Seguridad en sistemas distribuidos

1. Introducción
2. Amenazas y ataques
3. Políticas de seguridad
4. Mecanismos de seguridad
5. Ejemplo de servicio de seguridad: Kerberos

Bibliografía:

[COU05] Cap. 7

[TAN02] Cap. 8

1 Introducción

- **Políticas de seguridad**: establecen límites definidos en la compartición de recursos. Independientes de la tecnología.
- **Mecanismos de seguridad**: cómo se implementan las políticas. Conjunto de técnicas dependientes de la tecnología.

2 Amenazas y ataques

Amenazas (Pfleeger, 1997)

- **Intercepción**. Escucha de mensajes, ...
- **Interrupción**. Retardo de mensajes, denegación del servicio, ...
- **Modificación**. Alteración o corrupción de mensajes, ...
- **Fabricación**. Suplantación de identidad, ...

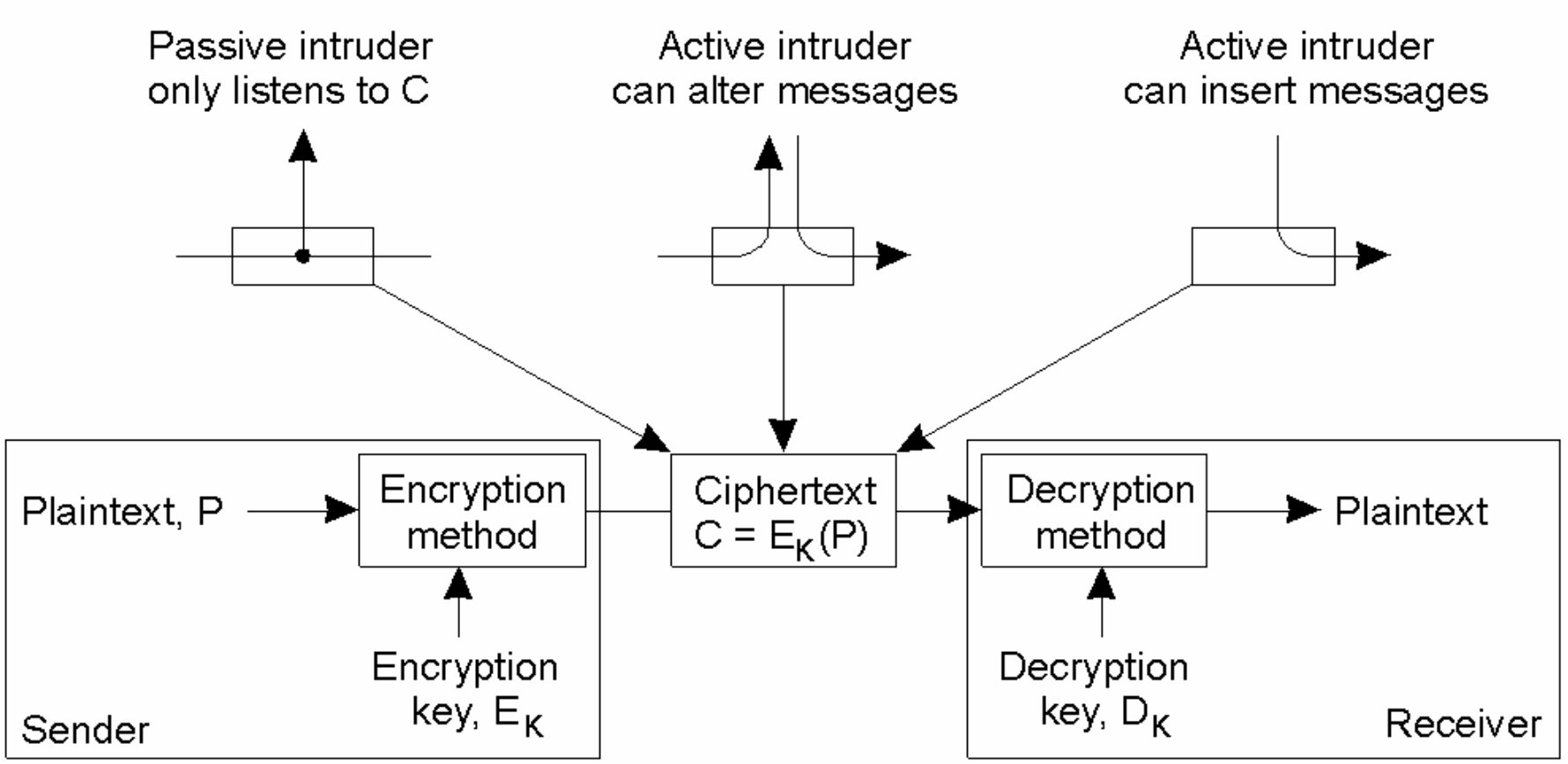
3 Políticas de seguridad

- **Confidencialidad**
  - La información estará disponible sólo para los sujetos autorizados.
- **Integridad**
  - Las modificaciones de la información sólo se realizarán por los sujetos autorizados.

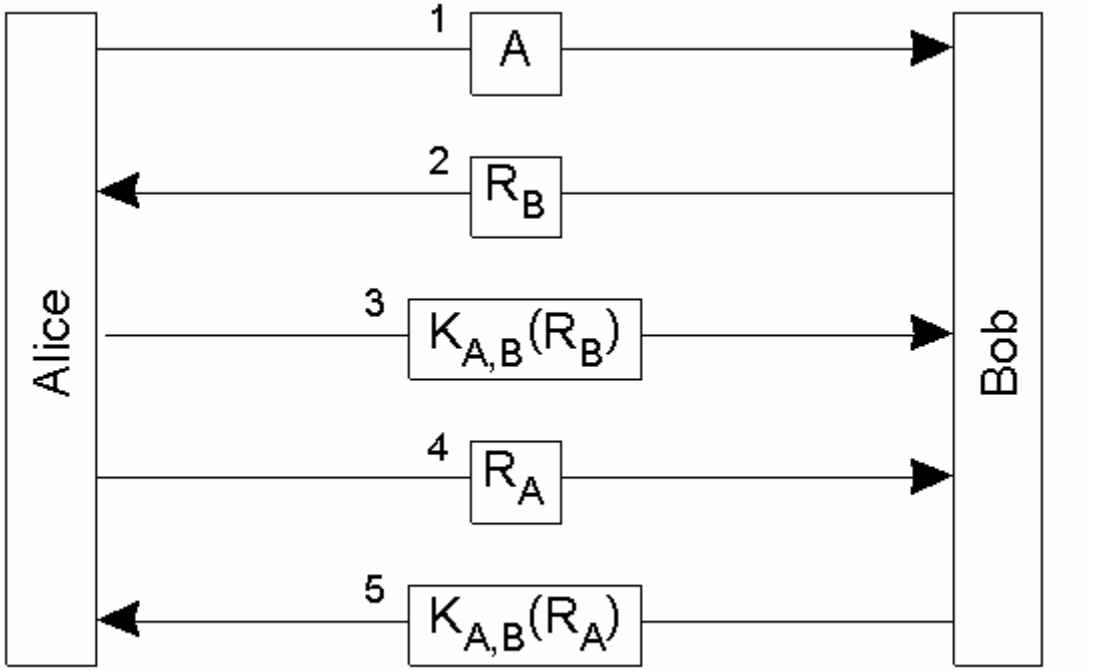
4 Mecanismos de seguridad

- Cifrado
  - Simétrico (clave secreta)
  - Asimétrico (par de claves pública y privada)
- Autenticación
  - Passwords
  - Protocolos de reto-respuesta.
- Autorización
  - Listas de control de accesos, Credenciales
  - Firewalls
- Auditoría
  - Mantenimiento y análisis de trazas (*logs*)

Cifrado [TAN02]

