Criptografía: Firma Digital y Certificados Digitales

Organización de Datos (75.06)
- Cátedra Servetto -

FACULTAD DE INGENIERIA
Universidad de Buenos Aires

AGENDA

- Firmas
- Firma Digital Clave Privada
- Firma Digital Clave Pública
- Función Resumen
- Certificados Digitales

OBJETIVOS DE LA CRIPTOGRAFÍA

- ¿Qué problemas quiero resolver?
  - **Confidencialidad:** Garantizar que el mensaje solo pueda ser leído por sus destinatarios
  - **Autenticación:** Asegurarse que una persona es quien dice ser
  - **Integridad:** Asegurarse que el mensaje no fue modificado
  - **No repudio:** Evitar que alguien rechace ser autor de algo

FIRMA

¿Qué problemas resuelve la firma de un documento?

- Autenticación
- No repudio

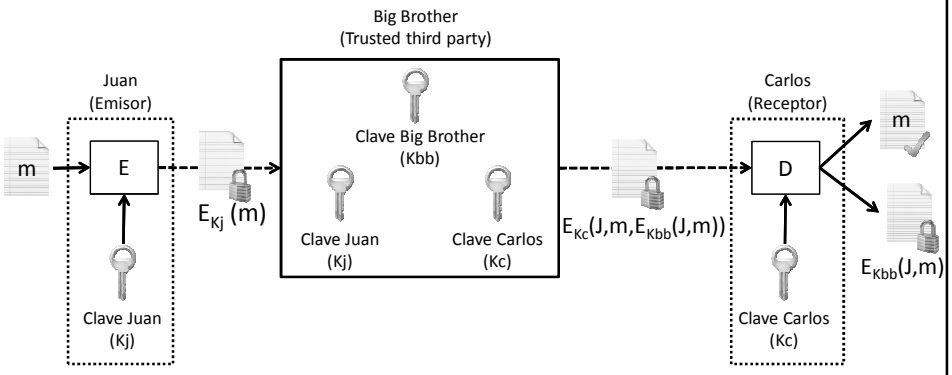
Procedimiento de Firma

- Asiento de la Firma en un Documento
- Proceso de Firma
- Proceso de Verificación

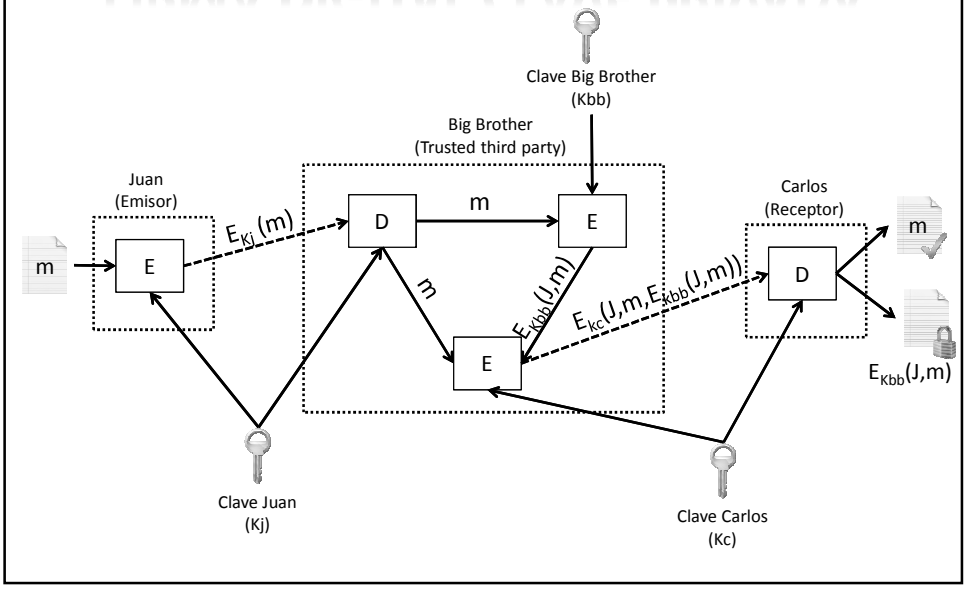
¿Cómo puedo lograr que esto pueda ser realizado entre dos computadoras?

