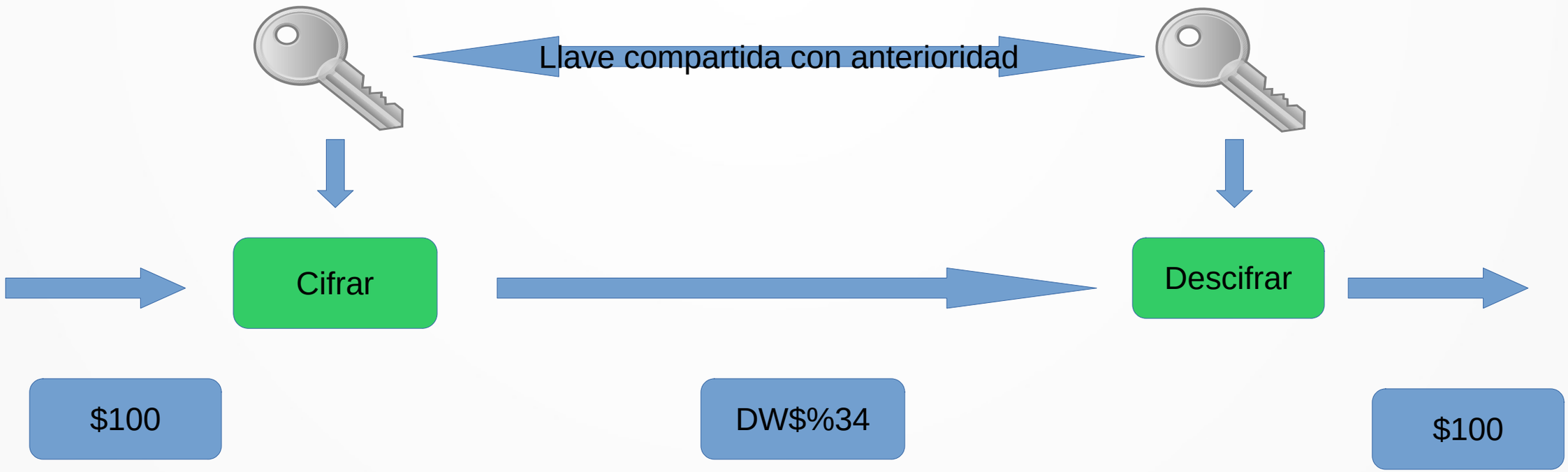
# Cifrado Asimétrico

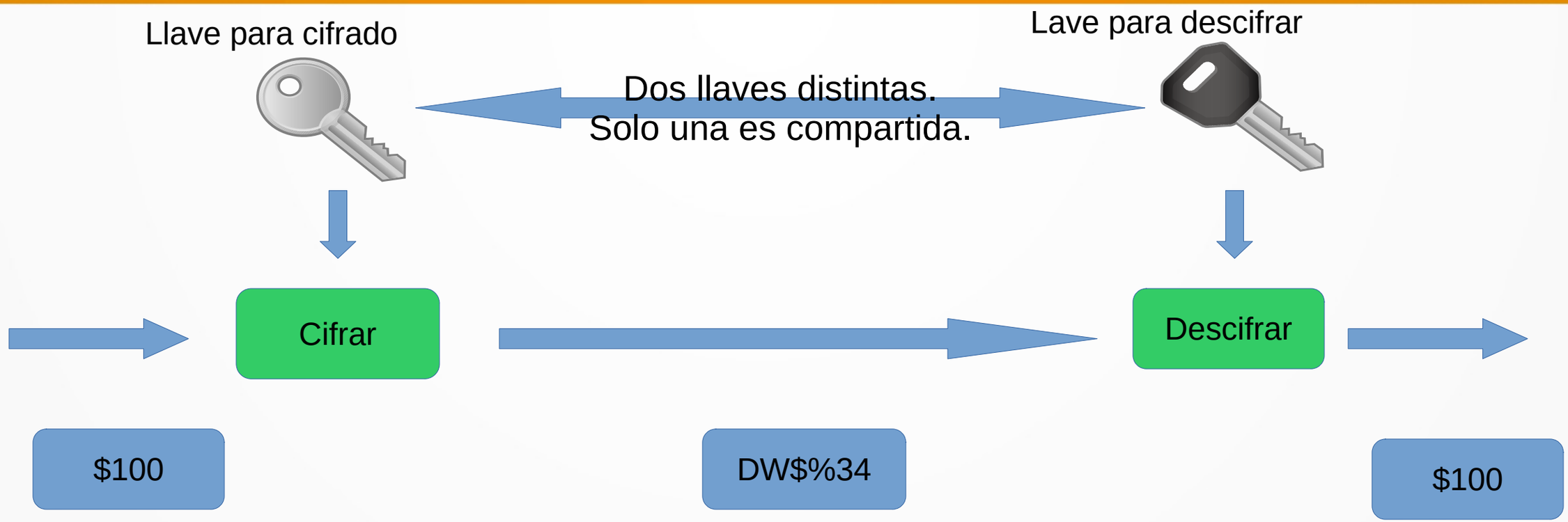
- Comparación vs simétrico
- Obteniendo CIA en algoritmos asimetricos
- Algoritmos:
  - DSA
  - RSA
- PKI
- TLS
- OpenPGP

# Sistemas de cifrado simétrico



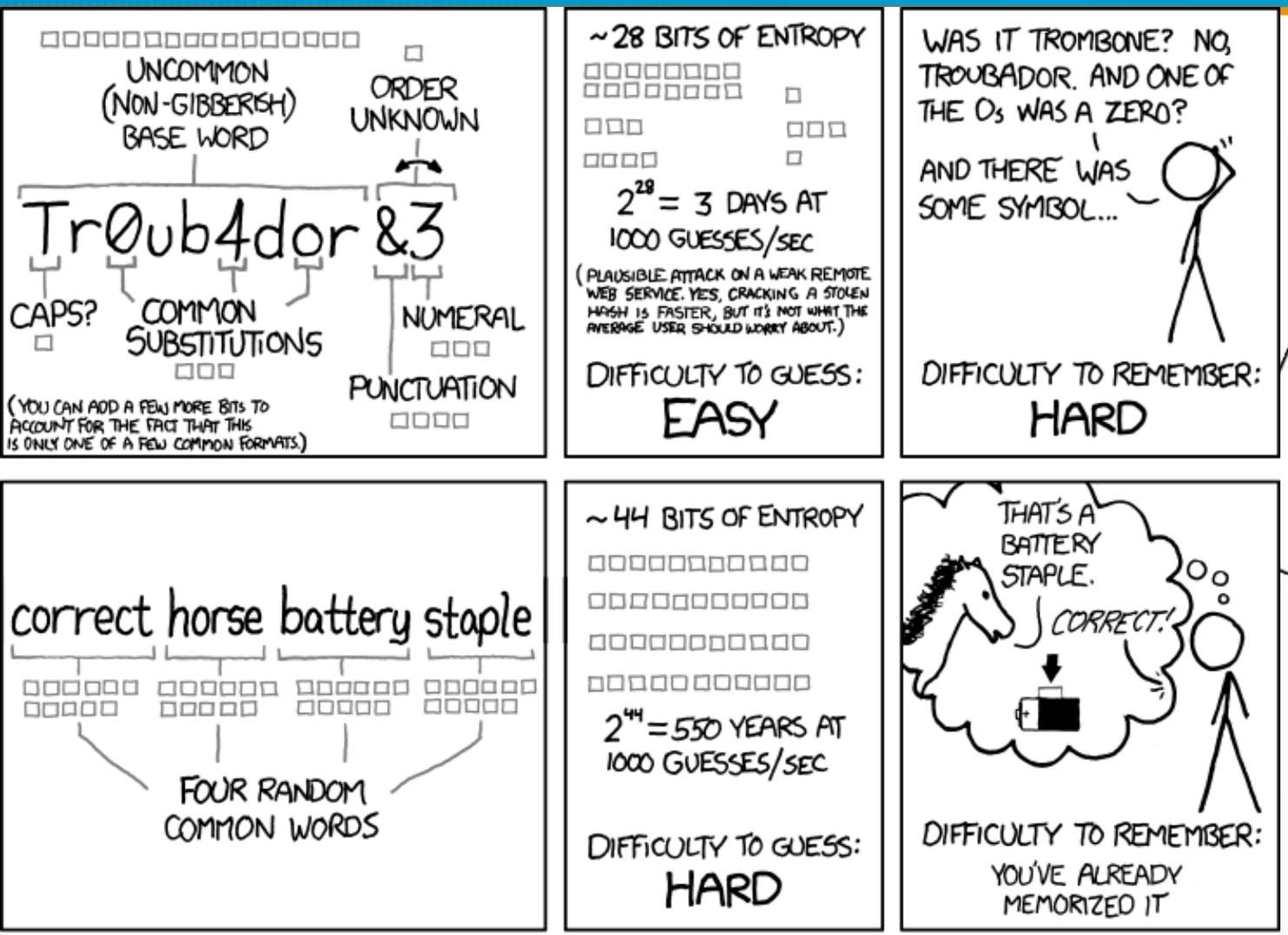

Algoritmos de cifrado simétrico
Largo de llave típico: 80 a 256 bits
Ejemplos: DES, 3DES, AES, Blowfish