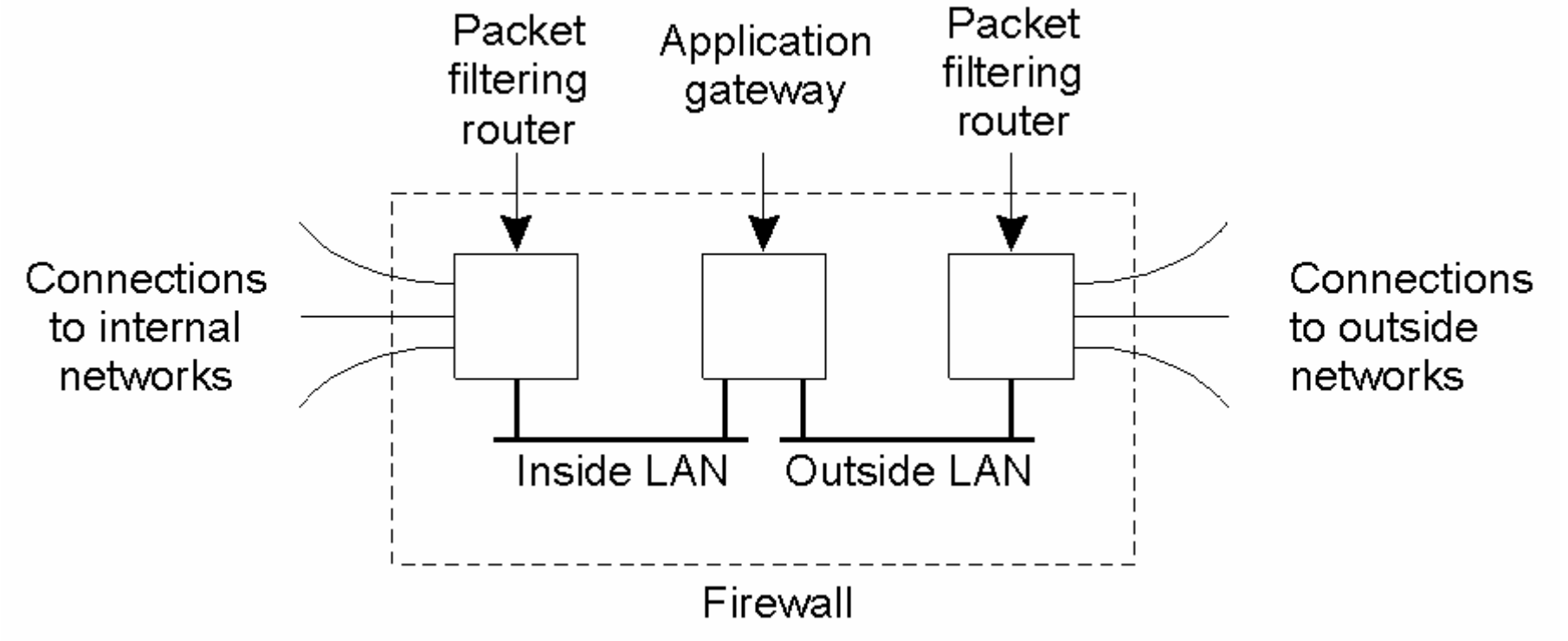


Autenticación [TAN02]
Protocolos de reto-respuesta



Authentication based on a shared secret key.

Autorización [TAN02]
Firewalls



A common implementation of a firewall.

5 Kerberos

- Incluye mecanismos de autenticación y otras herramientas de seguridad.
- Desarrollado en el MIT, años 80.
- Uso muy extendido en la actualidad (DCE, NFS, AFS-3, Windows2000).
- Existe versión de código fuente disponible (www.mit.edu).

