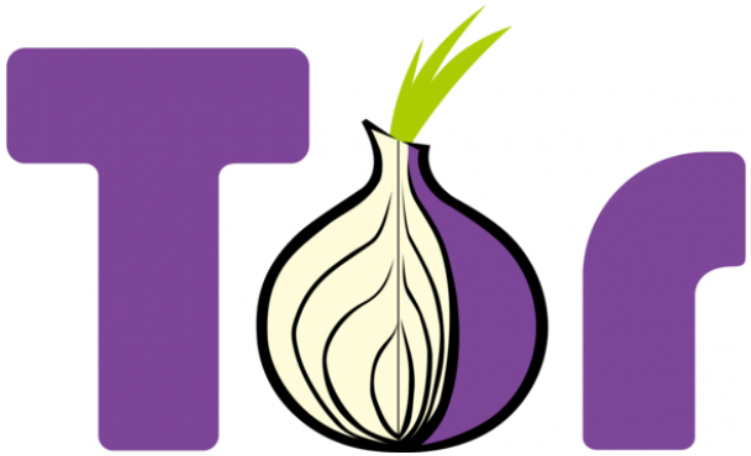


Abbildung1

The OnionRouter

KÖLTRINGER, PREGERNIGG

Übersicht

- Tor-Project
- Tor-Browser
- Anwendungszweck Tor-Browser
- Vor- und Nachteile
- Onion Routing
- Funktionsweise Onion Routing
- Diffie-Hellman-Verfahren
- VPN vs. Onion Routing

Tor-Project

- Nonprofit Organisation
- Private Spenden
- Kostenlose Software
- Privatsphäre schützen
- Analyse des Surfverhaltens

Tor-Browser

- Privates Surfen
- Tracking
- Darknet, Deep Web
- Aktivisten, Journalisten
- Legalität

Tor-Browser vs. herkömmliche Browser

- Provider speichert alle Daten
- "privates Surfen"
- HTTPS
- TCP Protokoll
- End to End Encryption

