# DARKWEB & ONION SERVICES

BOLDEANU MARIUS-PAUL
MASTERAND CSML2

# CUPRINS

# Surface web, Deep web & Dark web

**Surface web** cuprinde navigarea zilnică pe internet și este disponibil pentru publicul larg. Exemple:

- Google
- Yahoo
- Bing
- Firefox
- Wikipedia
- Surse de știri

**Deep web** protejează conturile private și informațiile care nu sunt destinate vizualizării publice. Exemple:

- Informații academice
- Dosare medicale
- Documente legale
- Rapoarte guvernamentale
- Baze de date private
- Platforme pe bază de abonament

**Dark web** este o extensie a internetului ascuns, operând pe conexiuni internet criptate. Exemple:

- Trafic de droguri
- Escrocherii cu criptomonede
- Activități ilegale
- Proteste politice
- Comunicații private

# De unde a inceput?

Rețeaua Tor a fost creată de către David Goldschlag, Mike Reed și Paul Syverson în anul **2002**, sub inițiativa **Laboratorului de Cercetare Navală al Statelor Unite**.

Scopul principal al rețelei Tor (The Onion Router) a fost să ofere utilizatorilor o metodă sigură și anonimă de navigare pe internet.

Inițial, tehnologia Tor a fost dezvoltată pentru a proteja **confidențialitatea** și **anonimitatea** comunicărilor online, permițând utilizatorilor să acceseze informații și servicii **fără teama de a fi urmăriți**, **monitorizați** sau **cenzurați** de către autorități sau alte părți interesate.

# De unde a inceput?

Conceptul de rutare prin straturi de ceapă (onion routing) a fost fundamental în implementarea Tor. Acest concept implică criptarea și redirecționarea traficului prin mai multe noduri (releuri) într-un mod care ascunde **originea și destinația reală** a datelor. Astfel, într-o rețea Tor, traficul utilizatorilor este transmis printr-o serie de relee alese aleatoriu, iar fiecare releu cunoaște doar releul de la care **a primit datele și către care le transmite**, menținând astfel **anonimitatea** utilizatorului.

De-a lungul anilor, rețeaua Tor a evoluat și a devenit cunoscută nu doar pentru **navigarea anonimă**, ci și pentru facilitarea accesului la **servicii ascunse** (Hidden Services) și pentru rezistența sa la **cenzură**. Utilizarea Tor a devenit populară în rândul celor preocupați de **confidențialitatea online, jurnaliștilor, activiștilor** și oricui dorește să-și protejeze identitatea în mediul digital.

# Ce este DarkWeb?

Dark Web se referă la o parte a internetului care nu este **indexată** de motoarele de căutare tradiționale și este adesea **asociată** cu activități **ilegale**. Funcționează pe rețele criptate și necesită instrumente speciale, cum ar fi Tor, pentru a accesa.

Exista **mituri** comune legate de Dark Web, cum ar fi faptul că este doar un **refugiu** pentru **activități criminale**, recunoscând totodată utilizările legitime, cum ar fi **protejarea confidențialității și ocolirea cenzurii**.

# CIA (Confidentialitate Integritate Disponibilitate)

1. Confidențialitate (Confidentiality)
Confidențialitatea se referă la **protejarea informațiilor de accesul neautorizat**. Scopul este de a se asigura că doar persoanele autorizate pot accesa și vizualiza informațiile sensibile.

2. Integritate (Integrity)
Integritatea implică asigurarea faptului că informațiile **sunt corecte** și **nu au fost modificate sau corupte neautorizat**. Aceasta include protecția datelor împotriva modificării de către părți neautorizate și detectarea eventualelor modificări neautorizate.

3. Disponibilitate (Availability)
Disponibilitatea se referă la asigurarea faptului că informațiile și resursele **sunt accesibile atunci când sunt necesare**. Scopul este de a minimiza întreruperile și de a asigura continuitatea operațională.

# Intimitatea si anonimizarea in cadrul Tor

Intimitatea:

- Se cunoaste identitatea persoanei.
- Nu se cunosc activitatile persoanei respective.

