Cifrado asimétrico

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Cifrado asimétrico

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Criptografía de clave pública

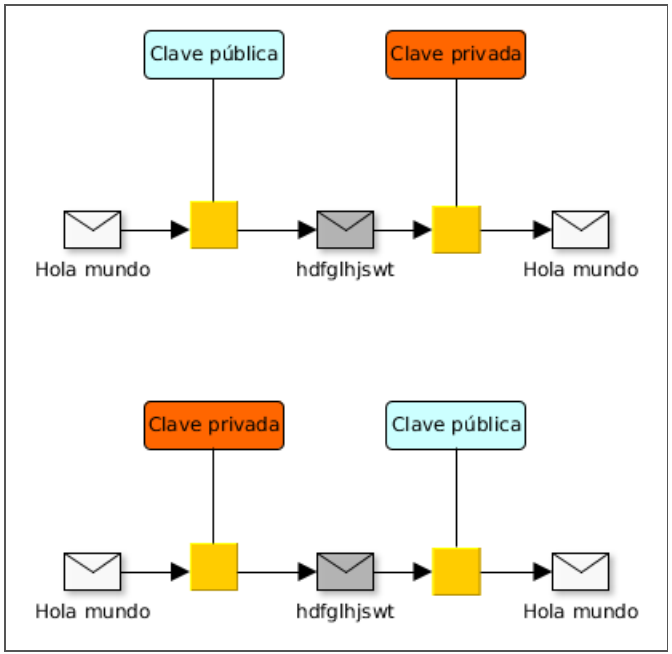
Usa algoritmos de clave asimétrica: la clave que cifra no es la que descifra

Usa dos claves por usuario:

- La clave pública que conoce todo el mundo
- La clave privada que sólo conoce el usuario

Lo que una clave cifra sólo lo puede descifrar la otra

Criptografía de clave pública



Criptografía de clave pública

Public key derivation

Criptografía de clave pública

- Iker tiene su clave privada $I_{privada}$ y todos tienen la clave pública de Iker, $I_{pública}$
- Miren cifra su mensaje m usando la clave pública de Iker: c = e (m , $I_{pública}$)
- Miren manda el criptograma c a Iker
- Iker recibe c
- Iker descifra c usando su clave privada I privada: m = d (c , $I_{privada}$)
- Confidencialidad. Sólo Iker puede descifrar el mensaje

Criptografía de clave pública

Ventajas:

- Sólo el destinatario puede leer el mensaje
- Sólo hay que almacenar una clave
- Cualquiera puede usar la clave pública para enviar un mensaje confidencial a Iker
- No son necesarios canales seguros para comunicar la clave pública

Criptografía de clave pública

Problemas:

- La clave privada debe mantenerse privada
- Debería ser (prácticamente) imposible sacar la clave privada a partir de la clave pública
- Cifrado y descifrado son más lentos que en los sistemas de clave secreta
- Miren debe estar segura de que está usando la clave pública de Iker
- Debe ser fácil obtener las claves públicas

Criptografía de clave pública

Cada usuario genera su par (clave pública, clave privada) y publica la clave pública en un servidor de claves: Key Certification Authority o Key Distribution Center (KDC)

Criptografía de clave pública

Más problemas:

- ¿Cómo sabe Iker si el mensaje es realmente de Miren?
- Cuando Iker conteste ¿Cómo sabe Miren que el mensaje es realmente de Iker?