Deep Web

- Darknet
- Hidden Web
- Suchmaschine
- .onion

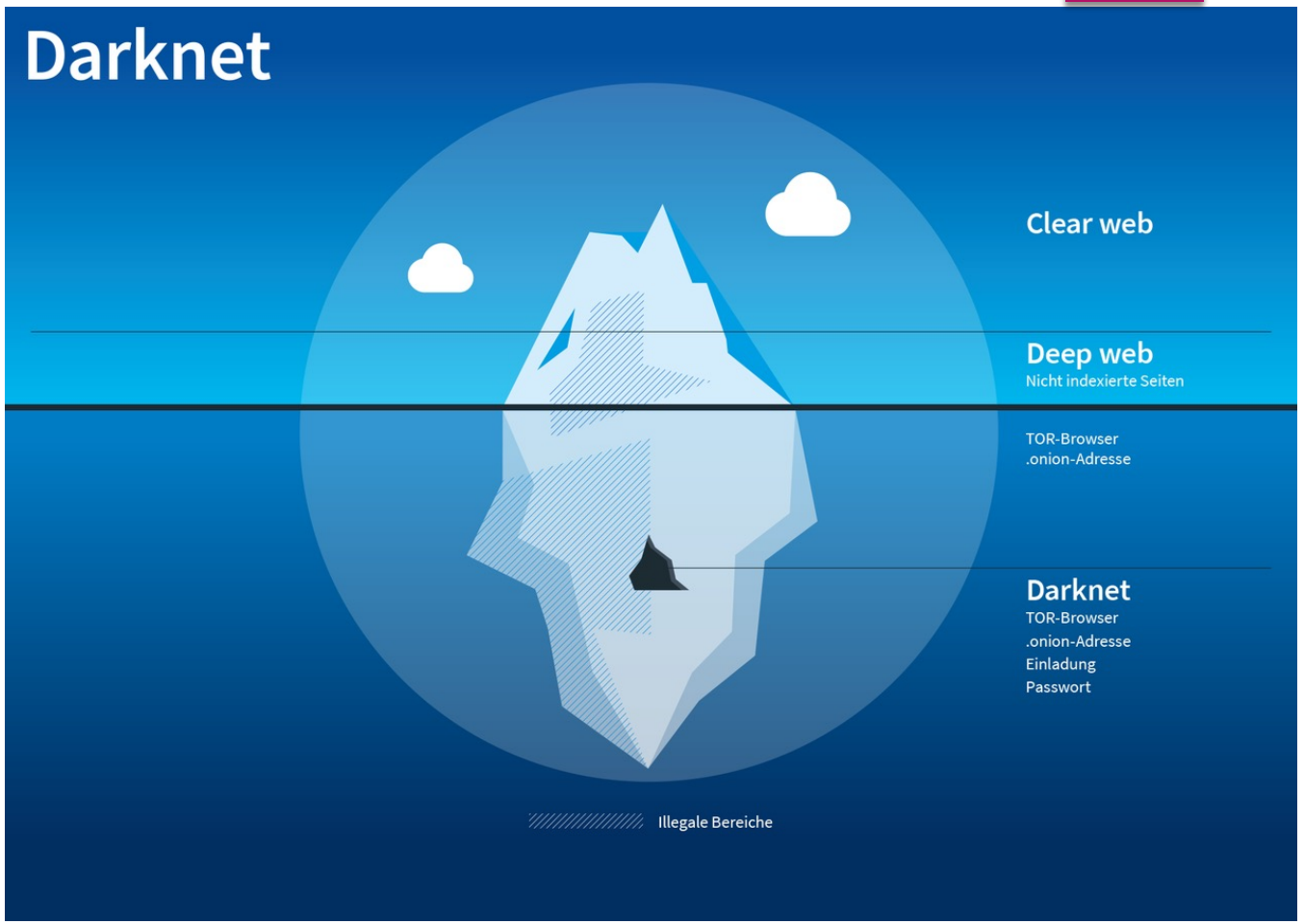


Abbildung 2

Vor- und Nachteile

- Geschwindigkeit
- Nicht zu 100% anonym
- Fußabdruck
- Cookies
- Suchverlauf
- Tracking
- IP-Adressen Verschleierung
- Fehlende Plugins

Onion-Routing

- Knoten
- Guard Node
- Exit Node
- Liste an Servern
- Verschlüsselung
- Zufällig gewählte Route
- Zwiebelschalenprinzip

Guard Node

- Eingangsknoten
- Echte IP-Adresse sichtbar
- Min 2 MBytes/s
- Öffentliche Liste von Tor Knoten
- Werden minütlich aktualisiert
- Anfällig für Angriffe
- Circuit wechseln

Exit Node

- Ausgangsknoten
- Sieht die richtigen Daten zum Ziel
- IP-Adresse ist sichtbar
- Muss sich um Probleme kümmern
- Anfällig für Angriffe