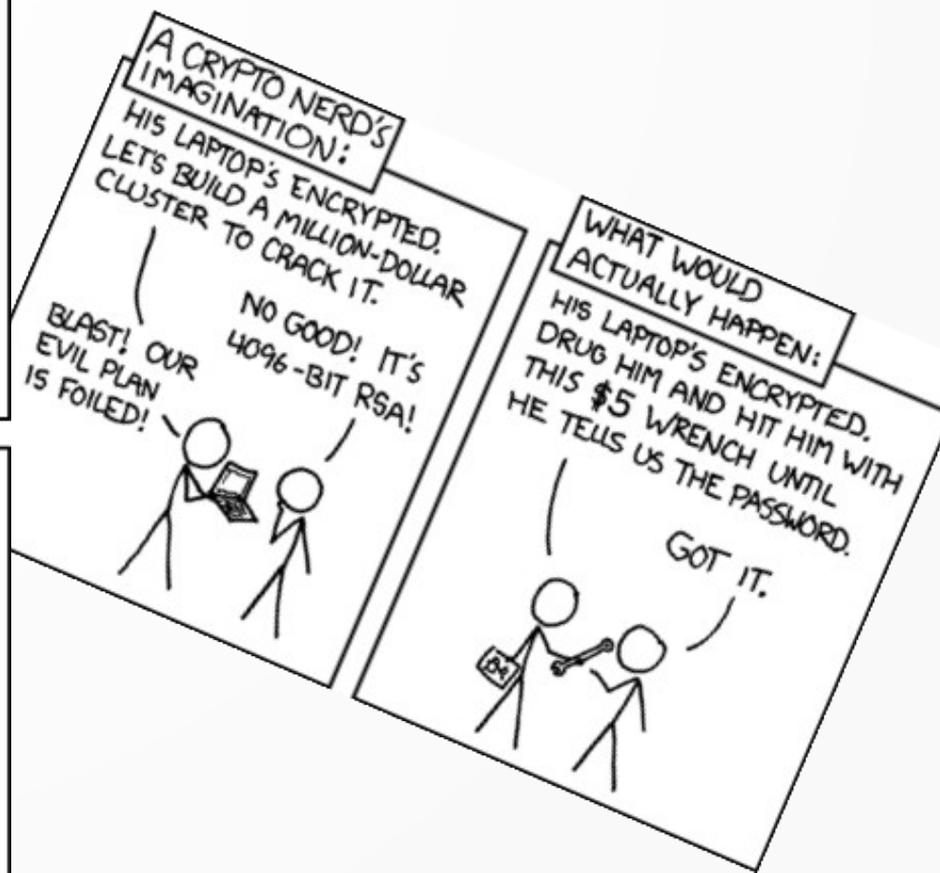
# Sistemas de cifrado asimétrico




Algoritmos de cifrado Asimétrico
Largo de llave típico: 512 a 4096 bits
Ejemplos: DSA, RSA, ElGamal, DH

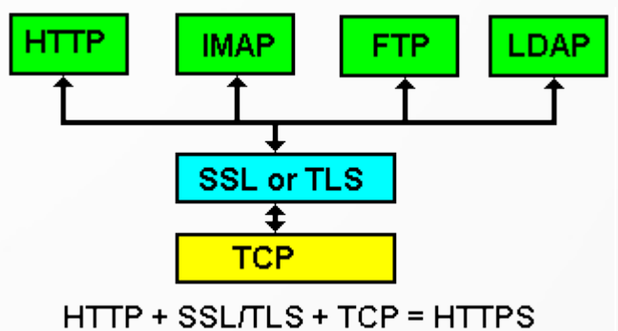
# Elección de la contraseña



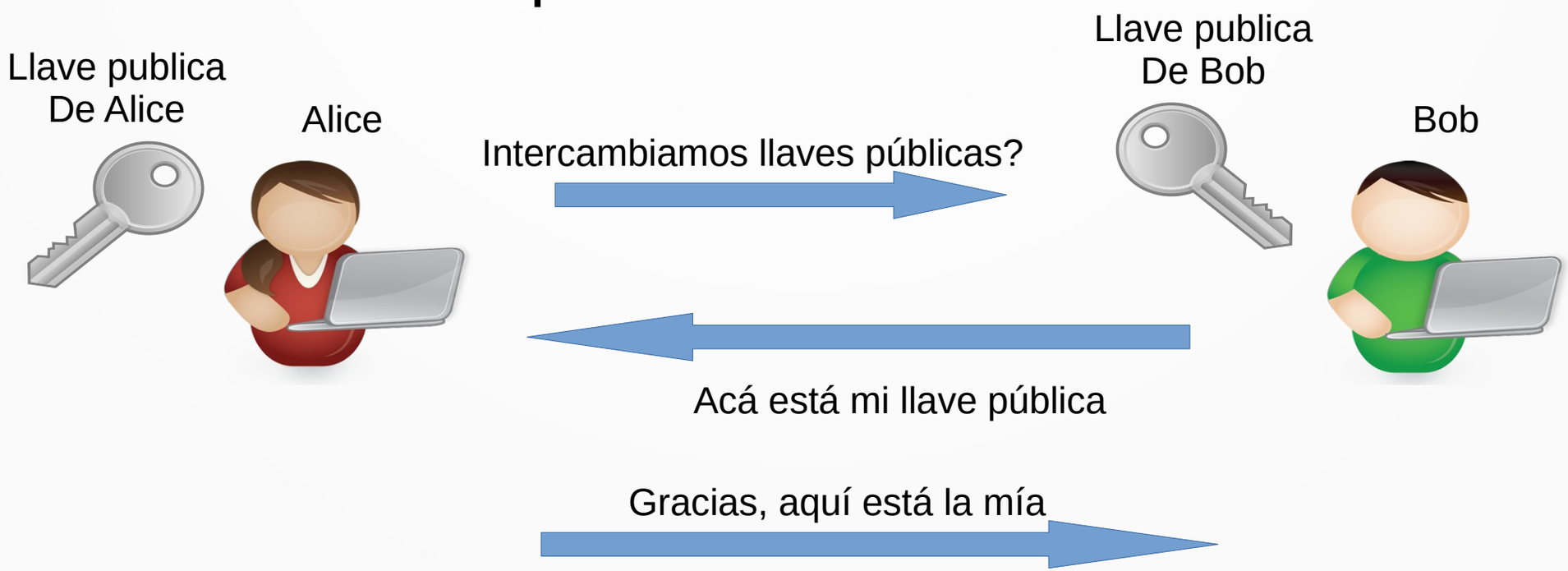
# Cifrado Asimétrico

- Protocolos que utilizan cifrado asimétrico
  - TLS (Transport Layer Security) - SSL (Secure Socket Layer)
    - HTTP – Acceso a sitios web
    - FTP – Transferencia de archivos
    - DNS – Resolución de nombres
    - SMTP – Transferencia de emails
    - SIP – Comunicacion de voz (VoIP)
    - VPN – Interconexión segura de redes
  - SSH (Secure Shell)
  - OpenPGP (Pretty Good Privacy)



