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

A principios de los 70 surgen los sistemas criptográficos asimétricos como solución al problema de compartir la clave en sistemas simétricos

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

Criptografía de clave pública

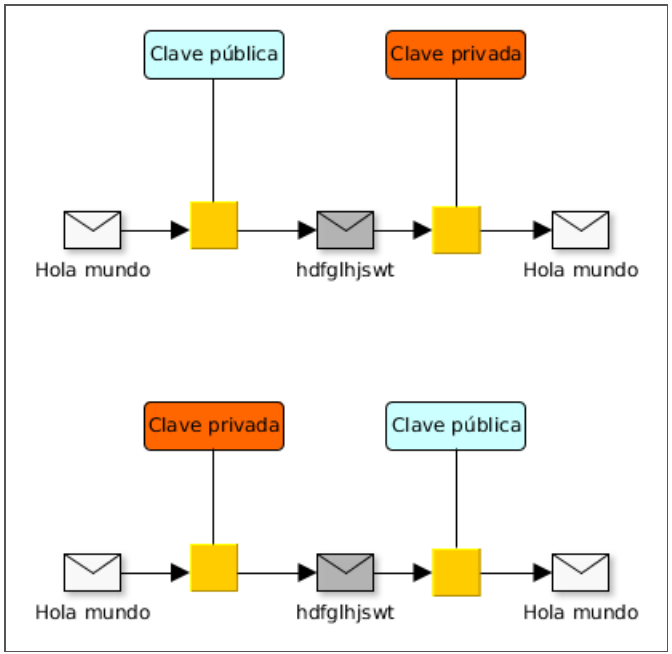
Dos claves por usuario:

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

Están relacionadas matemáticamente

Lo que una clave cifra sólo lo puede descifrar la otra

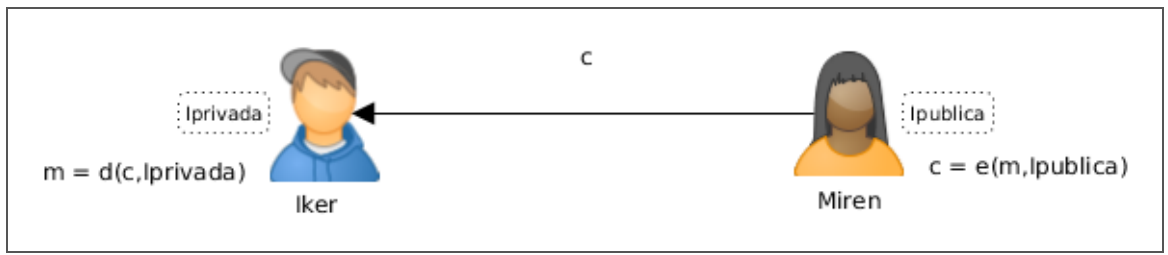
Criptografía de clave pública



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



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 deducir 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?