Funktionsweise Onion Routing

- Request
- Circuit
- Nachricht N-mal verschlüsseln
- Guard Node

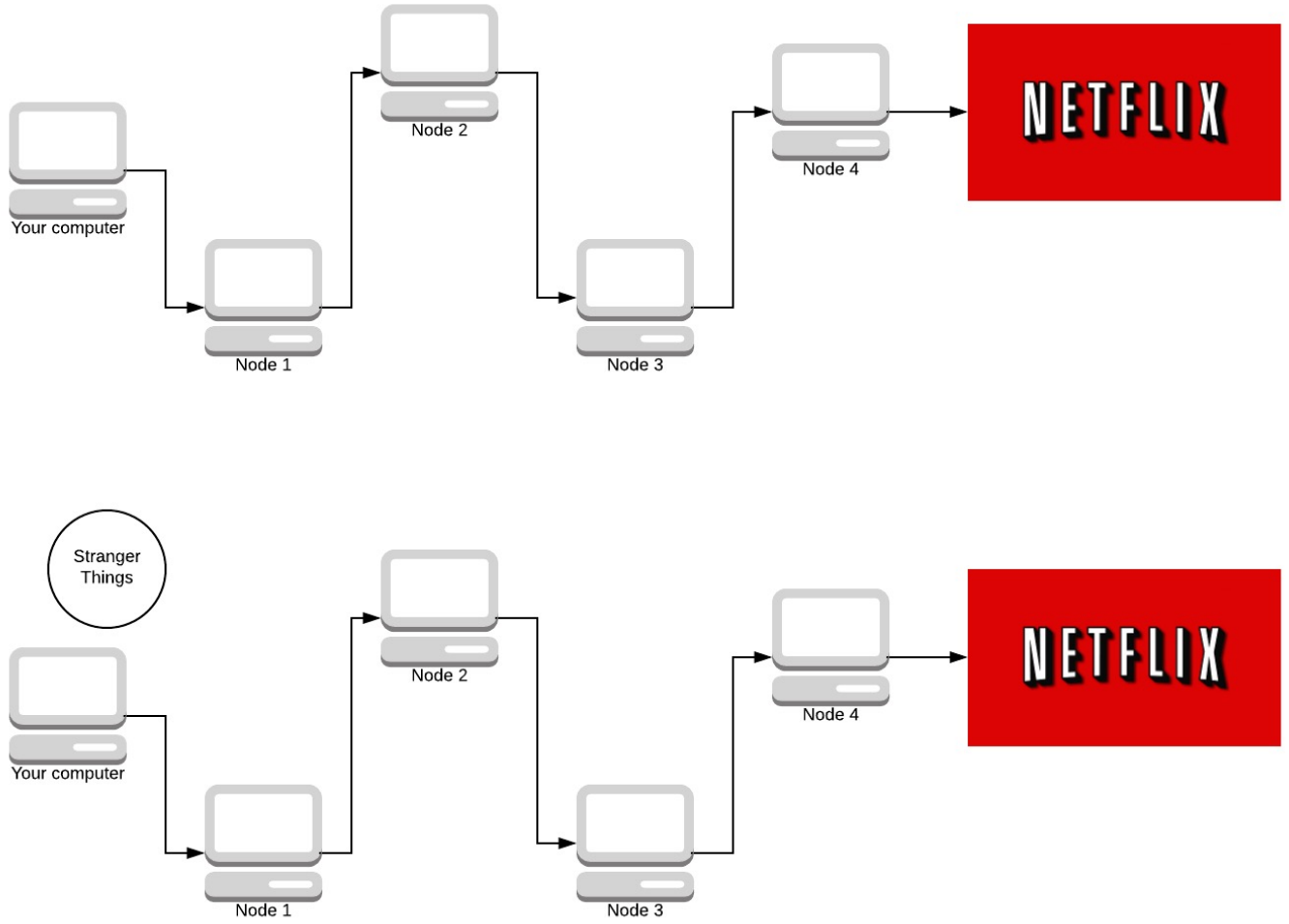


Abbildung 3

Funktionsweise Onion Routing

- 4 Schichten
- Node1 entschlüsselt erste Schicht
- Diffie-Hellman-Verfahren
- Symmetric Key