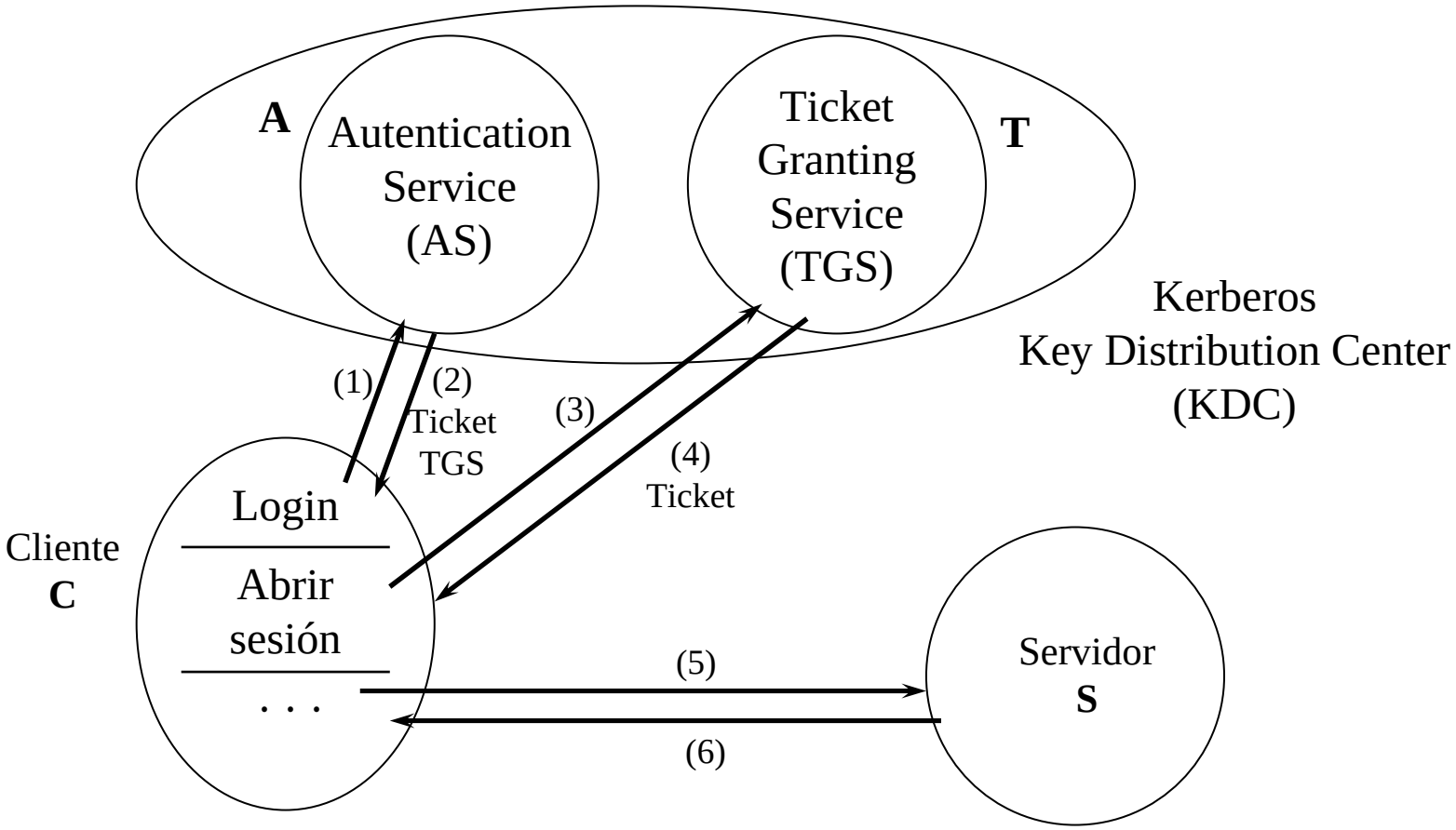
5 Kerberos
Servicios

- Un **Key Distribution Centre** con dos servicios:
  - **Servicio de autenticación (AS)**. Autentica a los clientes en el login y expide tickets para el acceso al TGS.
  - **Servicio de expedición de tickets (TGS)**. Expide tickets y claves de sesión para el acceso de los clientes a servicios específicos.

5 Kerberos
Objetos de seguridad

- **Tickets**: expedidos por el TGS para el acceso de un cliente a un servicio determinado con un plazo de expiración.
- **Autenticaciones**: las construye un cliente con su identidad y una marca de tiempos (cifrados) para un solo uso en una comunicación con un servidor.
- **Clave de sesión**: clave secreta, expedida por el AS, que se incluye en el ticket del cliente y es usada por un servidor para descifrar la autenticación.