Criptografía de clave pública

- Si Iker lo cifra con su clave privada lo puede descifrar cualquiera ($I_{pública}$ la conoce todo el mundo)
- Solución:
  - Iker cifra el mensaje con su clave privada: C1 = e (m, $I_{privada}$)
  - Luego lo vuelve a cifrar con la clave pública de Miren: C2 = e (C1 , M $_{pública}$)

Criptografía de clave pública

- Sólo Miren puede desencriptarlo con su clave privada:
  - Confidencialidad: Sólo Miren puede descifrar el mensaje: C1 = d (C2 , $M_{privada}$)
  - Autenticidad y No Repudio: Sólo Iker ha podido enviar el mensaje: m = d (C1, $I_{pública}$)

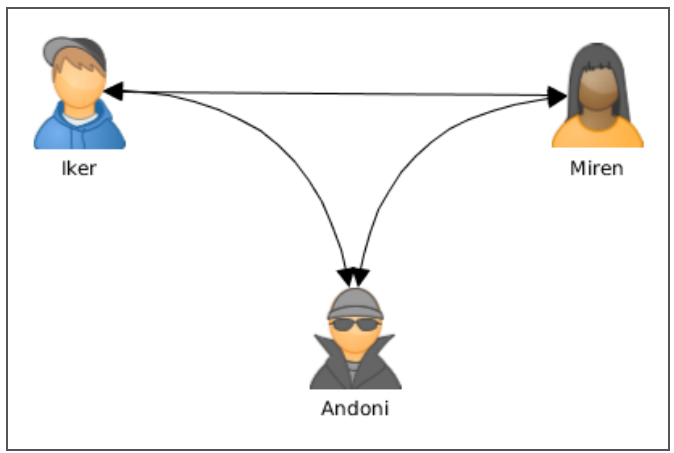
Criptografía de clave pública

¿Qué ocurre si se interpone alguien en las comunicaciones?

Ataque Man in the middle:

- Un intermediario recibe todos los mensajes sin que las otras partes se enteren
- Se necesita interceptar todas las comunicaciones entre las dos partes

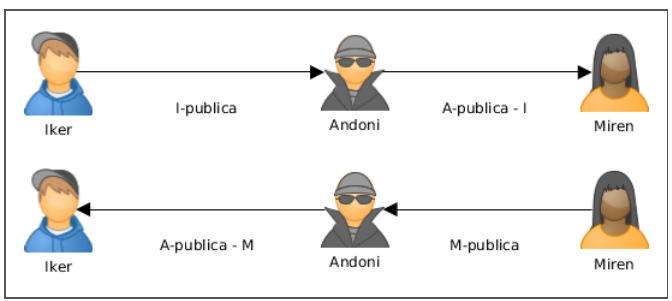
Criptografía de clave pública



Criptografía de clave pública

Cuando Iker y Miren quieren comenzar a comunicarse de manera secreta, se intercambian las respectivas claves públicas

Andoni las intercepta y las intercambia por la suya

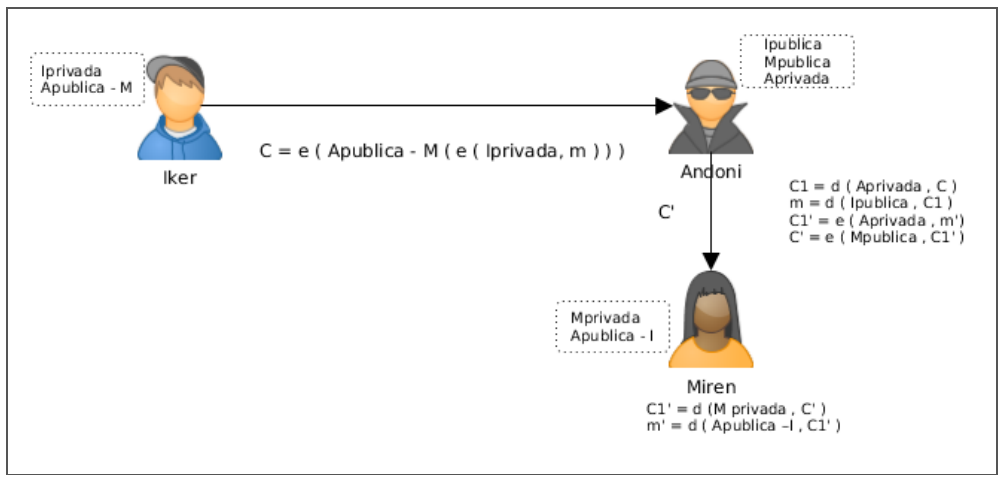


Criptografía de clave pública

Iker y Miren cifran sus mensajes con la que CREEN la clave pública del otro y con su clave privada