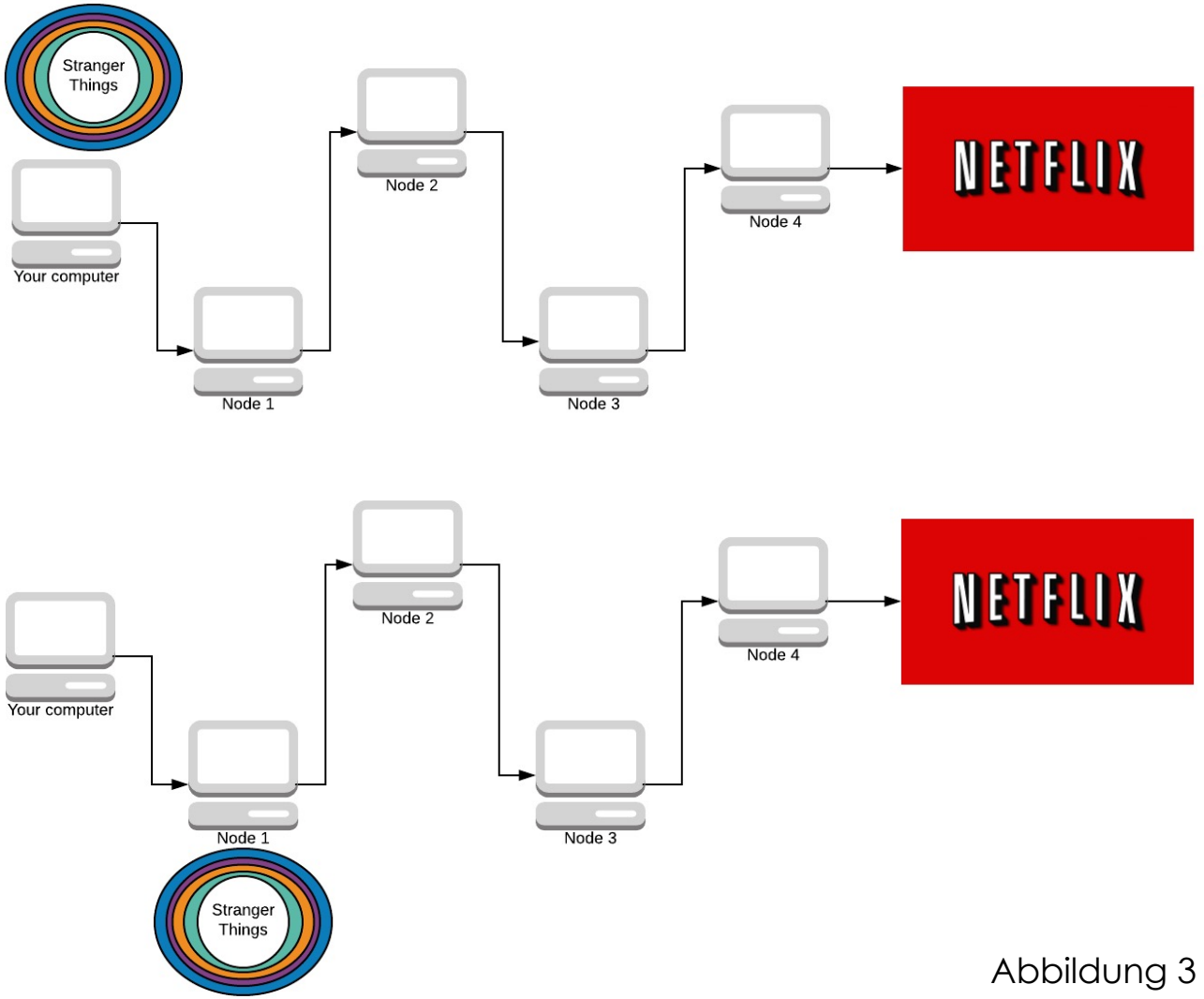


Abbildung 3

Funktionsweise Onion Routing

- Node 1 kennt den Absender
- Kein Inhalt bekannt
- Node 2 kennt den Absender nicht mehr
- Node 2 entschlüsselt zweite Schicht