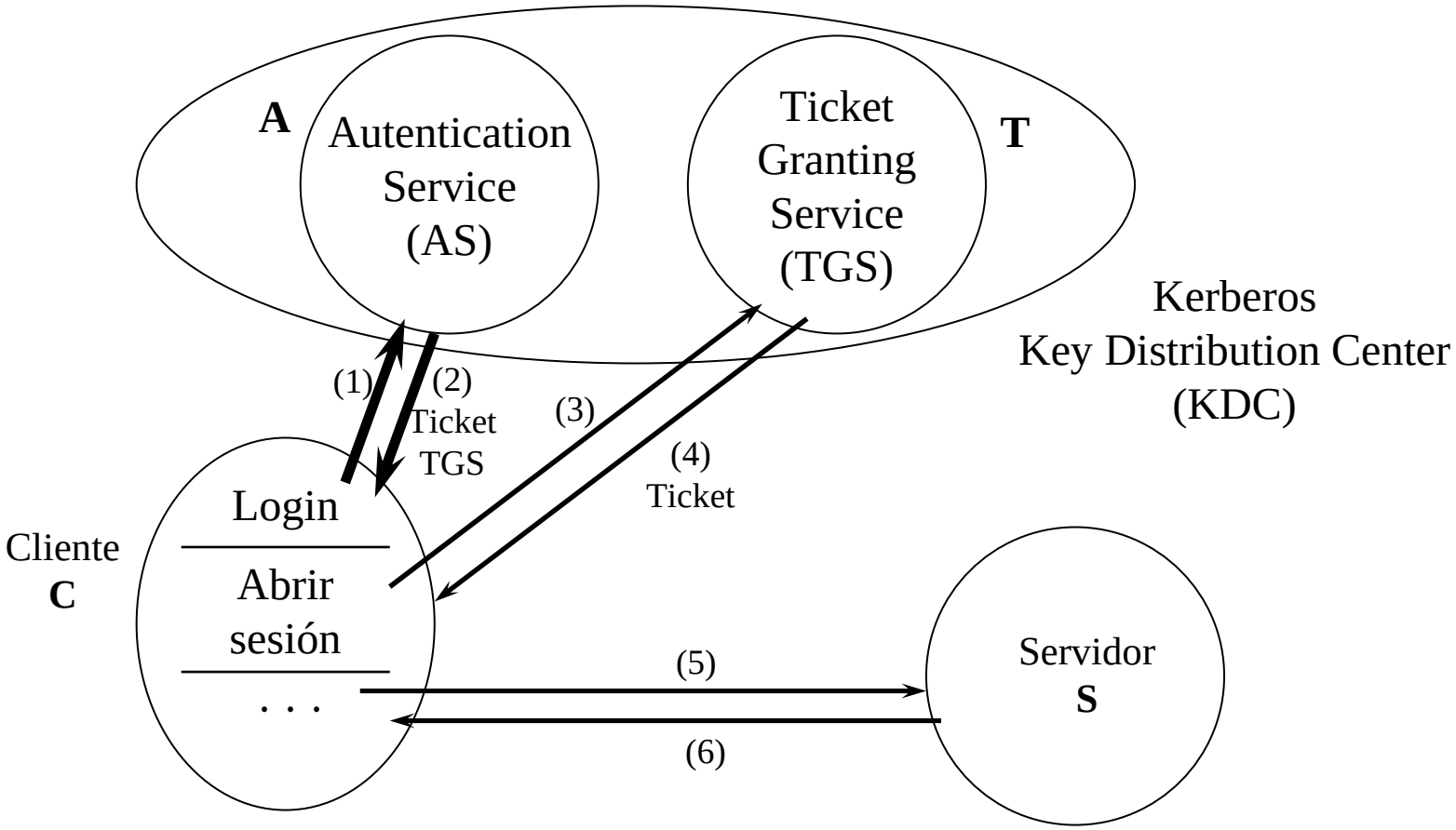
5 Kerberos
Arquitectura



5 Kerberos
Notación

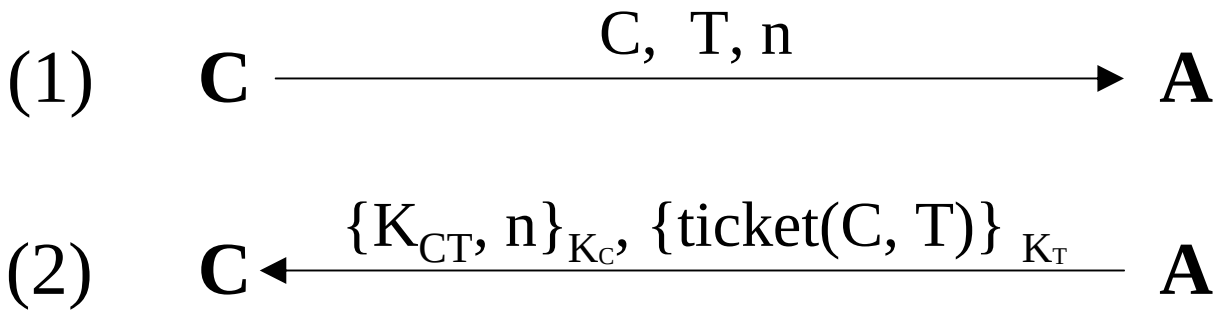
- $\{M\}_k$: mensaje M cifrado con clave K
- K_C: clave del cliente C
- *ticket*(C, S) = (C, S, t_1, t_2, K_{CS})
  - t_1: comienzo del periodo de validez del ticket
  - t_2: final del periodo de validez del ticket