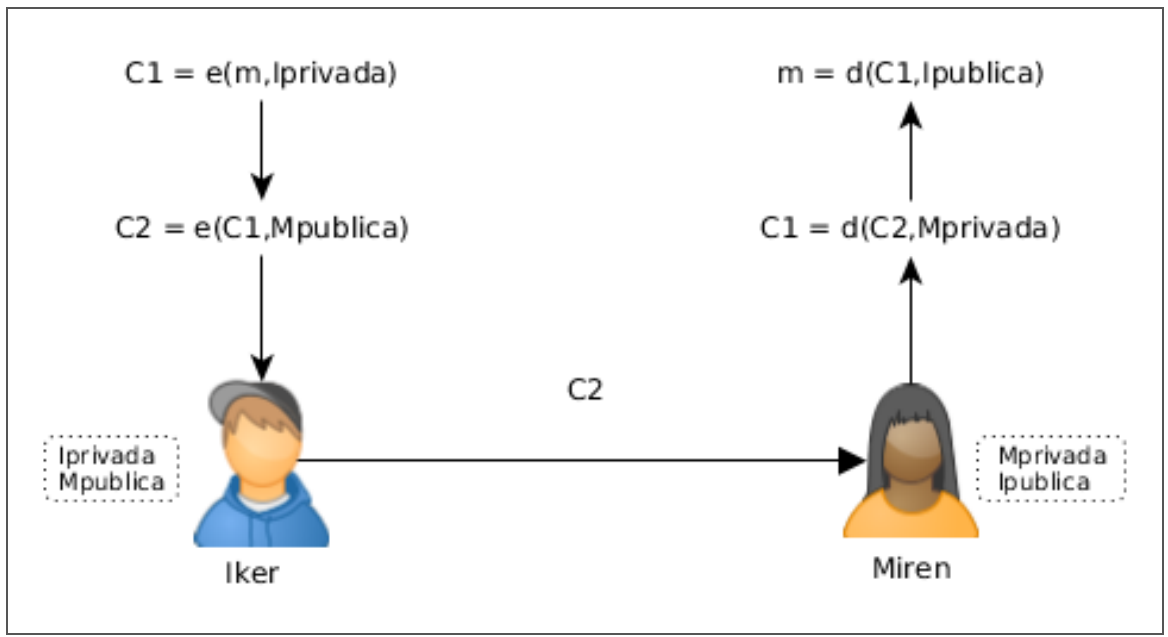
Criptografía de clave pública

- Si Iker lo cifra con su clave privada lo puede descifrar cualquiera (Todo el mundo conoce $I_{pública}$)
- 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