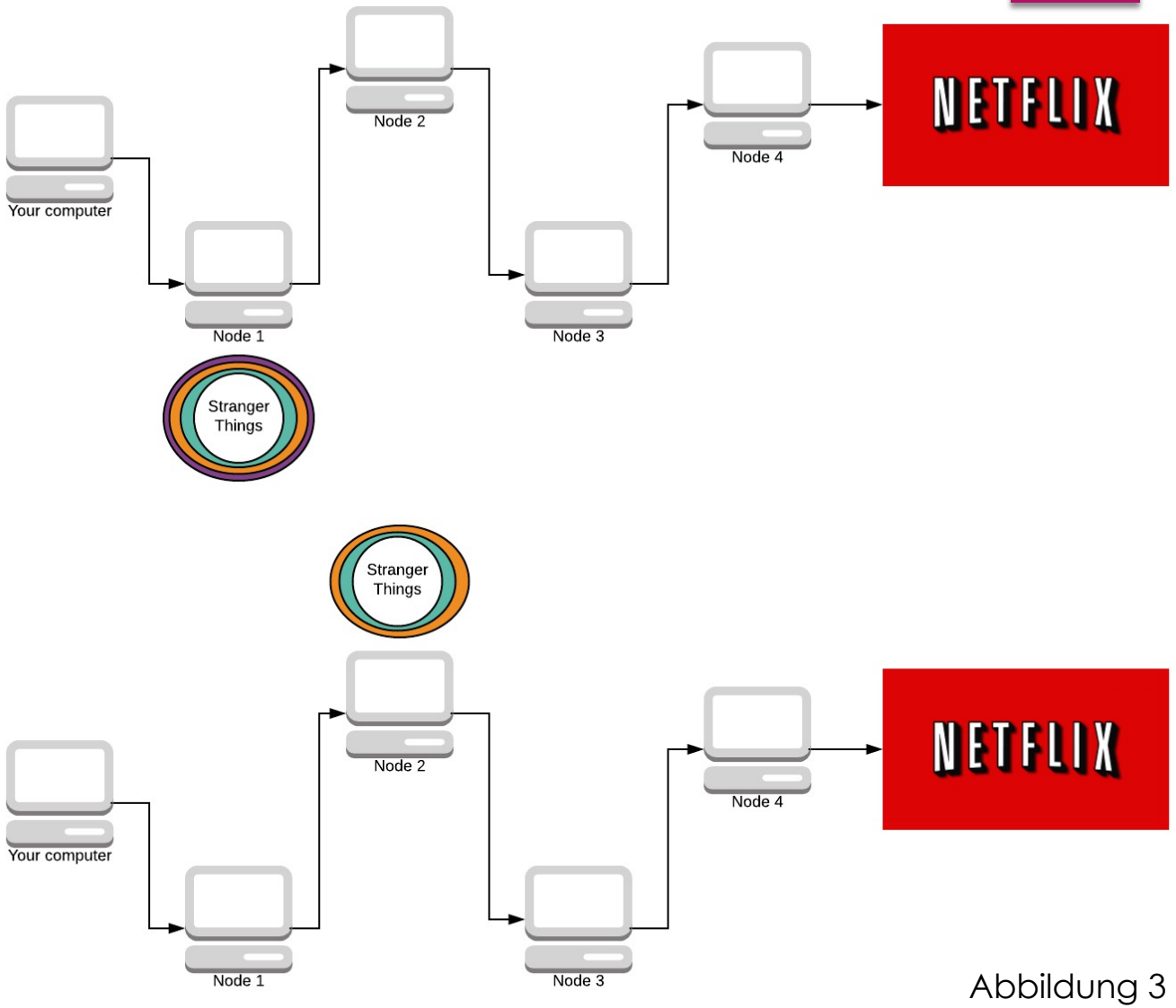


Abbildung 3

Funktionsweise Onion Routing

- Node 3 entschlüsselt dritte Schicht
- Node 4 entschlüsselt letzte Schicht
- Anzahl der Schichten für alle Knoten unbekannt
- Node 4 kennt Nachricht und Empfänger