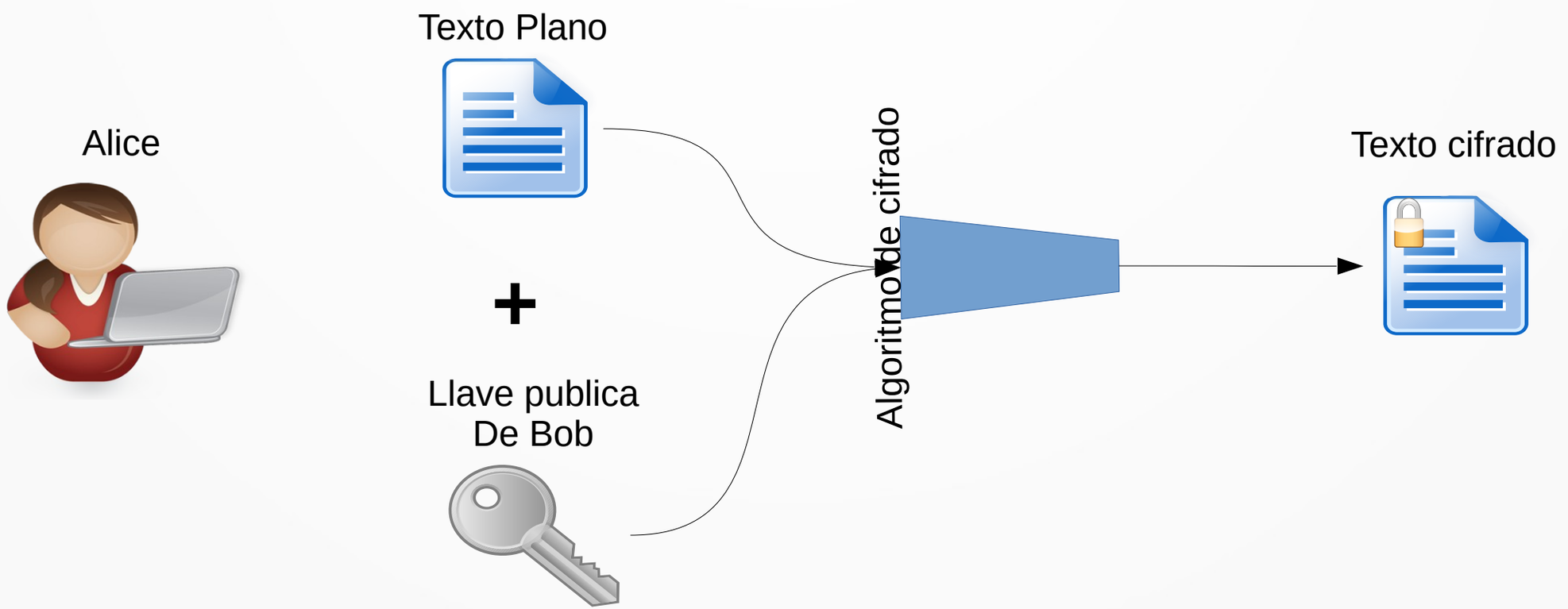
# Confidencialidad

- Llave Pública (Cifra) + Llave Privada (Descifra)
- Alice y Bob generan su par de llaves e intercambian la publica



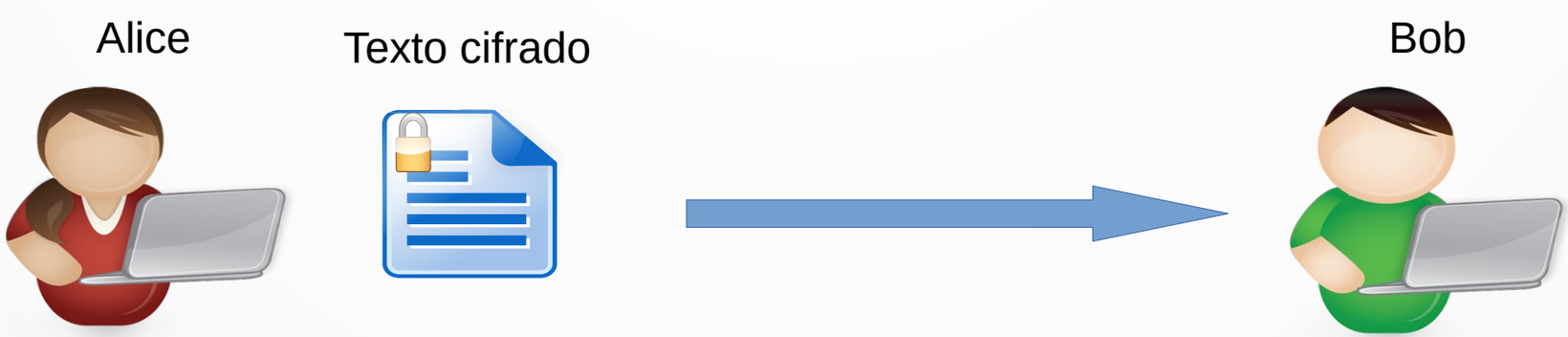
# Confidencialidad (Cont.)

- Alice utiliza la llave publica de Bob y un algoritmo de cifrado



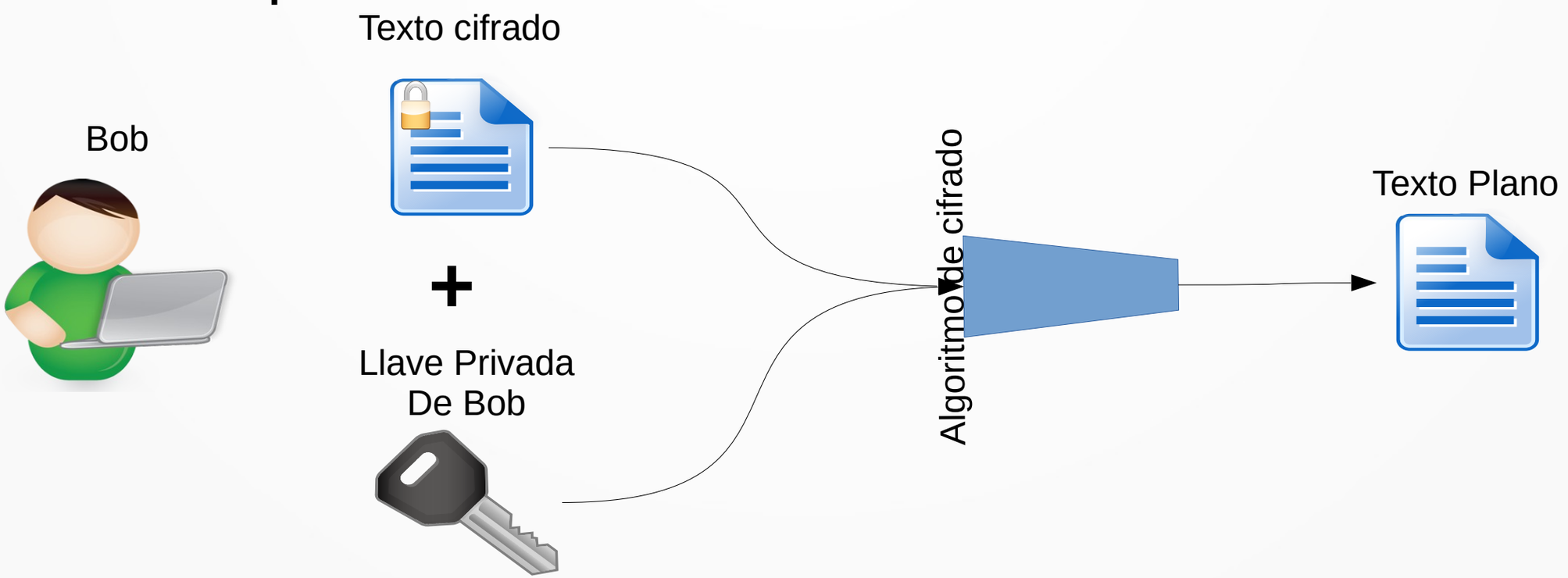
# Confidencialidad (Cont.)

- Alice le envía el documento cifrado a Bob



# Confidencialidad (Cont.)

- Bob utiliza su llave privada y el algoritmo de cifrado para descifrar



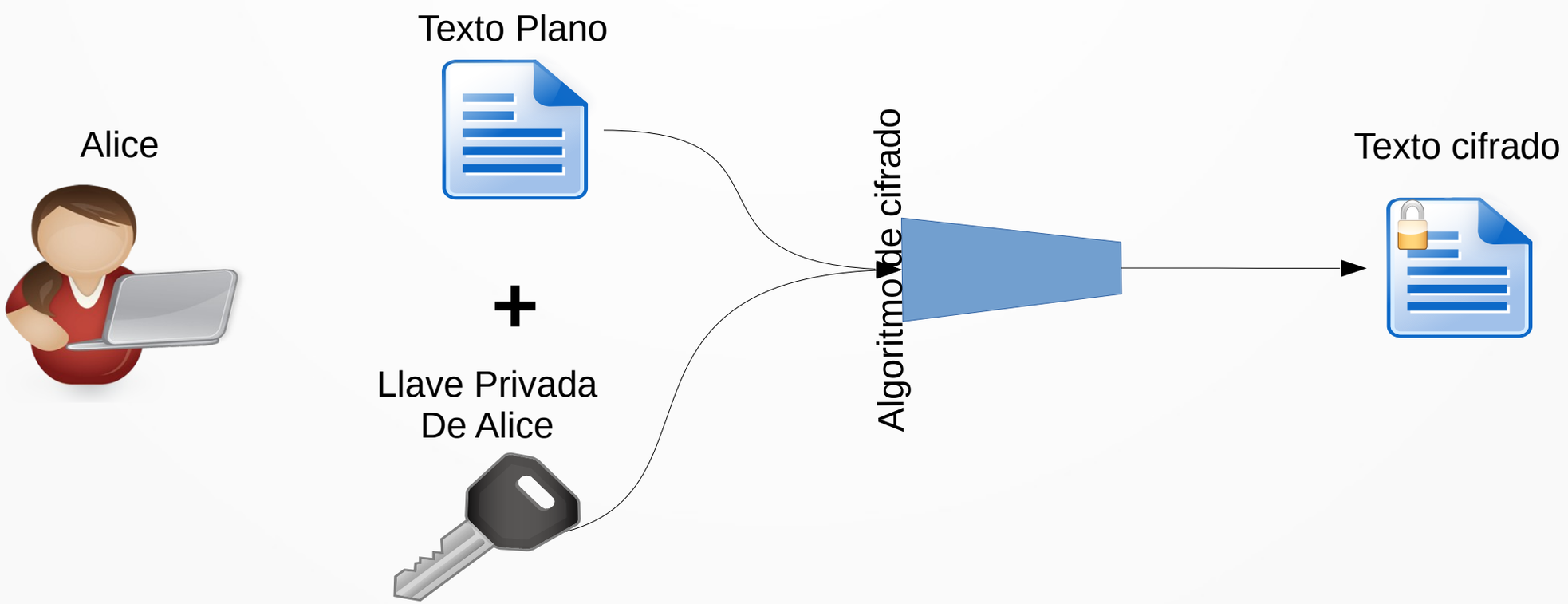
# Confidencialidad (cont.)