FIRMA DIGITAL CLAVE PRIVADA

- Se basa en la criptografía **simétrica**
- Provee confidencialidad, autenticación y no repudio

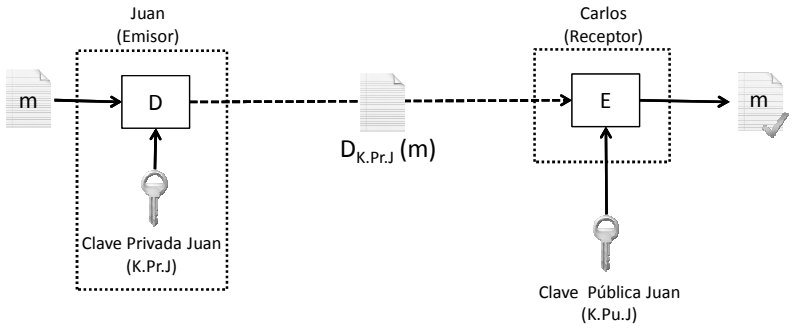


FIRMA DIGITAL CLAVE PRIVADA



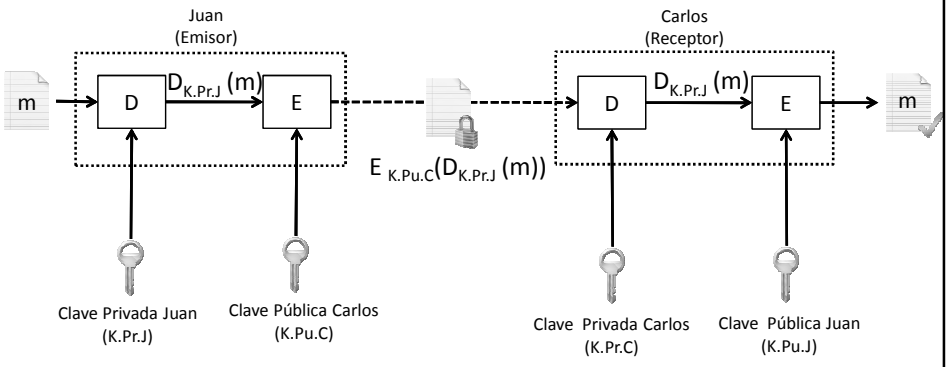
FIRMA DIGITAL CLAVE PÚBLICA

- Se basa en la criptografía **asimétrica**
- Provee autenticación y no repudio



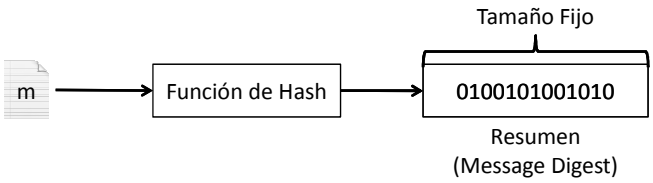
FIRMA DIGITAL CLAVE PÚBLICA

- Provee autenticación, no repudio y confidencialidad



FUNCIÓN RESUMEN

•¿Cómo lograr integridad? ¿Cómo acelerar el proceso firma?

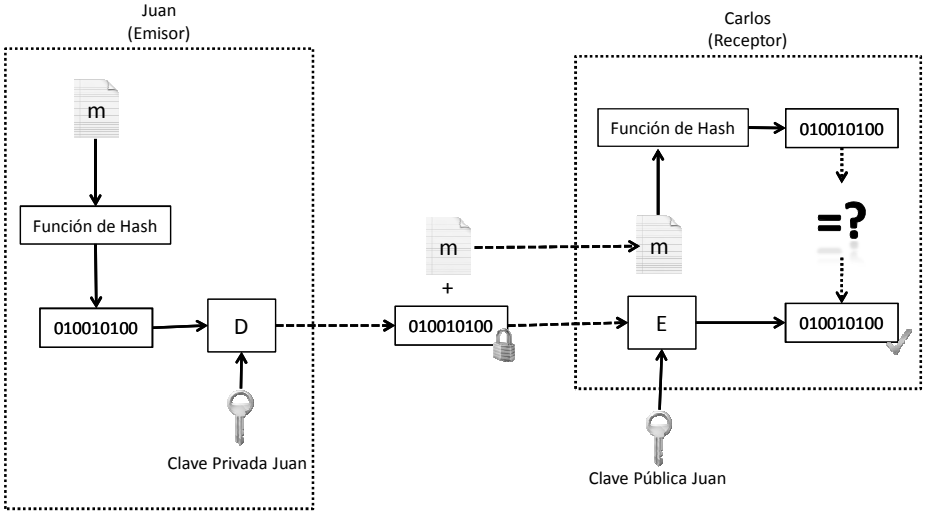


•La función tiene las siguientes **características**:

- Dado m, es fácil calcular r(m)
- Dado r(m), es imposible calcular m
- Dado m, no se puede encontrar m' de manera tal que r(m') = r(m)
- Un cambio de m de incluso un bit produce una salida muy diferente