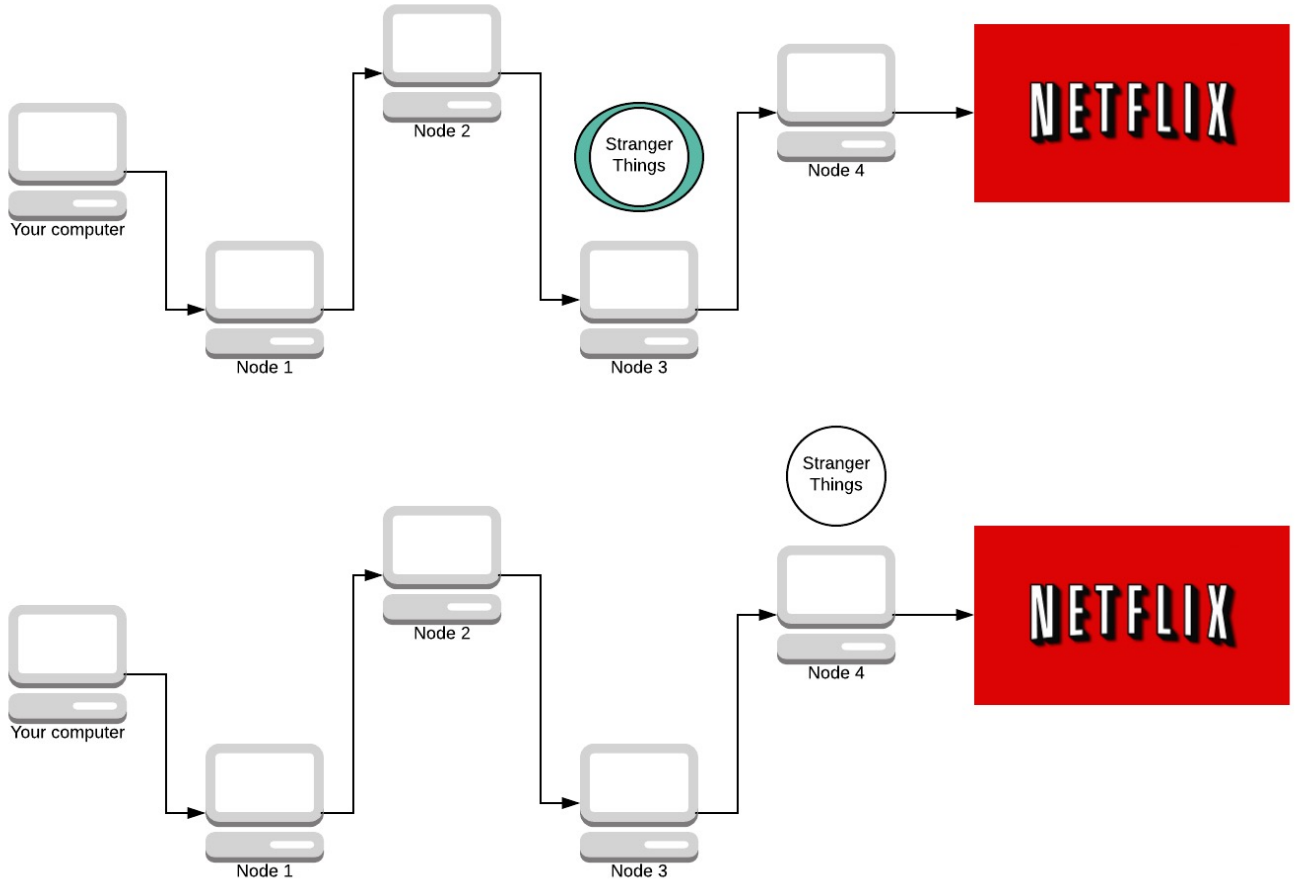


Abbildung 3

Circuit

- Kombination aus Guard Node, Exit Node und Middle Node
- Mindestens 3 Knoten
- Knoten wird immer gewechselt
- Exit Node
- Web Traffic
- Email

Mögliche Gefahren

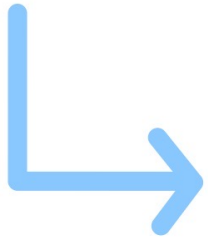
- Man-In-The-Middle
- Guard Node
- Exit Node
- End-To-End-Encryption

Diffie-Hellman-Verfahren

- Geheimer Sitzungsschlüssel
- Ergebnis wird übermittelt
- Tor-Client setzt mit Tor-Server Verschlüsslung fest
- Sitzungsschlüssel wird nie übermittelt
- Mehr Sicherheit gegenüber Angreifern