- Cuando se cifra utilizando una llave pública solo se puede descifrar usando su par privado

- Todavía no tenemos Autenticidad.
  - Trudy puede pretender ser Alice
- Tampoco tenemos Integridad.
  - Trudy puede interceptar el mensaje y enviar otro en su lugar

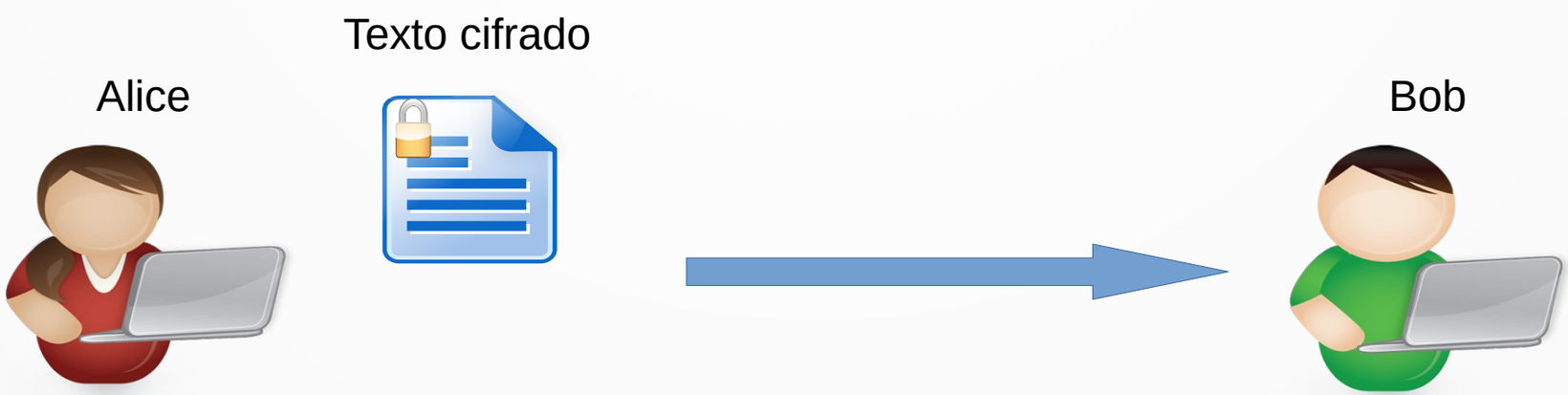
# Autenticidad

- Llave Privada (Cifra) + Llave Pública (Descifra)



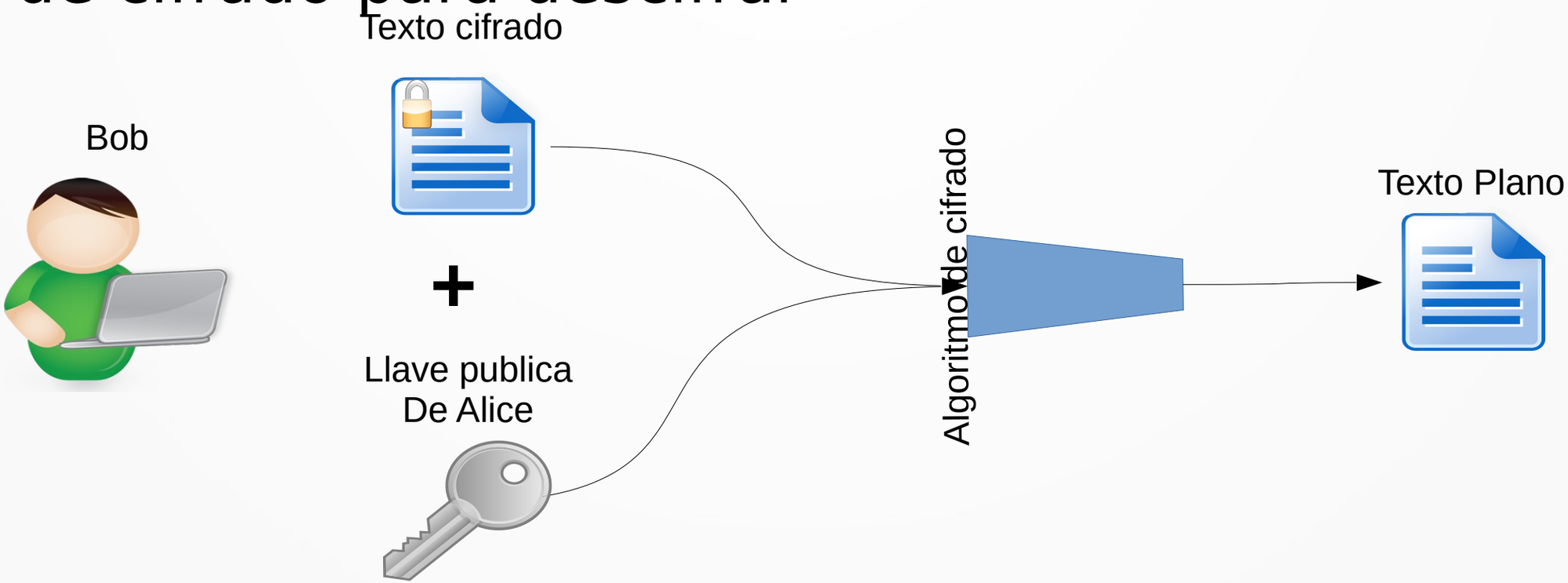
# Autenticidad (Cont.)

- Alice le envía el documento cifrado a Bob



# Autenticidad (Cont.)

- Bob utiliza la llave publica de Alice y el algoritmo de cifrado para descifrar



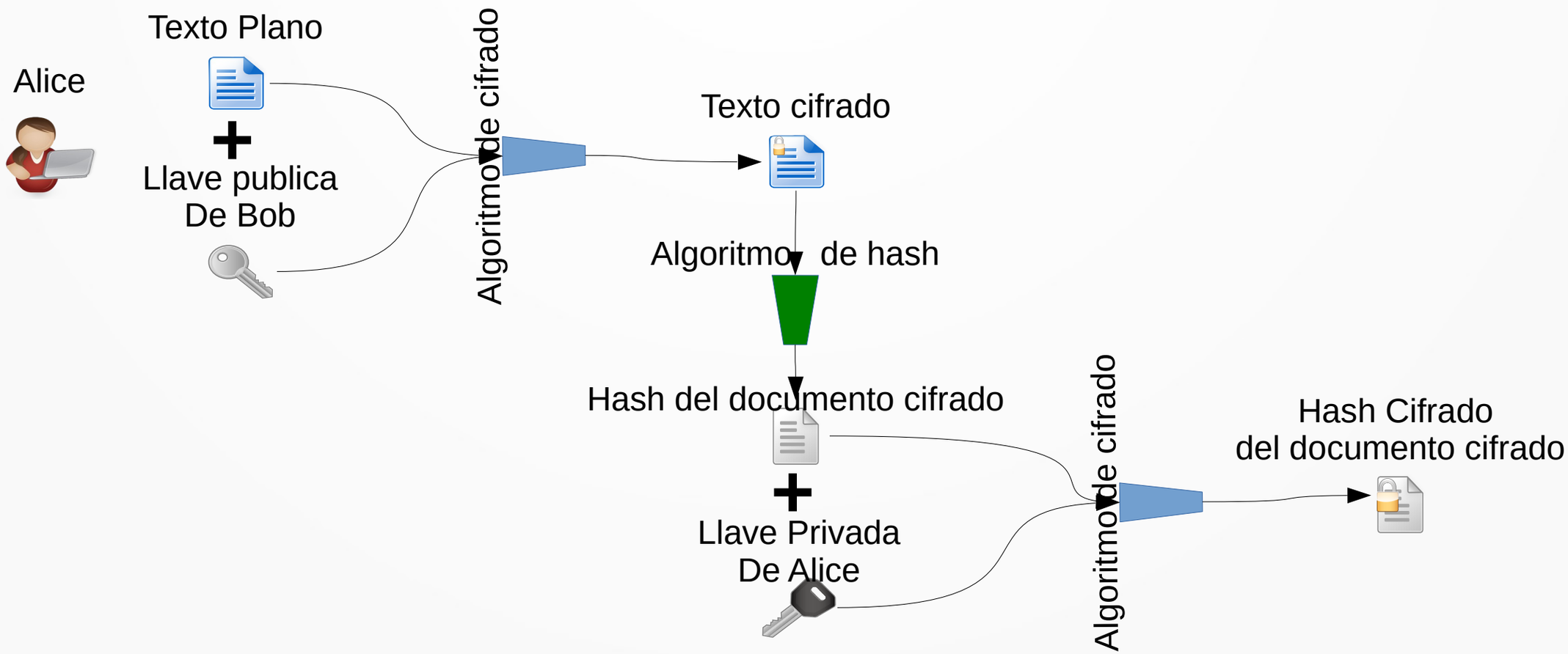
# Autenticidad (cont.)