  - K_{CS} : clave de sesión entre C y S (generada aleatoriamente)
- *autent*(C) = (C, t)
  - t: marca de tiempo
- n: contraste para identificar un mensaje
- A: nombre del AS
- T: nombre del TGS
- K_T: clave de T

5 Kerberos
Arquitectura



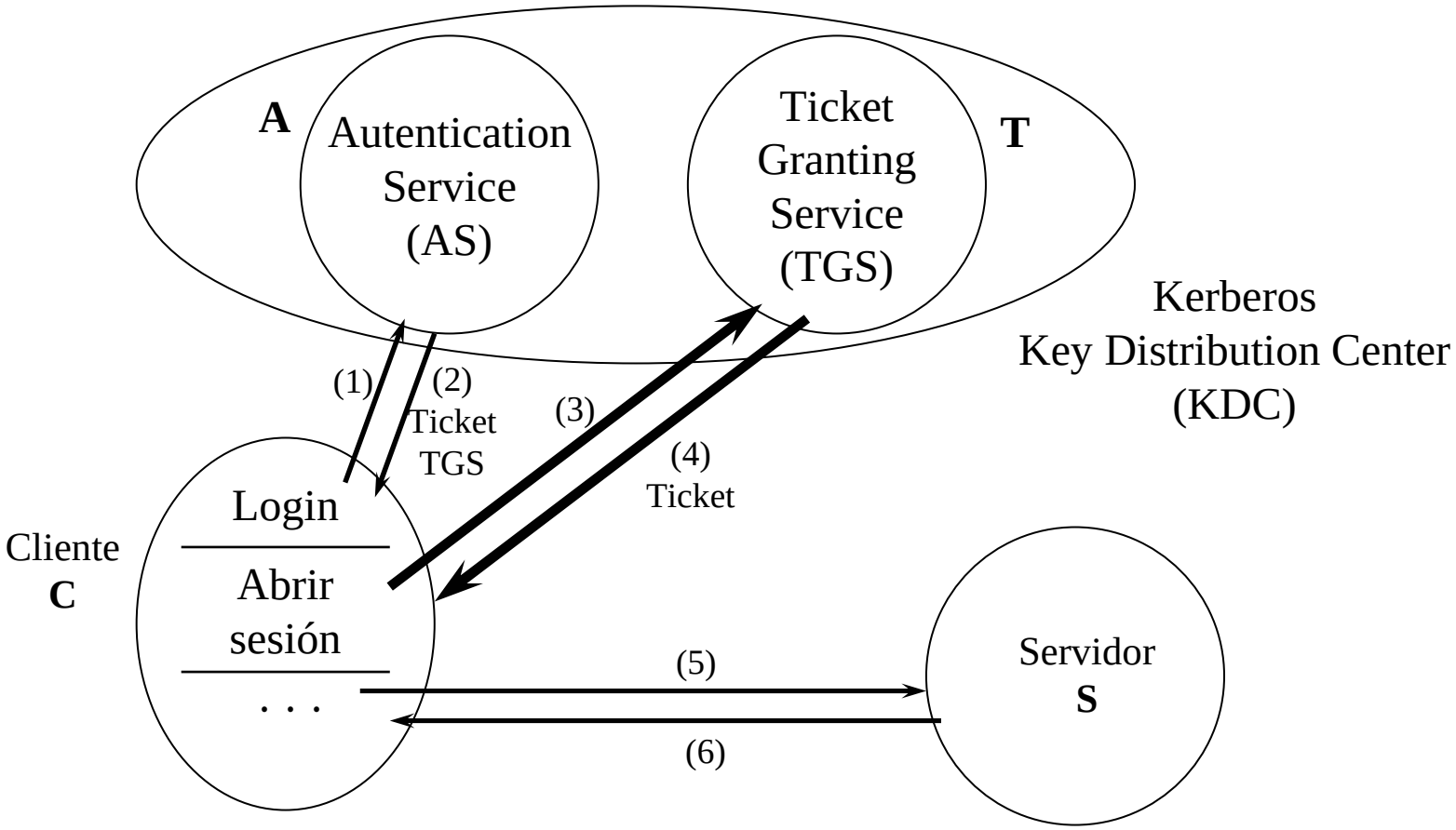
5 Kerberos
Protocolo (paso A)