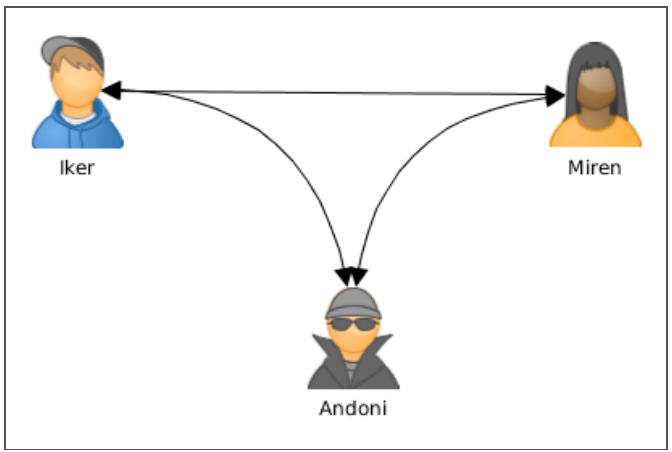
Criptografía de clave pública

¿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

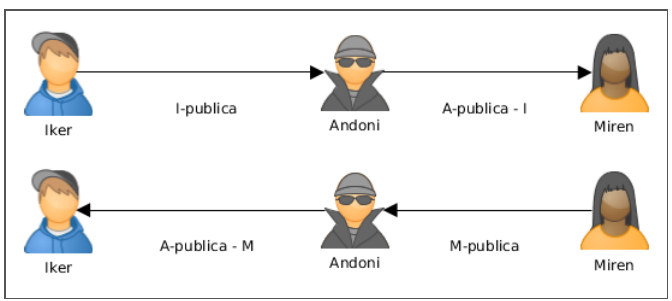
Criptografía de clave pública



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

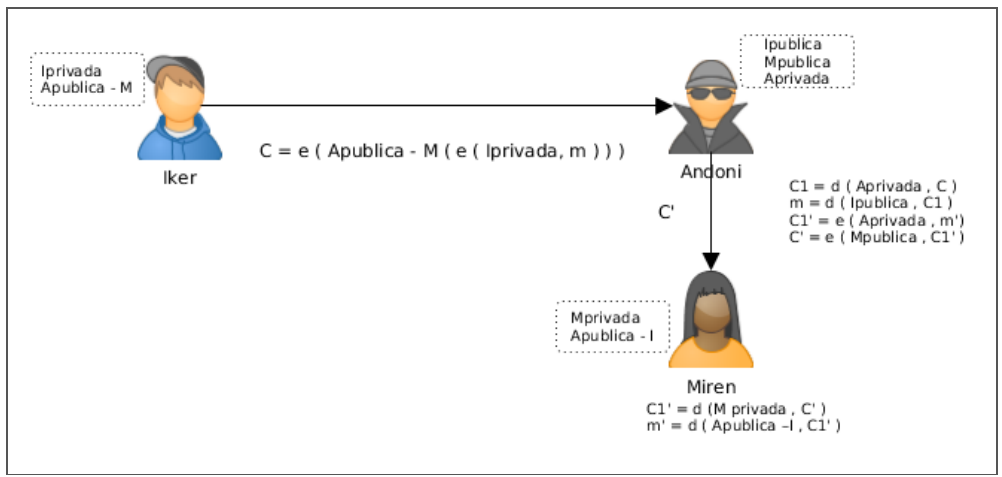


Criptografía de clave pública

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

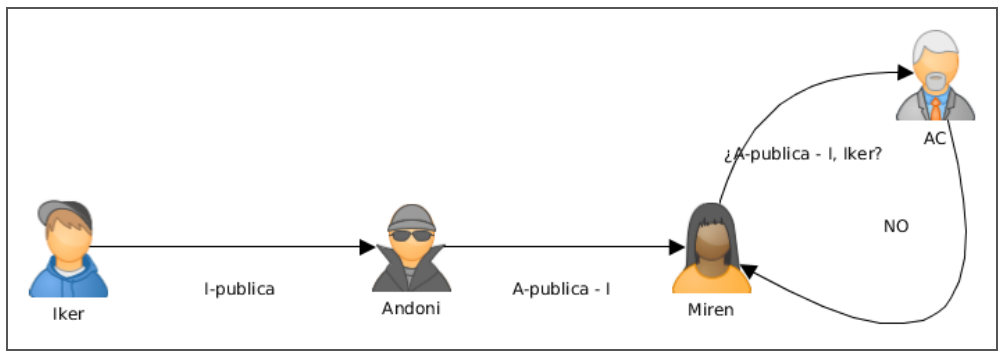
Iker y Miren creen que están comunicándose de manera segura

