TOR

Introducción a Onion Routing y Hidden Services

Marco Antonio Garrido Rojo[1]

4 de diciembre de 2017

[1] https://github.com/MaSteve/TOR

¿Qué es TOR?

- Tor (acrónimo de The Onion Router) es un software para establecer comunicaciones anónimas a través de Internet.
- Su objetivo es proporcionar a sus usuarios un modo de comunicación confidencial.
- Basado en el principio de "onion routing" desarrollado por el gobierno de Estados Unidos en los 90.
- Más información sobre el proyecto: `torproject.org`

¿Qué vamos a aprender hoy?

- Fundamentos del “onion routing”.
- Fundamentos de los Hidden Services.
- **No** vamos a hablar de Deep Web.

Criptografía: breve repaso

- Tor no obliga a encriptar la comunicación. Canal anónimo no es lo mismo que mensaje oculto.
- Necesita hacer uso de la criptografía para garantizar el anonimato.
- Diffie-Hellman + Criptografía de dos claves (clave pública).

Criptografía: breve repaso

- Diffie-Hellman es un método de establecimiento seguro de claves.
- A partir de una información conocida por todos (incluso por un man in the middle) se comparte un secreto conocido solo por los dos extremos.

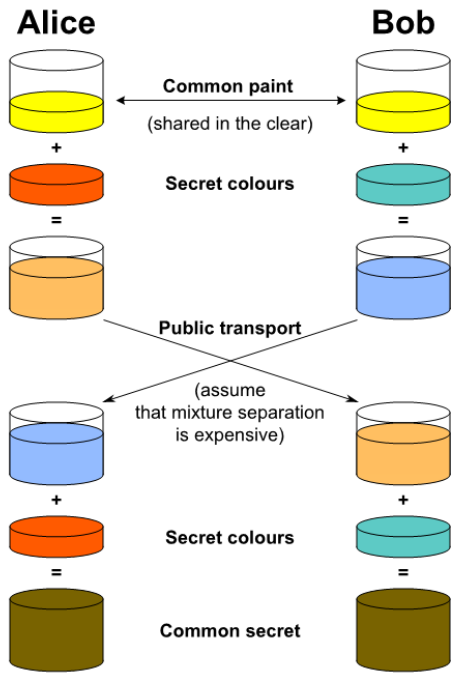


Figura: Illustration of the idea behind Diffie-Hellman key Exchange (Wikipedia)

Criptografía: breve repaso

- La criptografía de clave pública garantiza una comunicación unidireccional segura.
- El emisor puede encriptar mensajes usando la clave pública. Solo el receptor puede descifrar el mensaje con la clave privada.