Login: obtención de una clave de sesión y un ticket TGS



El cliente debe ser capaz de descifrar el mensaje (2), que está cifrado con su clave secreta K_C.

5 Kerberos
Arquitectura



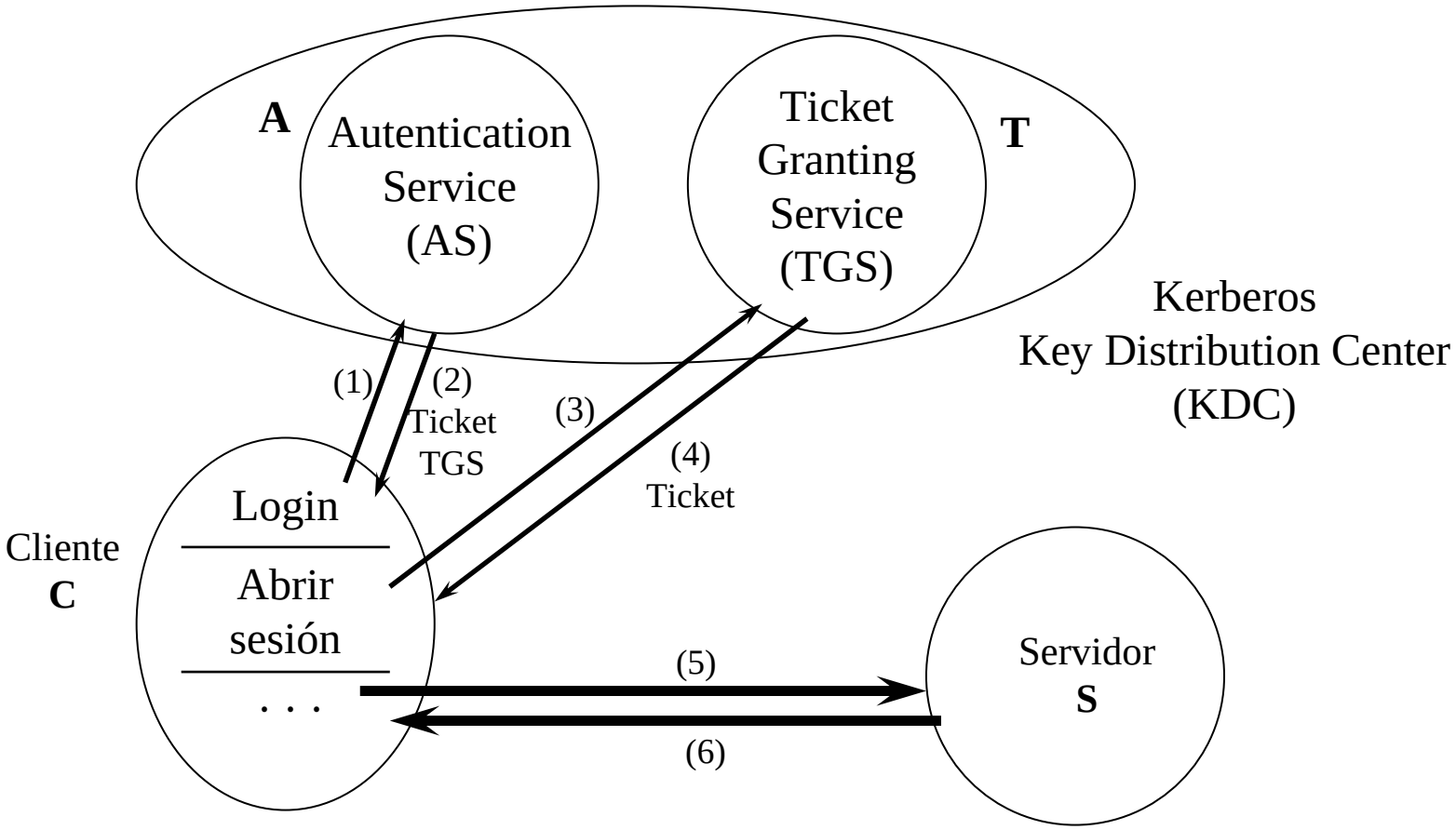
5 Kerberos
Protocolo (paso B)