Andoni intercepta los mensajes, los lee, modifica y los encripta con su clave privada

Criptografía de clave pública



Criptografía de clave pública

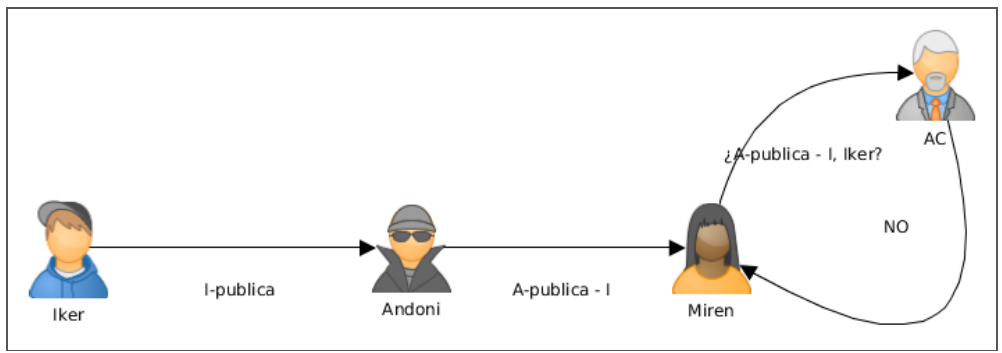
Iker y Miren creen que están comunicándose de manera segura

Andoni está enterándose de todo y modificándolo a su antojo

Formas de evitarlo:

- Paso de claves en canales "seguros"
- Uso de una autoridad que certifique que una clave pública pertenece a quien dice: Autoridad de Certificación (AC)

Criptografía de clave pública



Cifrado híbrido

Los sistemas de clave secreta son mucho más rápidos que los de clave pública

Muchas veces se usa una combinación: El sistema de clave pública se usa para compartir una clave secreta S que sólo se usa una vez

El sistema de clave secreta usa S para cifrar el mensaje

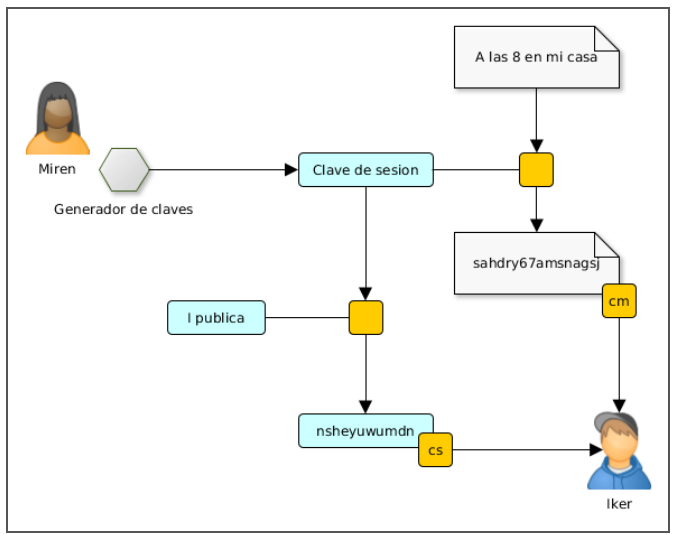
Cifrado híbrido

Miren genera una clave secreta S y cifra su mensaje usándola: cm = e1 (m,S)

Miren cifra S usando la clave pública de Iker cs = e2 (S , $I_{pública}$)

