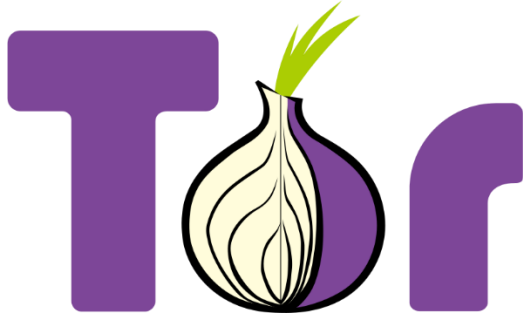


Tor Onion Routing



ReadMe :

Este documento explicará el funcionamiento del enrutamiento de cebolla (onion routing) en el servicio de Tor. El objetivo es detallar qué es Tor, cómo funciona, qué tecnologías y protocolos están involucrados, así como el manejo del tráfico y el uso de la criptografía.

[🔍] ¿Qué es Tor?

Tor (The Onion Router) es una red diseñada para proporcionar anonimato en Internet. Su objetivo es ocultar la identidad y la ubicación del usuario mediante un sistema de enrutamiento en capas, similar a las capas de una cebolla. Permite acceder a sitios web sin revelar la dirección IP real del usuario y también facilita el acceso a una web con contenido no indexado en navegadores convencionales a través de dominios “.onion”.

[?] ¿Cómo surgió y quién lo desarrolló?

Tor fue desarrollado inicialmente en la década de 1990 por el Laboratorio de Investigación Naval de EE.UU. como parte de un proyecto para proteger las comunicaciones gubernamentales. Posteriormente, el código fuente se hizo público y en 2002 se lanzó Tor como un proyecto de código abierto. En 2006, **The Tor Project**, una organización sin fines de lucro, tomó el control del desarrollo y mantenimiento de la red.

Si quieres saber mas detalles de la historia puedes acceder al link oficial de tor para mayor información: <https://www.torproject.org/es/about/history/>