- Cuando se cifra un documento utilizando una llave privada, cualquiera puede descifrar con la llave publica
- Solo el que tenga la llave privada pudo cifrar ese documento

- Todavía nos falta mantener la integridad del documento

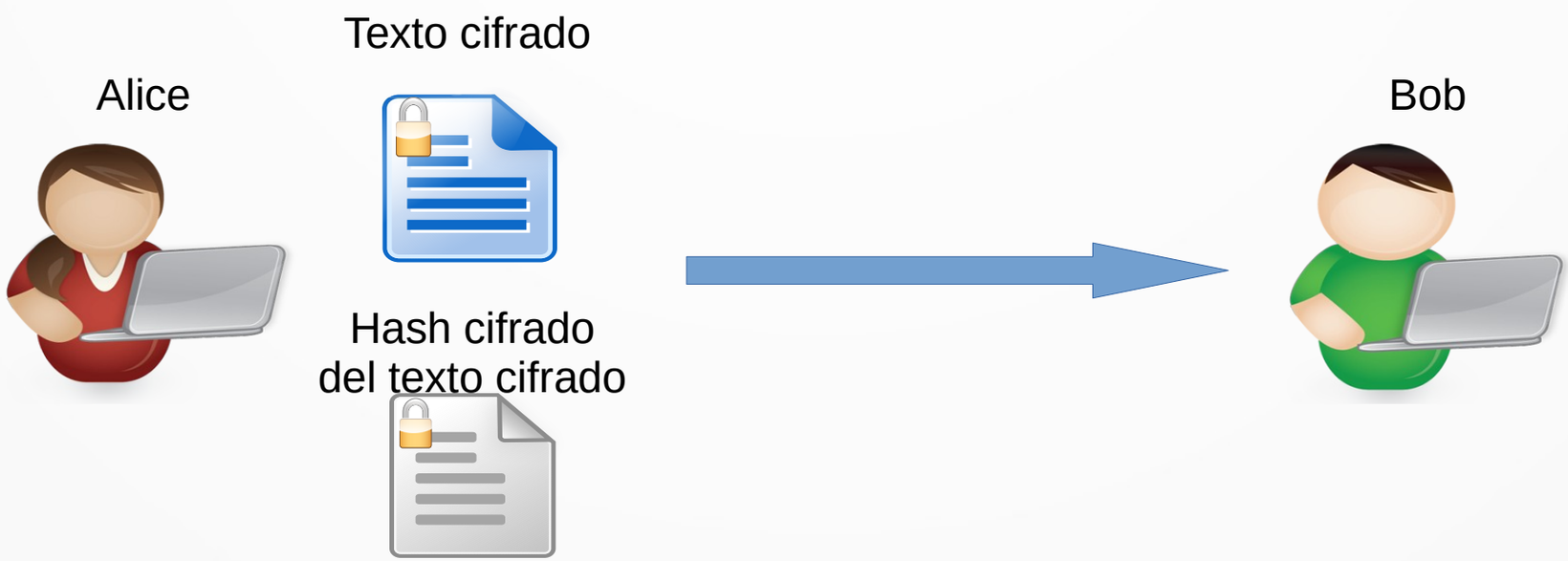
# CIA

- Hash del documento cifrado + Llave privada (cifrar)



# CIA (Cont.)

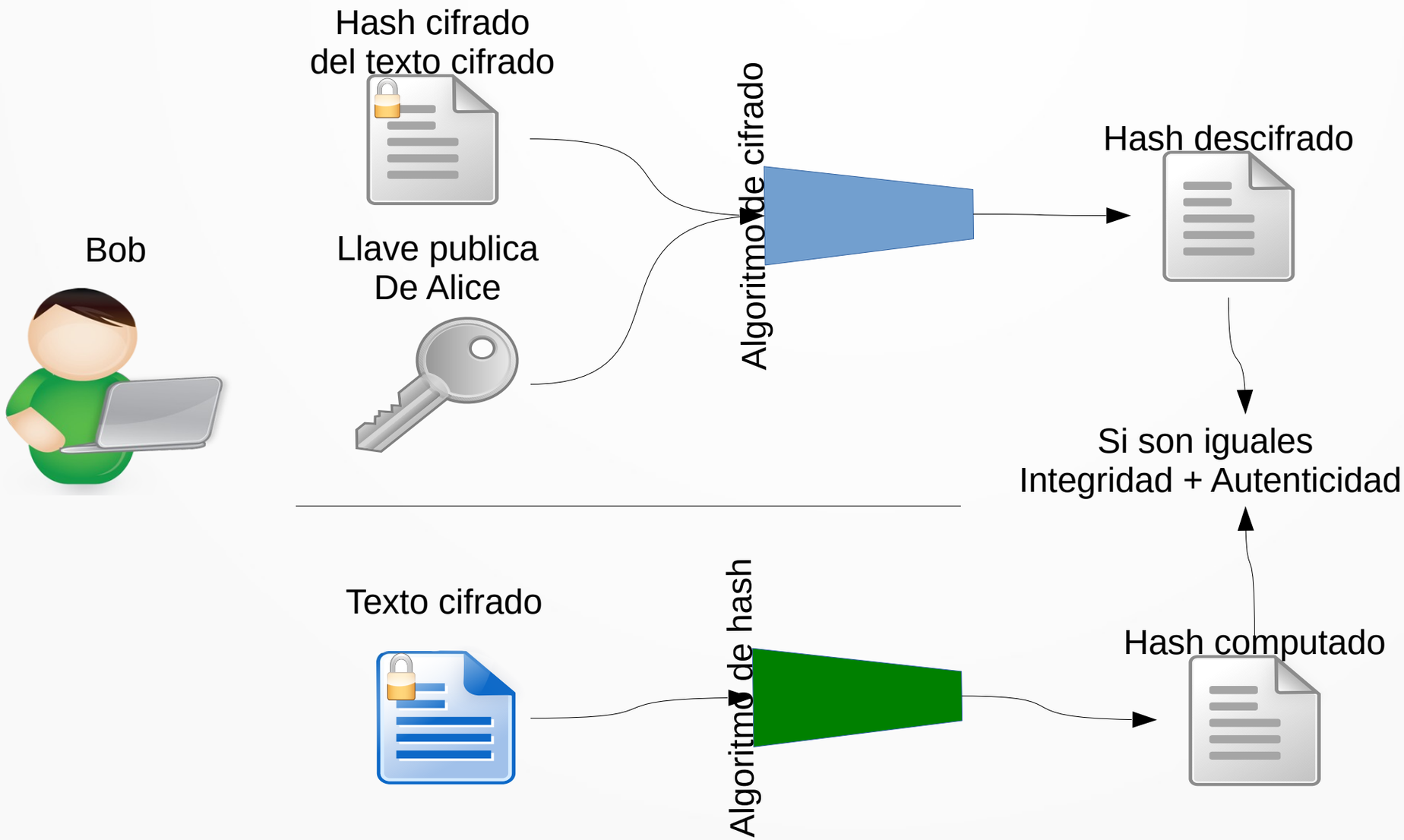
- Alice le envía a Bob el documento cifrado (con la llave publica de Bob) y el Hash de dicho documento (cifrado con la llave privada de Alice)