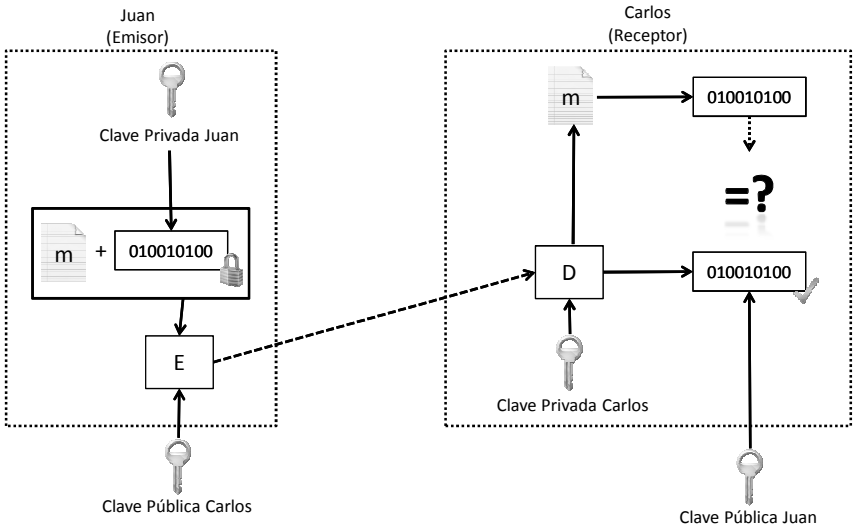
FIRMA DIGITAL CON RESUMEN

•Función resumen aplicada a un esquema asimétrico. Provee autenticación, no repudio e integridad



FIRMA DIGITAL CON RESUMEN

•Proveyendo autenticación, no repudio, integridad y confidencialidad

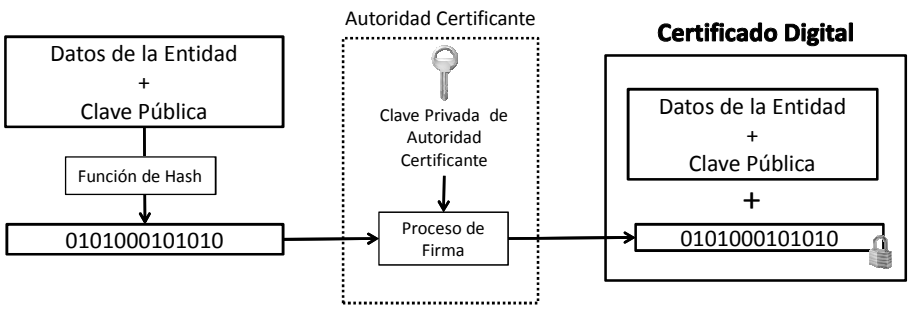


CERTIFICADOS DIGITALES

•¿Cómo obtener de forma segura la clave pública de otra persona?

✖ Centro de distribución de claves públicas

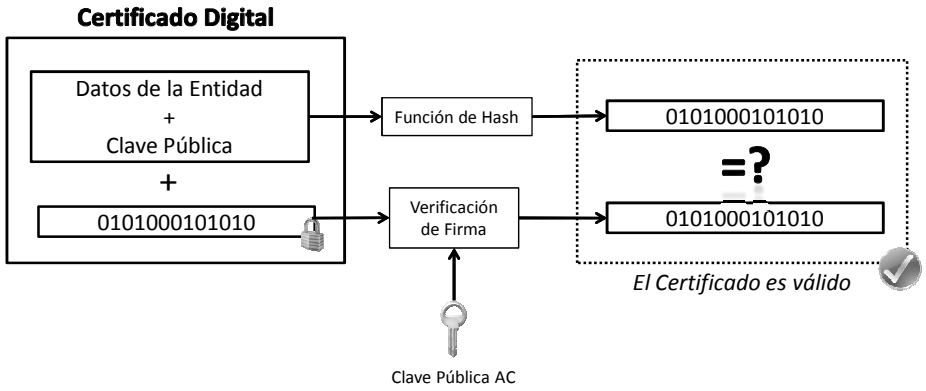
✓ Autoridad certificante + certificado digital de claves públicas



El objetivo de un certificado digital es relacionar inequívocamente una persona con su clave pública.

CERTIFICADOS DIGITALES

•Proceso de verificación del certificado digital



La seguridad del sistema de certificados digitales reside en la seguridad de la clave privada de la AC.

CERTIFICADOS DIGITALES

- Ejemplo de un certificado digital real