Miren manda [cm, cs] a Iker

Cifrado híbrido



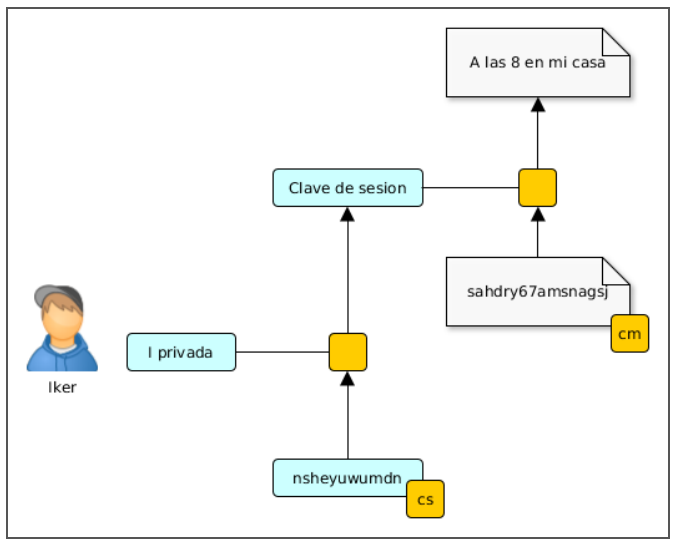
Cifrado híbrido

Iker recibe [cm , cs]

Iker descifra S usando su clave privada $I_{privada}$: d2 (cs , $I_{privada}$) = S

Iker descifra m usando S: d1 (cm , S) = m

Cifrado híbrido



Firma digital

Miren le manda un mensaje a Iker usando un sistema de clave pública

Nadie puede leer el mensaje de Miren a Iker pero cualquiera podría haberlo mandado

¿Cómo sabe Iker que se lo ha mandado Miren o que nadie lo ha modificado?

Solución: Miren firma sus mensajes

Firma digital

Sólo el usuario legítimo puede firmar su documento

Nadie podrá falsificar una firma

Cualquiera puede verificar una firma digital

Firma digital

No se puede reutilizar una firma

No se puede modificar una firma

No se puede negar haber firmado un documento

No se puede alterar un documento después de haberlo firmado

Logramos Autenticidad, Integridad y No repudio

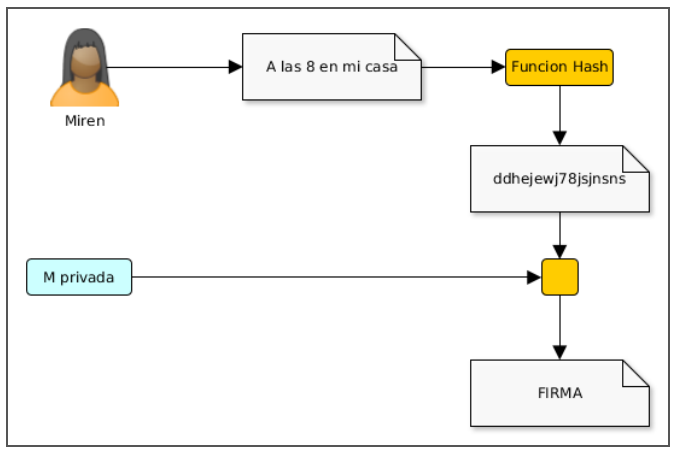
Firma digital

Miren obtiene un resumen criptográfico del mensaje: RC = hash (m)

Miren cifra el resumen criptográfico con su clave: Firma = e (RC, $M_{privada}$)

Miren envía el mensaje (cifrado o sin cifrar) y su Firma

Firma digital



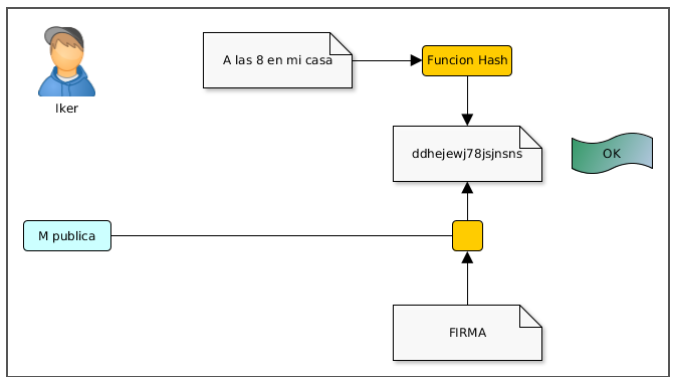
Firma digital

Iker desencripta la Firma usando la clave pública de Miren: RC = (Firma, $M_{pública}$)