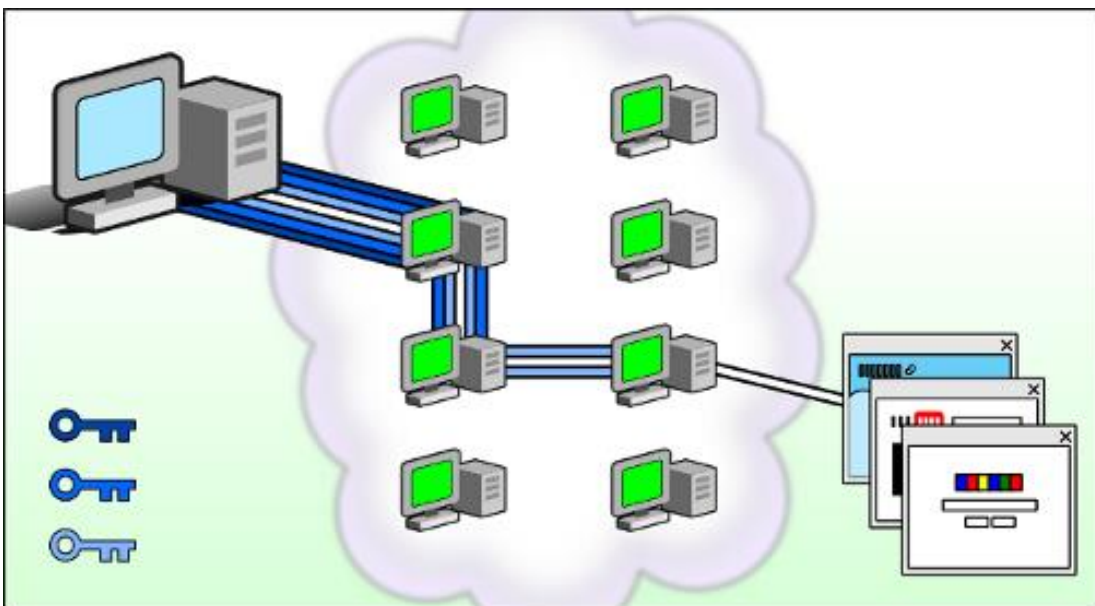
[🦉] Red Tor P2P

Tor es una plataforma de **software y una red de hosts P2P** que funcionan como enrutadores de Internet en la red Tor. La red Tor permite a los usuarios navegar por Internet de forma anónima. Los usuarios tienen acceso a la red Tor mediante un navegador especial o utilizando otro navegador e implementando un proxy con el servicio de Tor. Cuando se inicia una sesión de navegación, el navegador construye una ruta de extremo a extremo en capas a través de la red del servidor Tor que está encriptada. Cada capa encriptada se “pela” como las capas de una cebolla a medida que el tráfico atraviesa un retransmisor/nodo de Tor.



Las capas contienen información encriptada de siguiente salto que solamente puede leer el router que necesita leer la información. De esta manera, ningún dispositivo conoce toda la ruta al destino, y la información de enrutamiento solo puede ser leída por el dispositivo que la necesita.

Finalmente, al final de la ruta Tor, el tráfico llega a su destino de Internet. Cuando el tráfico regresa al origen, se crea una ruta con capas encriptadas nuevamente.



[🍷] ¿Cómo funciona Tor?

Tor usa un sistema de **enrutamiento por capas** que dirige el tráfico a través de una serie de servidores (nodos) distribuidos por todo el mundo. Este proceso se realiza en tres pasos principales:

1. **Entrada en la red:** Cuando un usuario se conecta a Tor, su tráfico pasa primero por un nodo de entrada.

Nodo de Entrada (Entry Node o Guard Relay)

- Es el primer nodo al que se conecta tu navegador Tor.
- Es el único nodo que conoce la **IP real del usuario**.
- **No sabe el destino final**, solo que los datos deben ir al siguiente nodo.
- Se elige con base en su estabilidad y reputación en la red.

2. **Enrutamiento en capas:** Luego, el tráfico se reenvía a través de múltiples nodos intermedios, cada uno de los cuales solo conoce el nodo anterior y el siguiente, sin saber el destino final.

Nodo Intermedio (Middle Relay)

- Actúa como un puente entre el nodo de entrada y el de salida.
- **Solo conoce la dirección del nodo anterior y del siguiente.**
- Su función es romper la relación entre el nodo de entrada y el de salida.
- No tiene acceso al contenido del tráfico (ya que sigue cifrado).

3. **Nodo de salida:** Finalmente, el tráfico sale por un nodo de salida y llega a su destino (por ejemplo, una página web).

Nodo de Salida (Exit Node)

- Es el último nodo por donde el tráfico sale a Internet.
- **Es el único nodo que se comunica con el destino final** (como un sitio web).
- Puede ver el contenido del tráfico si no está cifrado (HTTP en vez de HTTPS).
- Es el nodo más riesgoso, ya que la IP del nodo de salida es la que verá el destino final.

📌 Tú → ● Nodo de entrada → ● Nodos intermedios → ● Nodo de salida → 🌐 Internet

[🔒] ¿Cómo funciona el cifrado en Tor?

Tor usa dos tipos de cifrado para implementar su sistema de capas.

Cifrado de tráfico --> clave simétrica

Cifrado de capas --> clave asimétrica

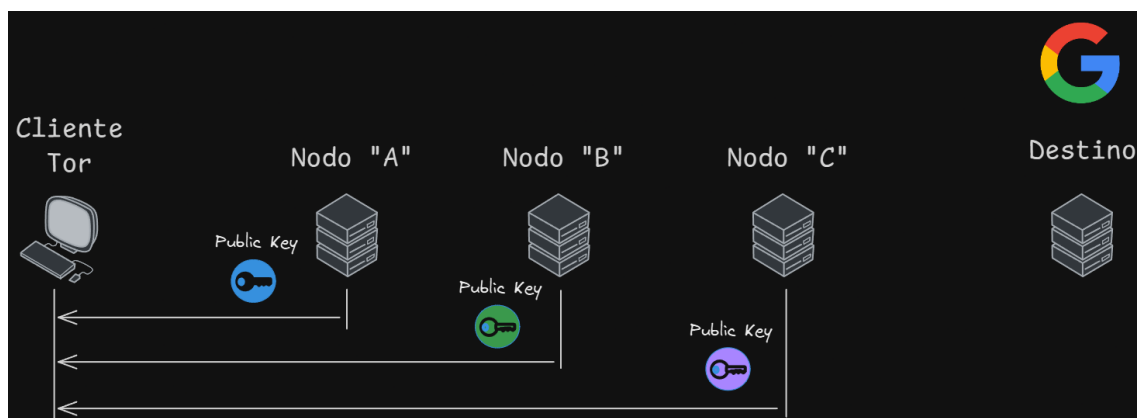
El cifrado simétrico y el cifrado asimétrico son dos técnicas de cifrado de información que usan claves para codificar y decodificar datos.