# CIA (Cont.)

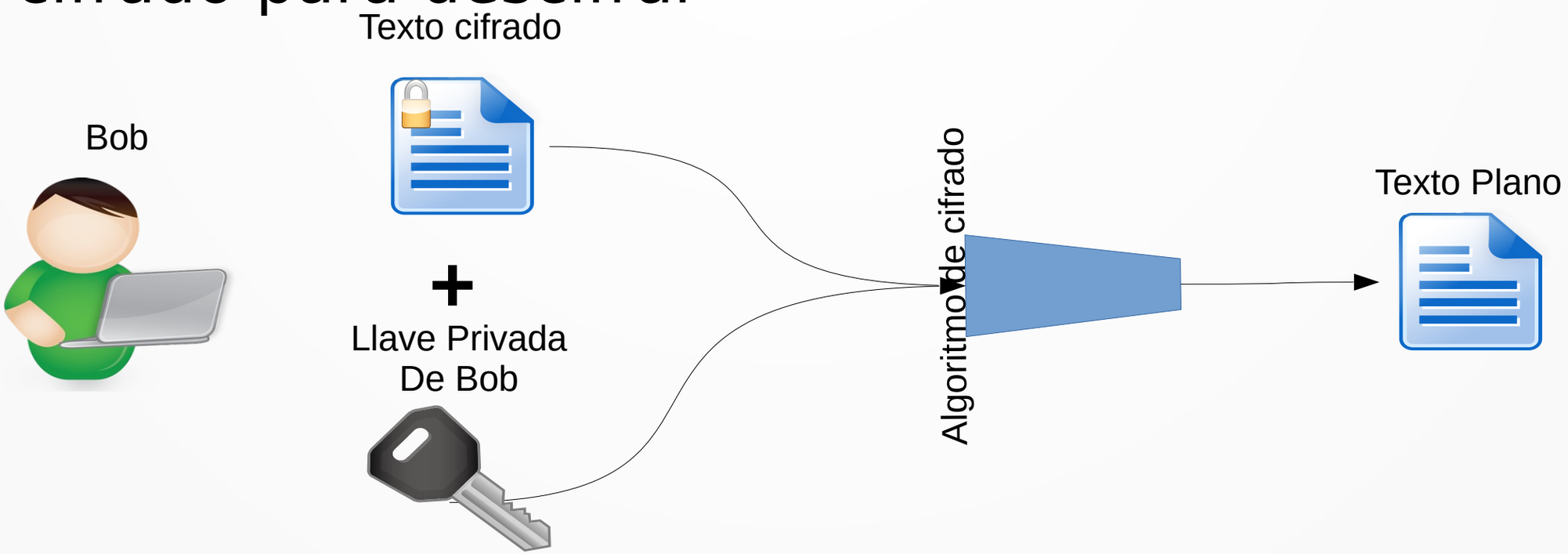
- Bob descifra el hash usando la llave pública de Alice
- Computa por su cuenta el hash del documento cifrado y lo compara con el hash descifrado
- Si son iguales se logra INTEGRIDAD + AUTENTICIDAD

# CIA (Cont.)


Hash cifrado
del texto cifrado
Bob
Llave publica
De Alice
Algoritmo de cifrado
Hash descifrado
Si son iguales
Integridad + Autenticidad
Texto cifrado
Algoritmo de hash
Hash computado

# CIA (Cont.)

- Bob utiliza su llave privada y el algoritmo de cifrado para descifrar



# CIA (Cont.)

- Hash cifrado usando llave privada = Firma digital
- Posibles problemas:
  - Llave privada comprometida
    - Se consigue una copia de su llave privada
      - El que tiene la copia se puede hacer pasar por Alice
      - Puede descifrar los documentos que solo Alice podía descifrar
  - Llave publica falsa
    - Se genera un par de llaves a nombre de Alice
      - Se distribuye la llave publica (falsa) de Alice
      - Bob recibe documentos firmados con la llave privada (falsa) de Alice y los descifra usando la llave publica (falsa) de Alice – Efectivamente cree que es Alice quien le envía el documento.

# Algoritmo DSA

- Digital Signature Algorithm
- Únicamente para proveer firmas digitales
- Permite firmar un documento, código, aplicación, etc.
  - hash (sha-2) cifrado con DSA utilizando llaves de 2048bits o mas.

# Algoritmo RSA

- Ron RIVEST, Adi SHAMIR, Len ADLEMAN
- Ampliamente utilizado
- No solo se usa para firma digital como el DSA
- Llaves de 2048bits o mas

# Public Key Certificate

- Utilizado para acreditar la titularidad (la pertenencia) de una llave pública.
- Basado en X.509
- Incluye (entre otros) información sobre:
  - La identidad del titular
  - El algoritmo utilizado para generar la llave
  - Firma digital del titular
  - La llave pública del titular
  - Información sobre el certificante (quien provee la autenticidad del certificado)
  - Firma del certificante
  - Propósito del certificado
  - Fechas de validez

# PKI

- Public Key Infrastructure
- Infraestructura que provee los servicios necesarios para dar el soporte en  cualquier escala a los certificados de llave pública
- La infraestructura necesita contar con diversos elementos de hardware, software, personas, políticas y procedimientos.
- Utilizado para crear, administrar, almacenar, distribuir y revocar certificados de llave pública

# PKI (cont.)

- Certificados PKI
  - Documento que identifica al titular y su llave pública
  - Debe ser firmado por la CA para proveer autenticidad
- Autoridad Certificante de PKI (CA)
  - Un tercero confiable el cual firma las llaves públicas de las entidades en un sistema de PKI

# PKI (cont.)

- Componentes básicos
  - Usuarios de PKI: Personas, Dispositivos, Servidores, Empresas
  - CA para la administración
  - Almacenamiento y protocolos
  - Infraestructura organizacional como Local Registry Authorities (LRAs)
  - Marco Legal
    - https://www.argentina.gob.ar/modernizacion/firmadigital

# PKI (cont)

- Se puede proveer certificados de diferentes clases que determinan cuan confiable es una entidad
- Cuanto mas alto el numero de clase, mas riguroso es el procedimiento para obtener el certificado
- Clase 0 – Propósitos de testeo. No se realizan verificaciones de identidad
- Clase 1 – Para individuos, pensado para emails.
- Clase 2 – Para organizaciones que necesitan demostrar su identidad
- Clase 3 – Para servidores y firma de software
- Clase 4 – Para transacciones de negocio entre empresas
- Clase 5 – Para organizaciones privadas o seguridad gubernamental

# PKI (cont.)

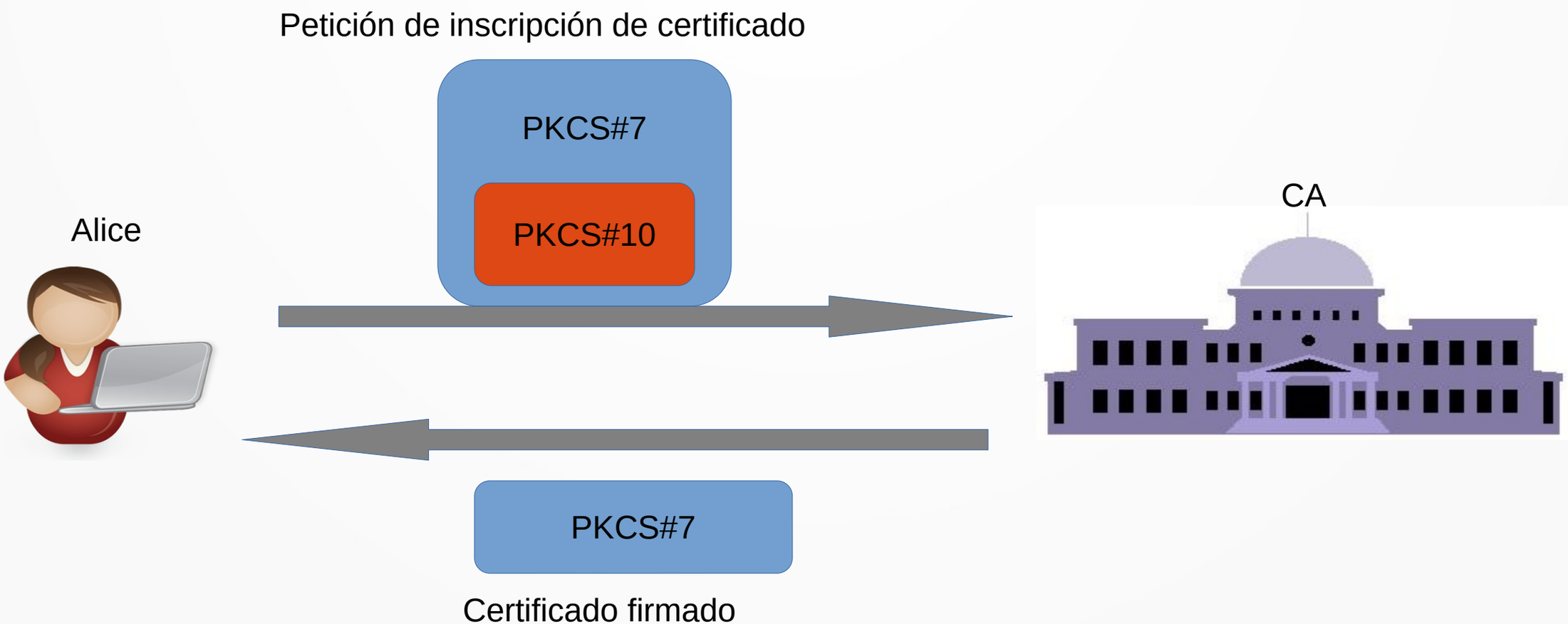
- Algunos PKIs ofrecen la posibilidad o inclusive requieren del uso/generación de dos juegos de llaves públicas y privadas
  - El primero solo para cifrar
    - La llave pública para cifrar, la privada descifrar
  - El segundo solo para firma digital
    - La llave privada para firmar, la publica se usa para verificación de la firma
  - Pueden diferir en largos de llaves y/o en algoritmos a utilizar