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

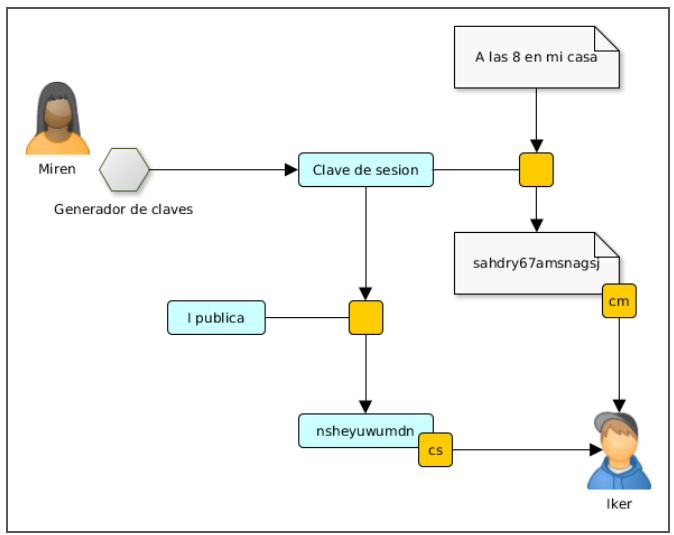
Cifrado híbrido

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



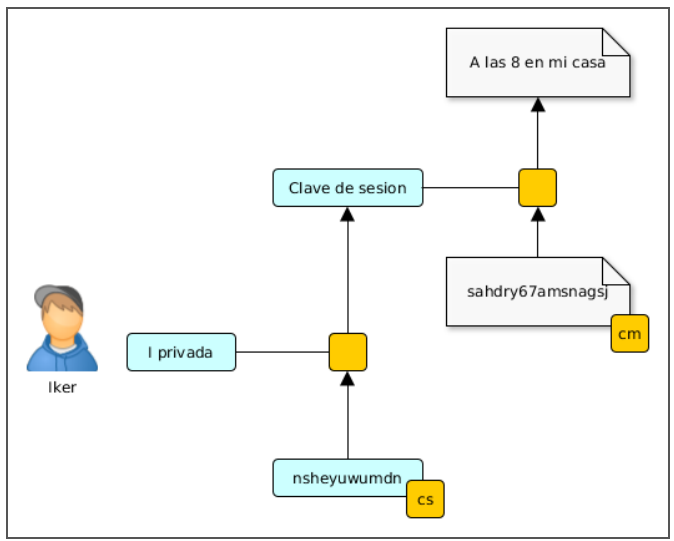
Cifrado híbrido

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



Algoritmos de clave pública

- Diffie-Hellman
- RSA
- ElGamal
- DSA
- Curvas elípticas

Diffie-Hellman

- 1976
- Intercambio de claves, sistemas hibridos

RSA

- 1977: factorización de números primos grandes

RSA

Encryption and HUGE numbers - Numberphile

ElGamal

- 1984

Basado en Diffie-Hellman

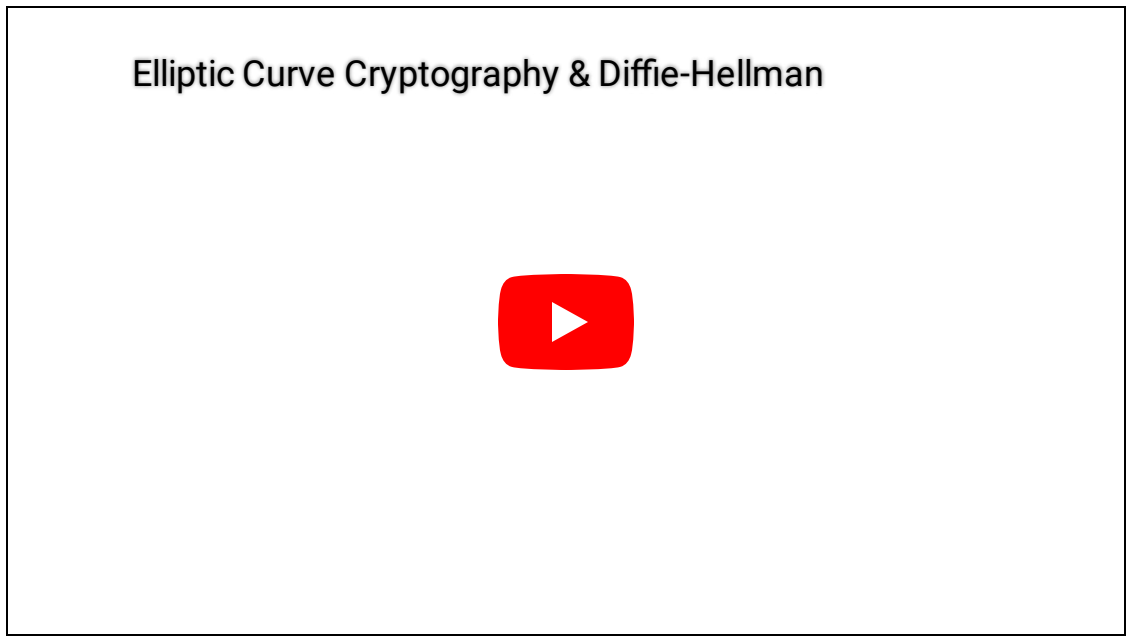
DSA

- 1991

Curvas elípticas

- 1985

Curvas elípticas



Algoritmos de clave pública

- DNI electrónico
- PGP
- SSH
- SSL / TLS

DNI electrónico (DNIe 3.0) COGER DEL LIBRO!!!!

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

PGP

- RSA / DSA
- IDEA / TripleDES

SSH

- RSA / DSA

SSL / TLS

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