Obtención de un ticket para acceder a un servidor S

(3) **C** $\xrightarrow{\{autent(C)\}_{K_{CT}},\ \{ticket(C,\ T)\}_{K_T},\ S,\ n}$ **T**

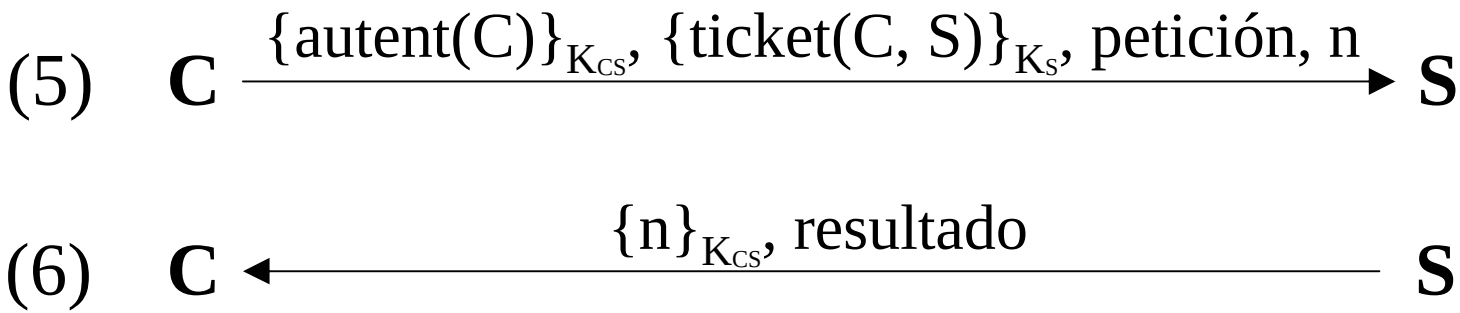
(4) **C** $\xleftarrow{\{K_{CS},\ n\}_{K_{CT}},\ \{ticket(C,\ S)\}_{K_S}}$ **T**

5 Kerberos
Arquitectura



5 Kerberos
Protocolo (paso C)

Acceso al servidor S



La inclusión (opcional) del contraste n en (6) permite al cliente asegurar la autenticidad de S