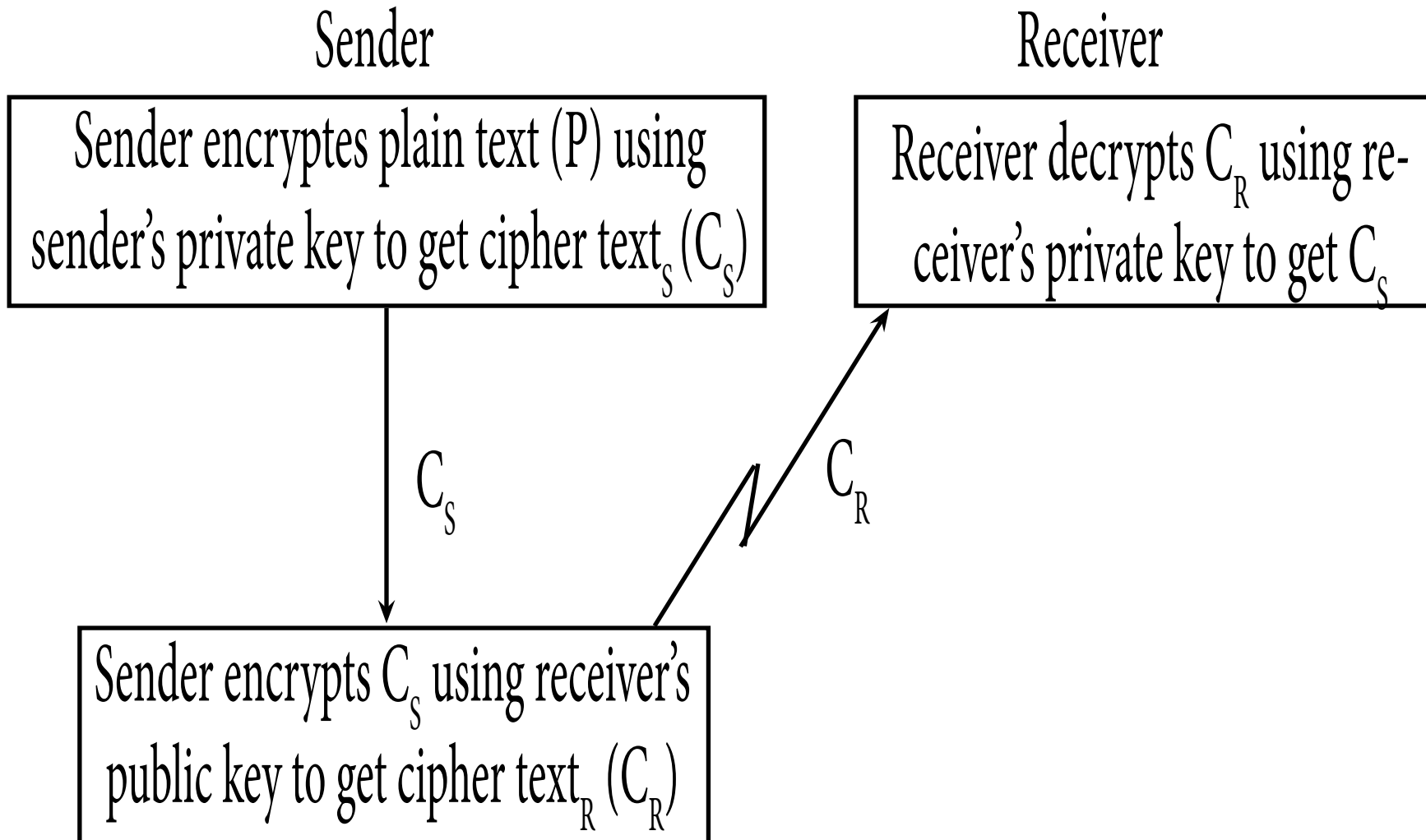
Sender encrypts plain text (P) using sender's private key to get cipher text<sub>s</sub> ( $C_s$ )

Receiver decrypts  $C_R$  using receiver's private key to get  $C_s$

$C_s$

$C_R$

Sender encrypts  $C_s$  using receiver's public key to get cipher text<sub>R</sub> ( $C_R$ )



# Disseminating Symmetric Keys using Asymmetric Cryptography (also used for digital signatures)

Sender

Receiver

Sender encrypts plain text (P) using sender's private key to get cipher text<sub>s</sub> ( $C_s$ )

Receiver decrypts  $C_R$  using receiver's private key to get  $C_s$

$C_s$

$C_R$

$C_s$

Sender encrypts  $C_s$  using receiver's public key to get cipher text<sub>R</sub> ( $C_R$ )

Receiver decrypts  $C_s$  using sender's public key to get the plain text P