Tor utiliza clave simétrica (pública) para cifrar el tráfico de cada salto de nodos por la red tor.

Además, utiliza clave asimétrica (pública-privada) para cifrar la información de la dirección IP del siguiente salto del nodo tor.

[🌐] Funcionamiento Onion Routing

Cifrado de capas:



1. Generación de claves asimétricas:

- El cliente Tor selecciona la ruta de nodos intermediarios




- El cliente Tor solicita la clave pública de los nodos intermediarios (ellos tienen su clave privada)
- El cliente Tor cifra en capas para cada nodo de la red
 - Primero, cifra el mensaje con la clave pública del nodo de salida.
 - Luego, cifra ese resultado con la clave pública del nodo intermedio.
 - Finalmente, cifra el resultado con la clave pública del nodo de entrada.



Cifrado de tráfico:



1. Generación de claves simétricas:

- El cliente Tor genera **tres claves simétricas diferentes**:
 -  K_entrada (para el nodo de entrada)
 -  K_intermedio (para el nodo intermedio)
 -  K_salida (para el nodo de salida)

2. Cifrado de las claves simétricas:

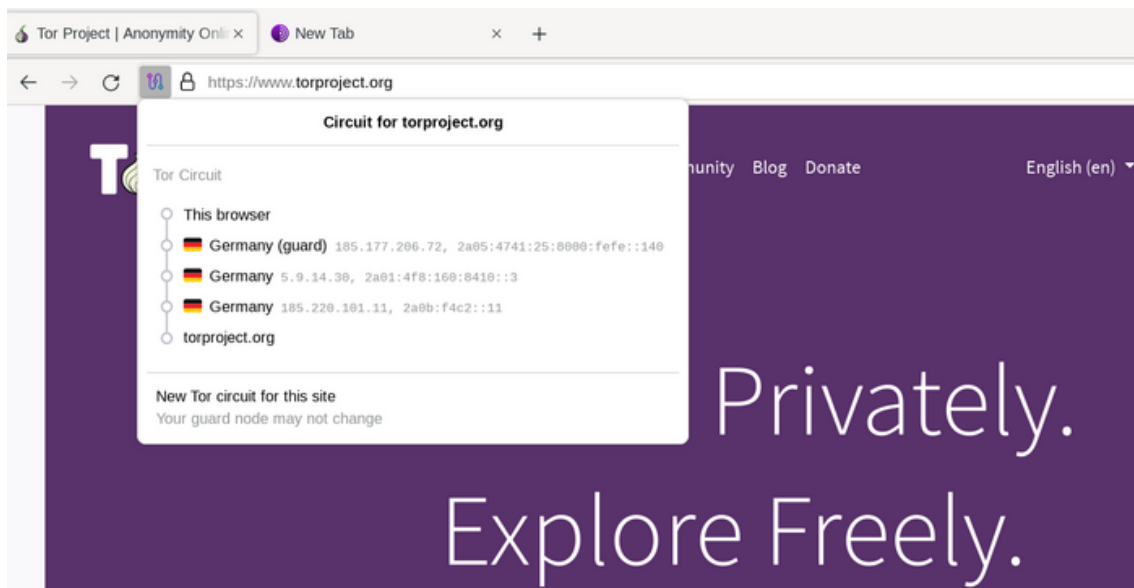
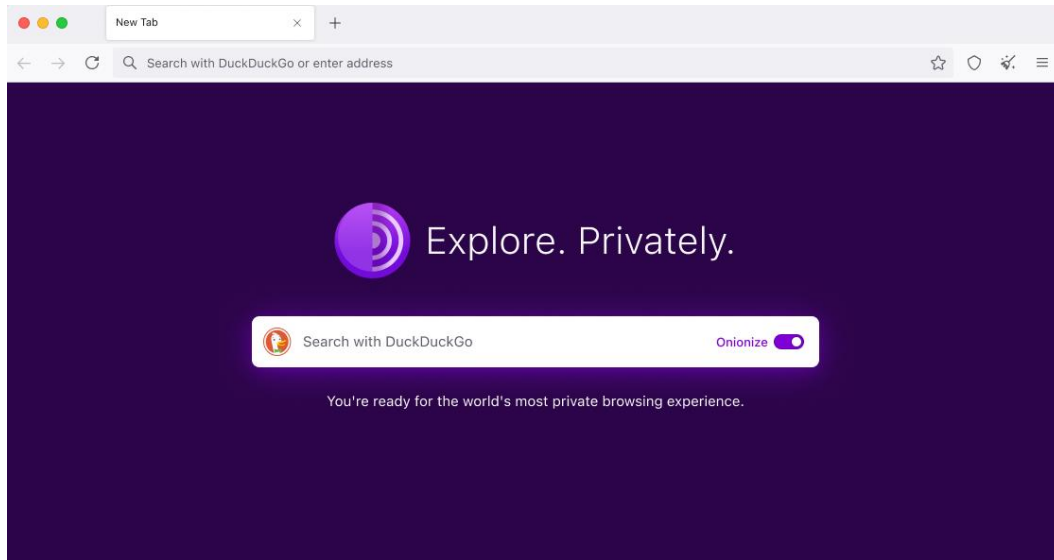
- El cliente cifra K_entrada con la clave pública del nodo de entrada.
- Cifra K_intermedio con la clave pública del nodo intermedio.
- Cifra K_salida con la clave pública del nodo de salida.

¿Qué es Tor Browser?

Tor Browser es un navegador basado en Mozilla Firefox que permite a los usuarios acceder a la red Tor de forma sencilla y segura. Está configurado para minimizar la