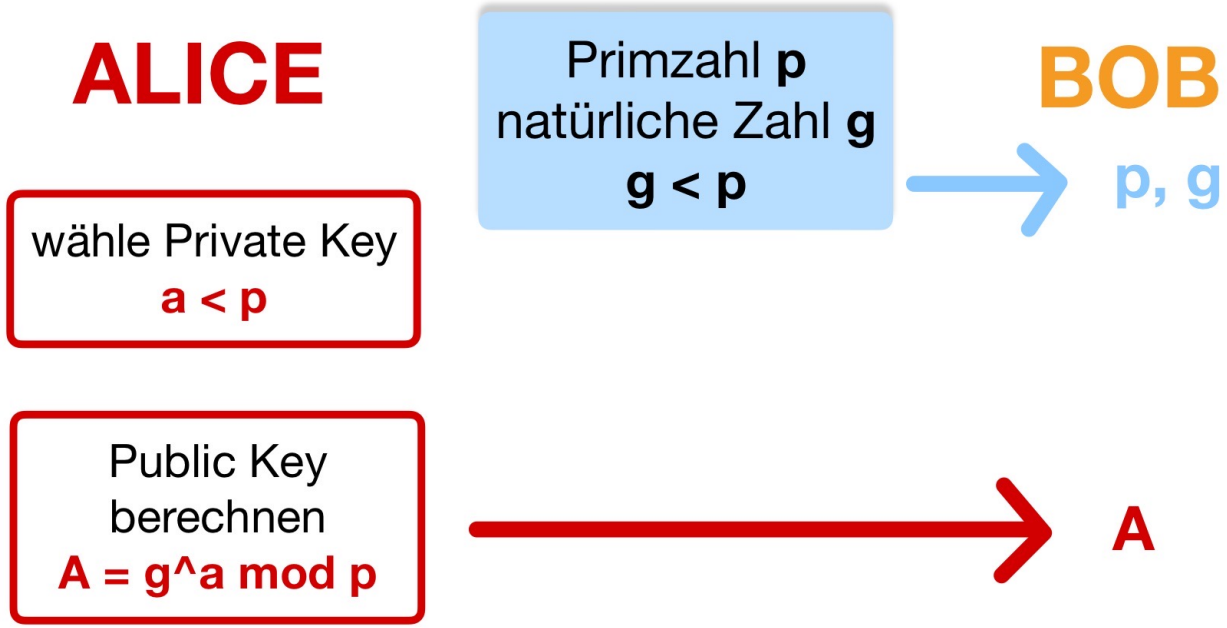
Diffie-Hellman

ALICE **BOB**

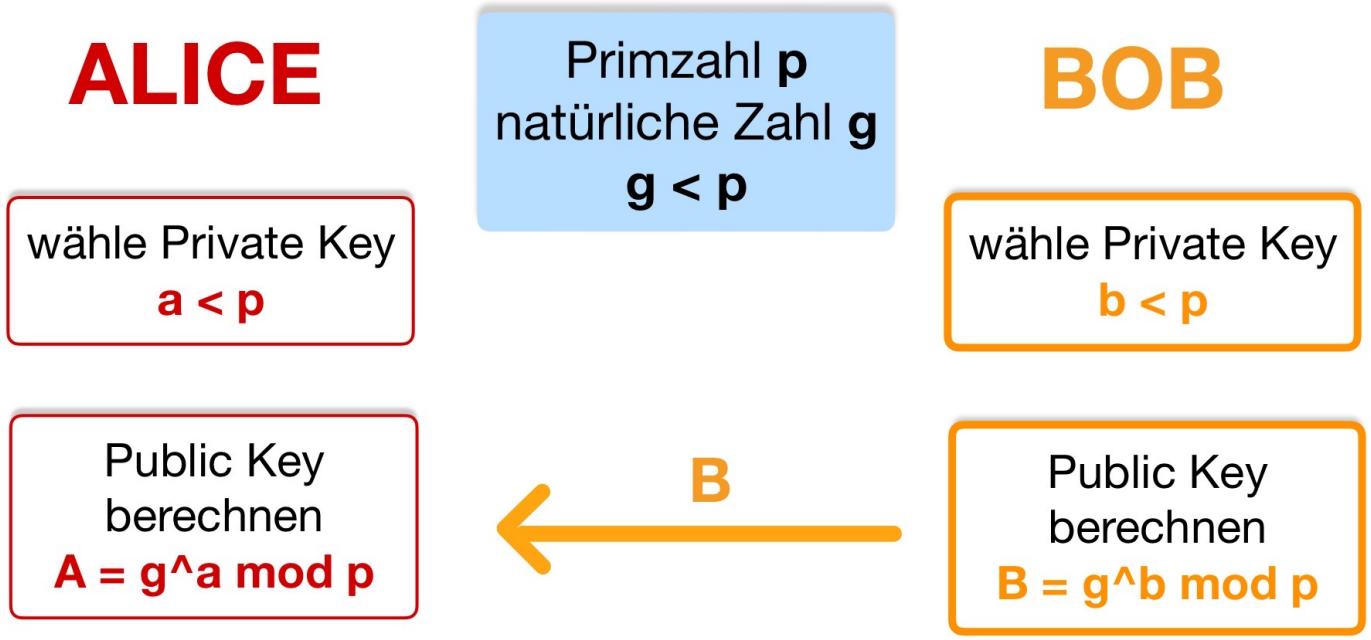


Primzahl **p**
natürliche Zahl **g**
g < p

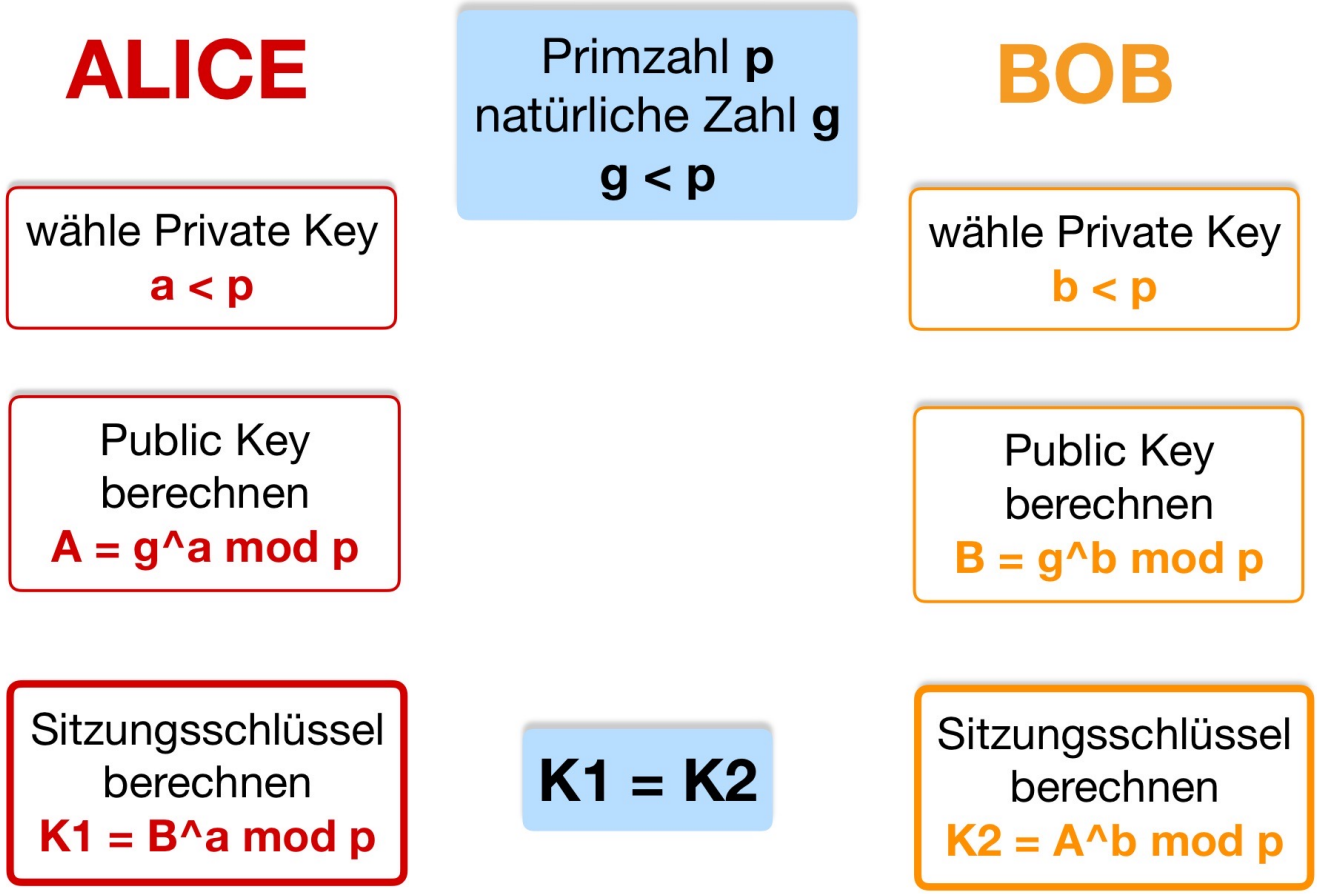
Diffie-Hellman



Diffie-Hellman



Diffie-Hellman



VPN vs. Onion-Routing

- Verschleierung
- Verschlüsselung
- Netzwerk vertrauen
- Man-In-The-Middle
- Tor über VPN

Danke für eure Aufmerksamkeit

Quellen

- Abbildung 1: https://www.pngwing.com/en/free-png-yqhvv
- Abbildung 2: https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet
- Abbildung 3: https://skerritt.blog/how-does-tor-really-work/