# PKI (cont.)

- Public Key Cryptography Standards (PKCS)
- Definen como es el formato para lograr el intercambio seguro de la información protegida
  - PKCS #1: RSA Cryptography Standard
  - PKCS #3: DH Key Agreement Standard
  - PKCS #5: Password-Based Cryptography Standard
  - PKCS #6: Extended-Certificate Syntax Standard
  - PKCS #7: Cryptographic Message Syntax Standard
  - PKCS #8: Private-Key Information Syntax Standard
  - PKCS #10: Certification Request Syntax Standard
  - PKCS #12: Personal Information Exchange Syntax Standard
  - PKCS #13: Elliptic Curve Cryptography Standard
  - PKCS #15: Cryptographic Token Information Format Standard

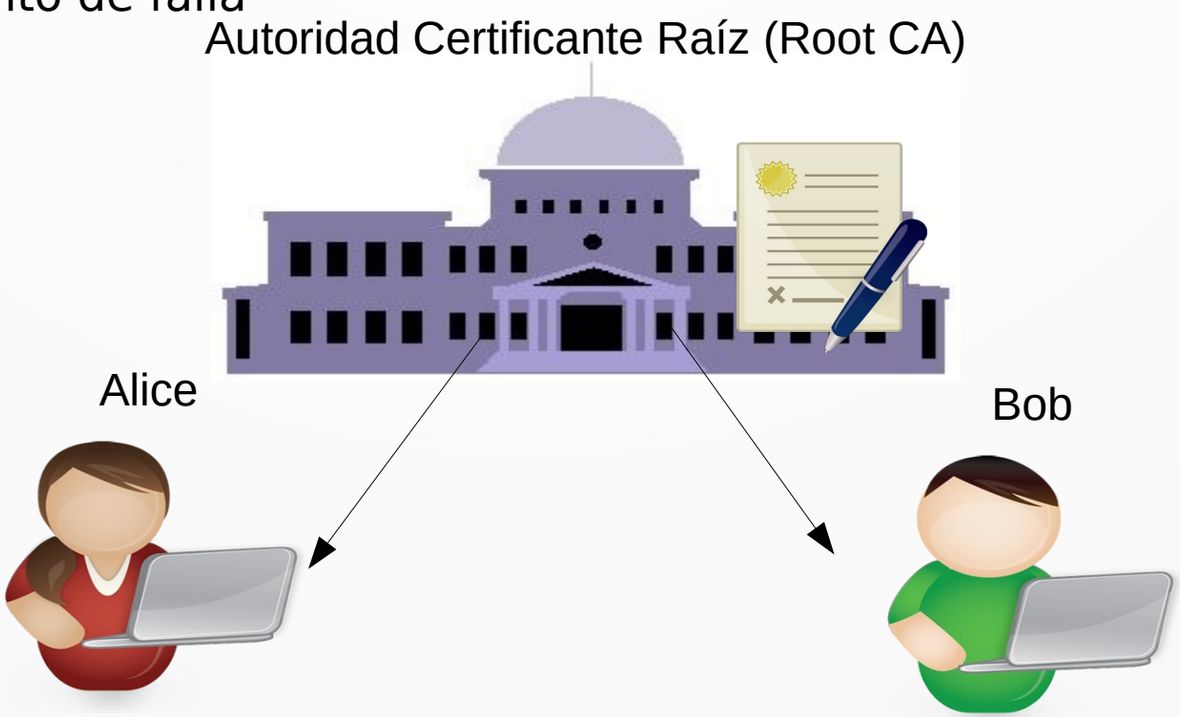
# PKI (cont.)

- Ejemplo PKCS



# PKI (cont.)

- Topología Básica de PKI – Single Root
- Emite todos los certificados para las entidades finales
- Difícil de escalar en grandes entornos
- Requiere de una administración estrictamente centralizada
- Genera un único punto de falla



# PKI (cont.)

- Topología jerárquica

Alice

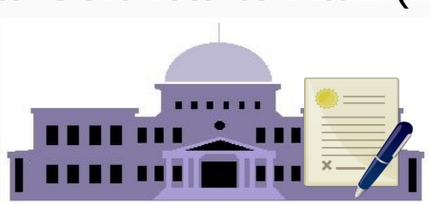
1 – Petición de Inscripción

Autoridad Regional (RA)

2 – Cuando la RA aprueba la Petición de Alice (proceso burocrático acorde a las políticas) agrega info adicional al certificado y lo envía a la CA

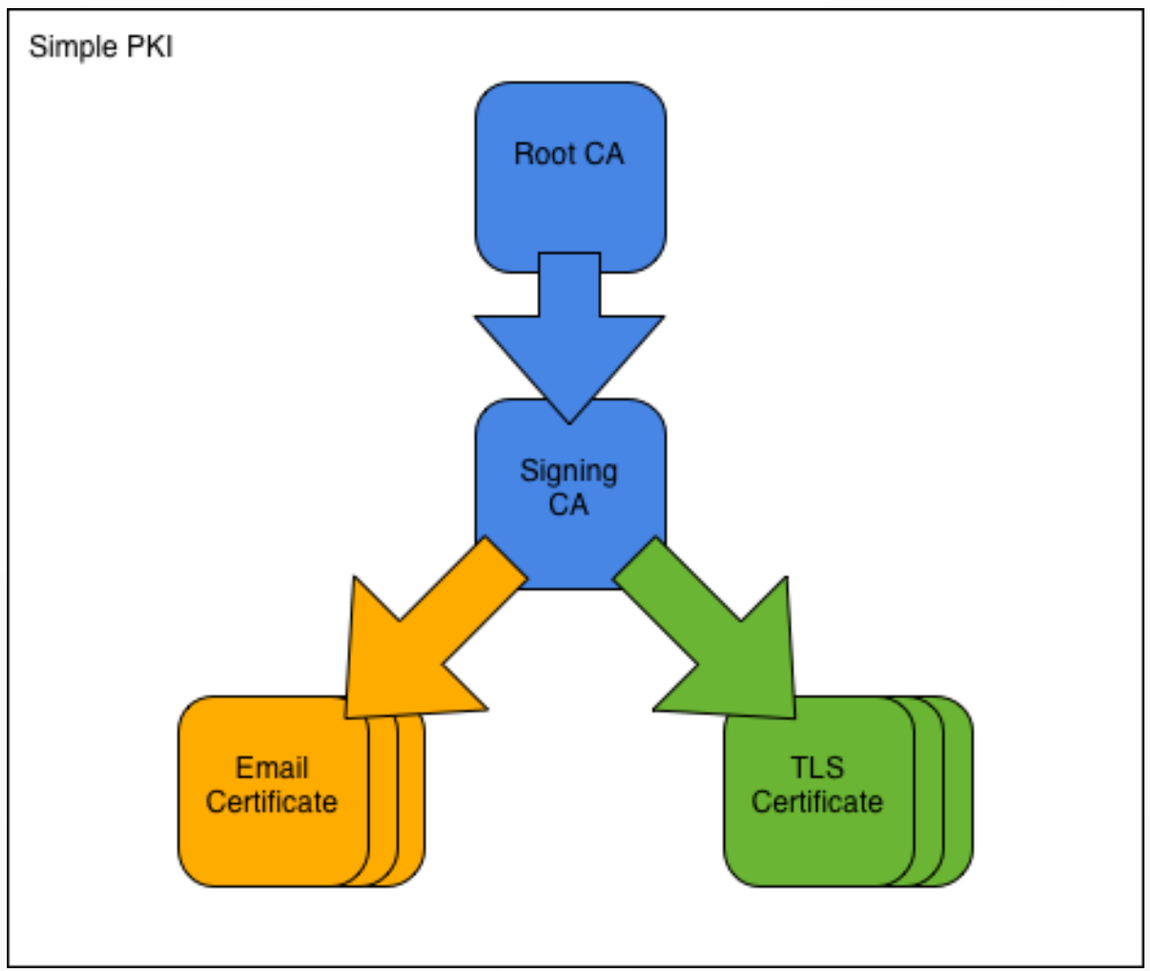
3 – La CA firma la petición de inscripción (el certificado) y se lo envía a la entidad que pidió la inscripción