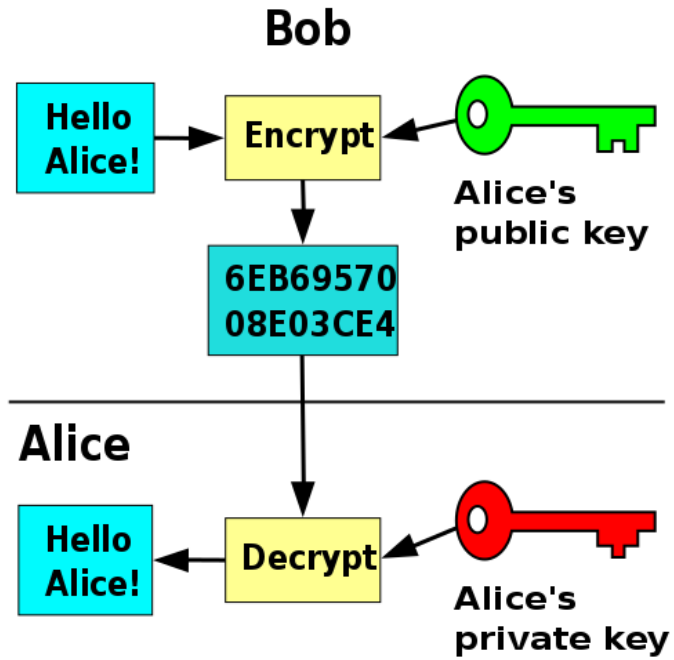
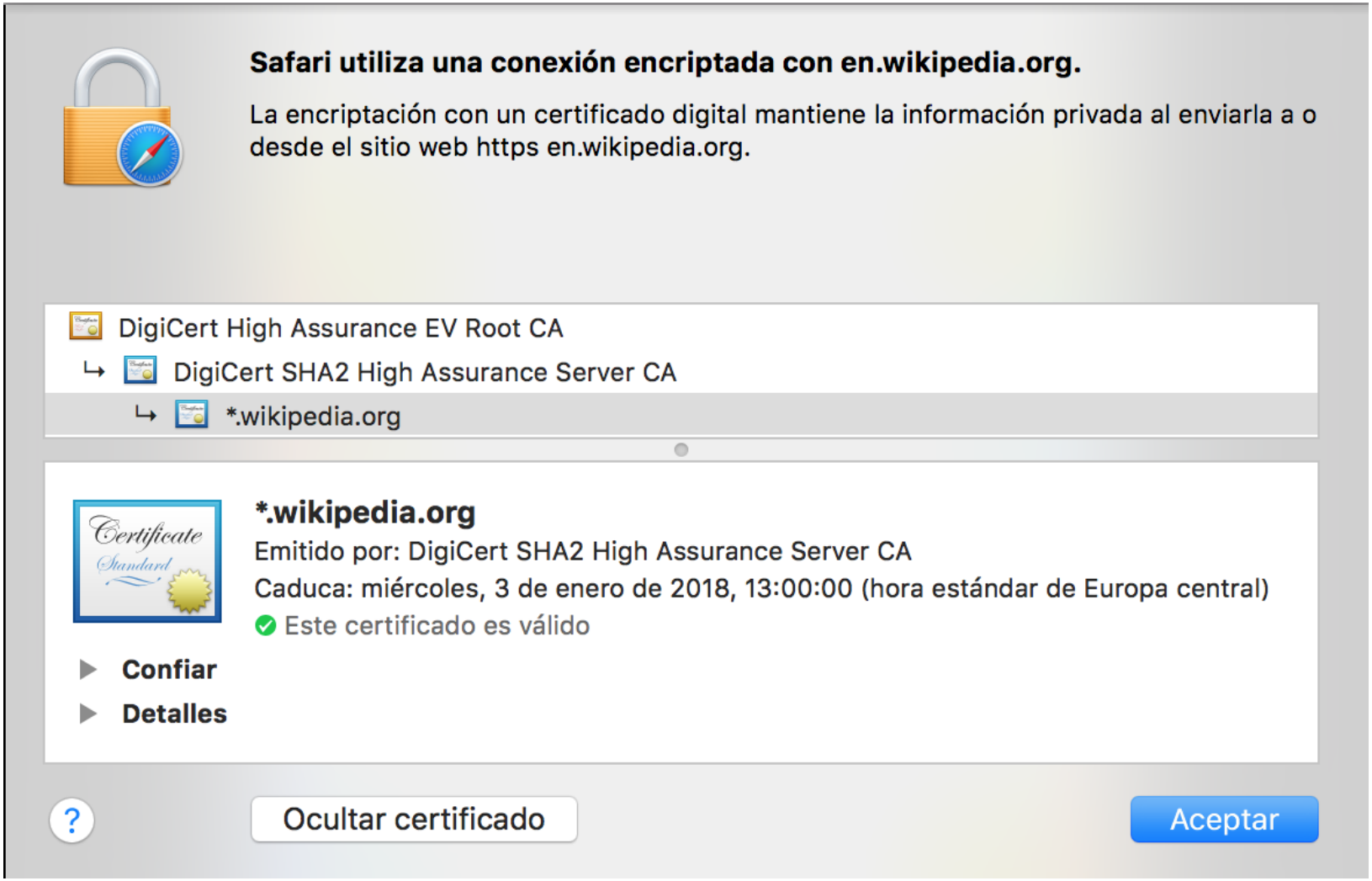


Figura: Illustration of Public-key cryptography (Wikipedia)

Criptografía: breve repaso



¿Qué problema queremos resolver?

- Alice (cliente) quiere hablar con Bob (servidor) sin que nadie sepa que ambos están hablando.
- No puede haber una conexión directa (man in the middle).
- Un VPN o un proxy actúan de puente pero conocen los extremos (hay que confiar).
- Una red de proxies parece ser la solución (con cuidado). Hay que garantizar que el usuario es completamente anónimo (nodos públicos y conocidos).
- Cada nodo solo puede conocer lo justo y necesario.
- "Onion routing" es la solución.

¿Qué problemas tiene?

- Comunicación no cifrada al final de la cadena (HTTP).
- Javascript puede obtener datos del cliente (MAC + IP).
- DNS sin Tor (fin de la magia).
- Escuchar mensajes al principio y al final de la cadena + Estadística.

¿Qué son los Hidden Services?

- ¿Qué ocurre si soy un servidor?
- Alice y Bob quieren permanecer ocultos en sus casas y comunicarse al mismo tiempo.
- Los Hidden Services solucionan este problema.
- ¿Cómo? "Onion routing" + Tabla hash de descriptores distribuida.

Preguntas

¿Preguntas? No os cortéis, es vuestro momento.