huella digital del usuario, bloqueando rastreadores, cookies y protegiendo contra técnicas avanzadas de identificación, como el fingerprinting del navegador.

Este navegador también permite acceder a sitios “.onion”, que no están disponibles en navegadores convencionales como Chrome o Firefox sin el servicio de Tor.



[🔧] Instalar Tor en Kali Linux

✅ Paso 1: Actualizar el sistema

```
sudo apt update && sudo apt upgrade -y
```

✅ Paso 2: Instalar Tor desde los repositorios oficiales

```
sudo apt install tor -y
```

✅ Paso 3: Configurar el servicio de Tor

```
sudo systemctl start tor
```

```
sudo systemctl enable tor
```

```
sudo systemctl status tor
```

```
(kali㉿kali)-[~]
└─$ sudo service tor start
[sudo] password for kali:

(kali㉿kali)-[~]
└─$ service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
   Active: active (exited) since Wed 2022-09-07 08:37:34 EDT; 25s ago
     Process: 7166 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 7166 (code=exited, status=0/SUCCESS)
       CPU: 1ms

Sep 07 08:37:34 kali systemd[1]: Starting Anonymizing overlay network for TCP (multi-inst
Sep 07 08:37:34 kali systemd[1]: Finished Anonymizing overlay network for TCP (multi-inst
```

✅ Paso 5: Instalar Tor Browser (Opcional)

```
sudo apt install torbrowser-launcher -y
```

```
torbrowser-launcher
```

[📢] Contacto

[🔗] <https://www.linkedin.com/in/david-padron-9a74aa323/>

[🔗] <https://github.com/FeathersMcgr4w>

[🔗] <https://feathersmcgr4w.github.io/cyber-portfolio/>