Iker obtiene el resumen criptográfico del mensaje: RC’ = hash (m)

Iker compara RC’ con RC para asegurarse que no ha sido modificado

Firma digital



Firma digital

Si además de firmarlo, Miren encripta su mensaje sólo Iker podrá leerlo: Se logra Confidencialidad, Autenticidad, Integridad y No Repudio

Puede hacerlo usando:

- Un sistema de criptografía asimétrica
- Un sistema de criptografía híbrido

Firma digital

Un sistema de criptografía asimétrica. Enviaría a Iker:

- Criptograma del mensaje cifrado con $M_{privada}$ y con $I_{pública}$
- Su Firma digital (el resumen criptográfico cifrado con $M_{privada}$)

Firma digital

Un sistema de criptografía híbrido. Enviaría a Iker:

- Criptograma del mensaje cifrado con la clave de sesión
- Criptograma con la clave de sesión cifrada con $I_{pública}$
- Su Firma digital (el resumen criptográfico cifrado con $M_{privada}$)

Algoritmos de clave pública

Diffie-Hellman - 1976

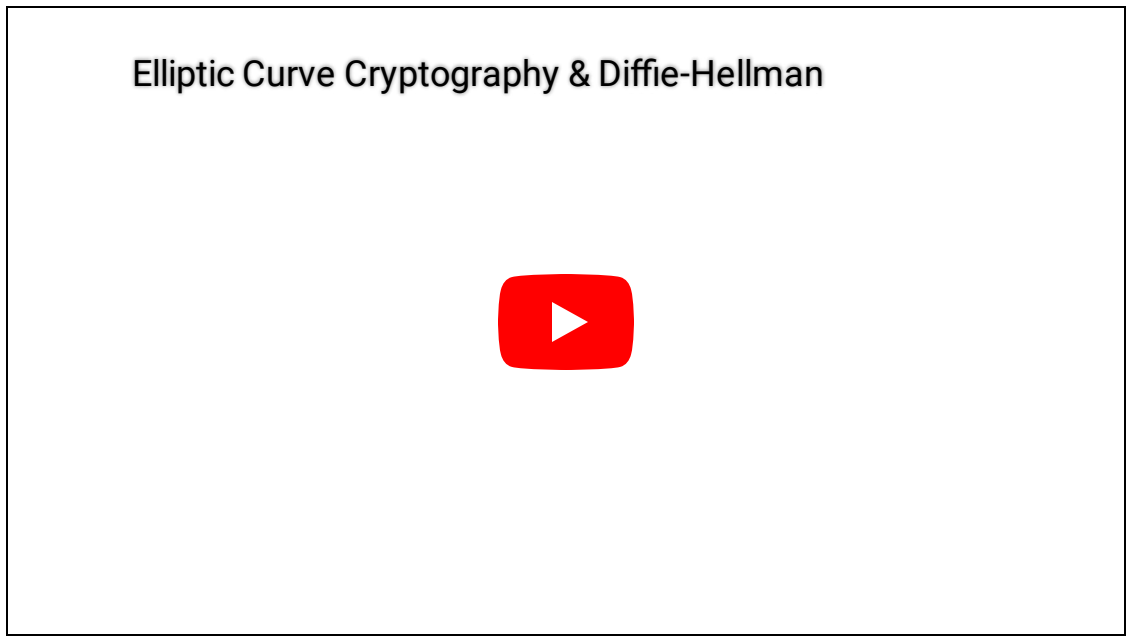
RSA - 1977

ElGamal - 1984

DSA - 1991

Curvas elípticas - 1985

Algoritmos de clave pública



Algoritmos de clave pública

Algoritmos de clave pública

DNI electrónico (DNIe 3.0):