Autoridad Certificante Raíz (Root CA)



# LAB PKI

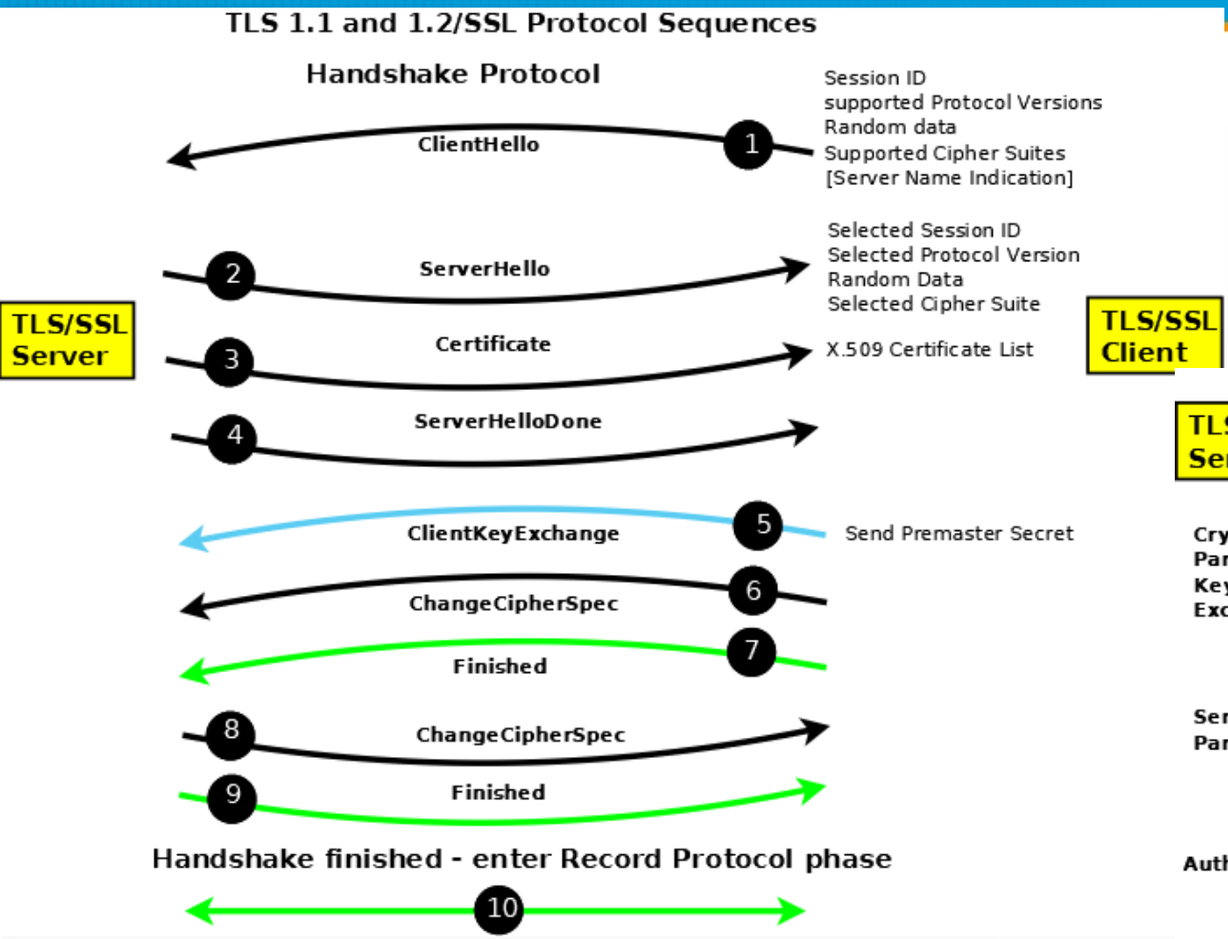
- https://pki-tutorial.readthedocs.org/en/latest/simple/index.html



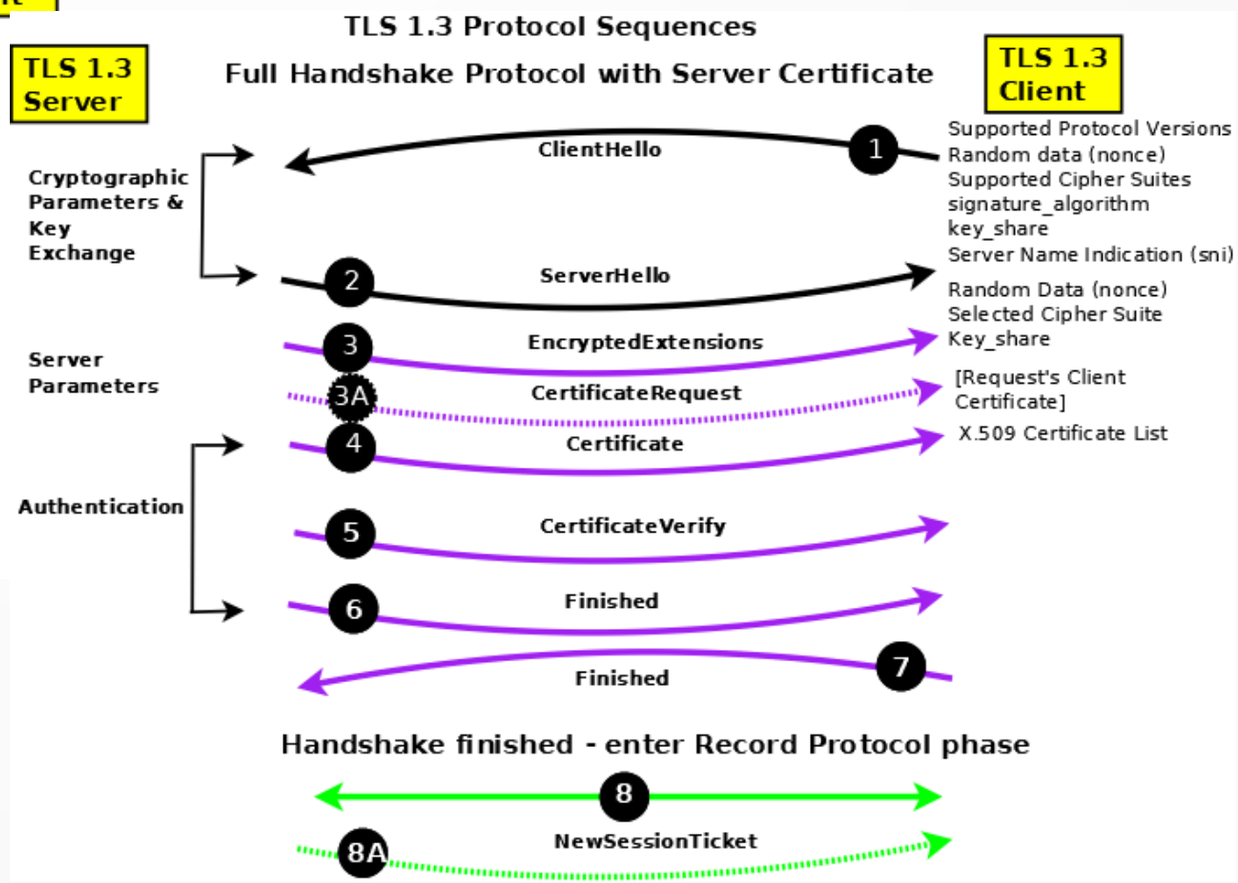
# TLS

- Ocurre un intercambio de mensajes entre el cliente y el servidor para intercambiar llaves y acordar algoritmos a usar
  - Handshake Protocol
    - El cliente ofrece un listado de posibilidades
    - El servidor responde con con opciones aceptadas negociando los algoritmos a utilizar, y presenta su certificado
    - Se establece un ID de sesión
    - Intercambio de llaves maestras de la sesion
    - Cierre de handshake
  - Record Protocol
    - El cliente y el servidor intercambian el resto de la información utilizando 'CIA'

# TLS (Cont.)




http://www.zytrax.com/tech/survival/ssl.html




https://www.comparitech.com/net-admin/decrypt-ssl-with-wireshark/

# OpenPGP

- Pretty Good Privacy
- GNU Privacy Guard
- Utilizado para 'CIA' de e-mails
- Publicación de Llave Pública en 'key servers'
- 'Web of Trust' vs CA
- https://emailselfdefense.fsf.org/es/