- RSA
- SHA-1 / SHA-256
- TripleDES / AES

Algoritmos de clave pública

PGP:

- RSA / DSA
- IDEA / TripleDES

Algoritmos de clave pública

SSH:

- RSA / DSA

SSL / TLS:

- RSA / DSA / Diffie-Hellman
- IDEA / DES / TripleDES /AES

Confianza de firmas

Aunque utilicemos firmas digitales:

- ¿Cómo sabemos que la firma es de quien dice ser?
- ¿Cómo nos asegura una autoridad de certificación que una firma es de quien dice ser?
- ¿No podemos fiarnos de una firma que no esté avalada por una autoridad de certificación?

Confianza de firmas

- Se usa en PGP, GnuPG y similares
- Un usuario certifica (firmando con su clave privada) que la clave pública de otro usuario es de confianza
- La confianza se propaga según la confianza que demos a los usuarios que firmen las claves

Niveles de confianza

- Desconocido: no nos fiamos de nada que firme ese usuario (por desconocimiento)
- Ninguno: no nos fiamos de nada que firme ese usuario (porque sabemos que lo hace mal)
- Marginal: nos fiamos de las claves firmadas por dos usuarios con confianza marginal
- Absoluto: nos fiamos de todo lo firmado por ese usuario

Certificados digitales

- Un certificado digital consiste en que una entidad “de confianza” firme mediante su clave privada, la clave pública de un usuario
- Sirve para certificar que el usuario es quien dice ser
- Depende de la confianza en la entidad que lo certifica

Certificados digitales

- Siguen el estándar X.509
- Validez != Confianza
  - Validez: cumple los requisitos de una firma (caducidad, etc.)
  - Confianza: nos podemos fiar de esa firma
- Una firma puede ser válida, pero no de confianza
- Una firma de confianza que no sea válida no tiene sentido

Certificados digitales

Una autoridad de certificación (AC) certifica la validez de una firma

- Prestadores de Servicios de Certificación (PSC): Ley de Firma Electrónica (Ley 59/2003, LFE), Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (Ley 11/2007, LAESCP)
- Los PSCs deben proporcionar un método de consulta de la vigencia de sus certificados: Sólo las Administraciones Públicas tienen la obligación de que sea gratuito

Certificados digitales

Jerarquía de certificación (RFC 1422)

Internet Policy Registration Authority (IPRA) >> Policy Certification Authorities (PCA) >> Certification Authorities (CA): Verisign, Thawte, GeoTrust, RapidSSL, DigiCertSSL

Un AC debe

- Mantener una base de datos de nombres distinguidos (ND) y de ACs subordinadas
- Permitir la revocación de certificados:
  - Clave privada del usuario comprometida
  - AC ha emitido un certificado a quien no debía
  - El usuario cambia de AC
  - Violación de la seguridad de la AC
- CRL, Certification Revocation List: ejemplo GeoTrust

Un AC debe

- El protocolo OCSP (Online Certificate Status Protocol RFC 2560) permite validar el estado de un certificado digital de manera online
- Es más eficiente que la verificación mediante Listas de Revocación de Certificados (CRL)
- Ventaja: su actualización constante
- Desventaja: necesidad de conexión para la comprobación

Certificados digitales

Cada AC que proporciona el servicio, mantiene un servidor OCSP

Este servicio responde a las aplicaciones cliente que remitan una petición estandarizada y sepan interpretar la respuesta

Certificados digitales

Tipos de certificados de clave pública:

- Certificado de autoridad
- Certificado de servidor
- Certificado personal
- Certificado de productor de software

Certificados digitales

Componentes de un certificado:

- Versión
- Número de serie
- Identificador del algoritmo de firmado
- Nombre del emisor
- Periodo de validez
- Nombre del sujeto

Certificados digitales

Con un certificado digital conseguimos:

- Confidencialidad al poder encriptar la información
- Integridad al poder realizar hash de la información y poder firmarla
- Autenticidad al venir firmada la información
- No repudio al firmar la información