Anonimizarea:

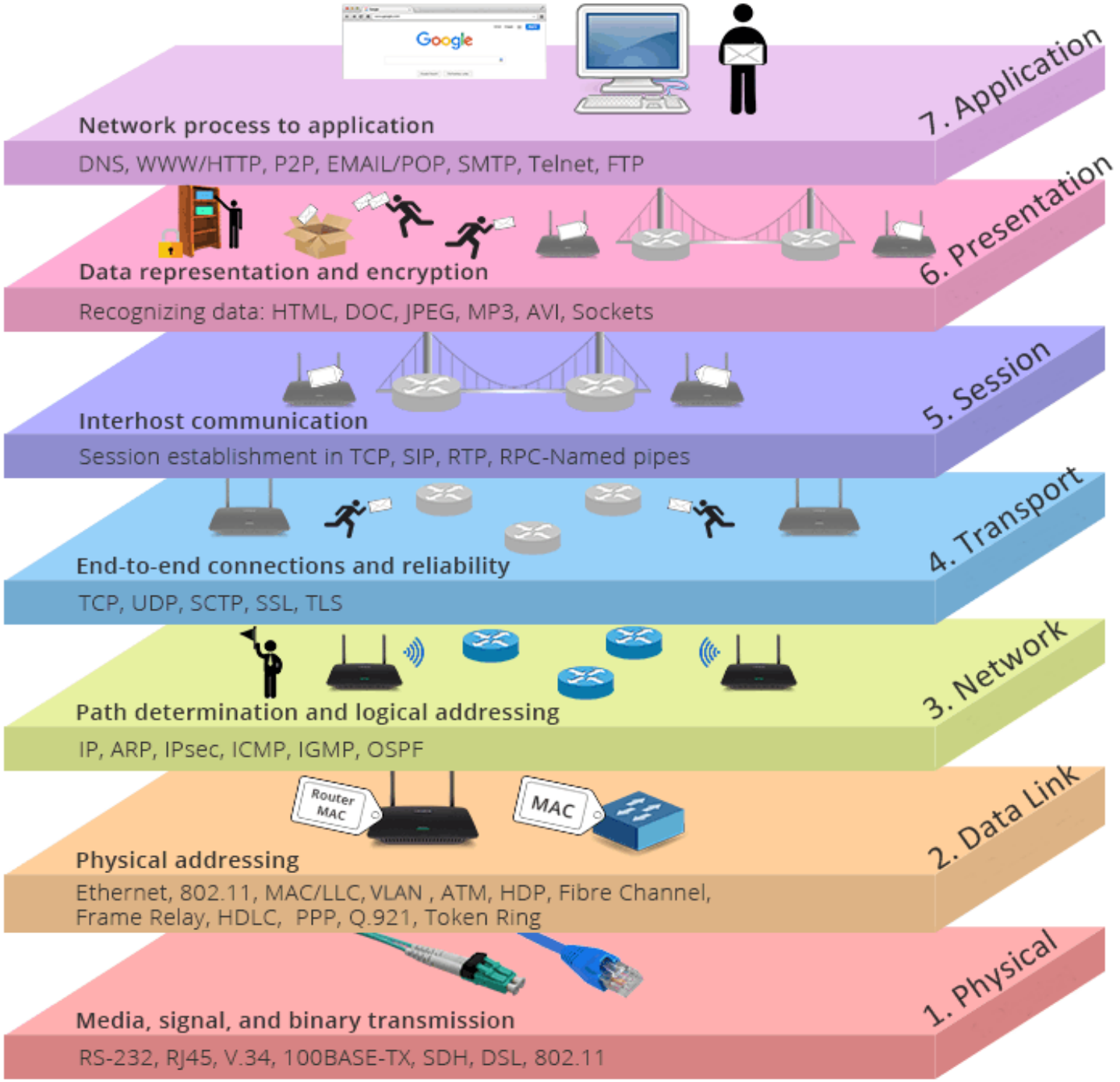
- Nu se cunoaste identitatea persoanei
- Se cunosc activitatile persoanei respective.

# Ce este un router?

Un router este un dispozitiv care conectează două sau mai multe rețele sau subrețele de comutare de pachete. Are două funcții principale: gestionează traficul între aceste rețele prin dirijarea pachetelor de date către adresele IP destinate și permite mai multor dispozitive să folosească aceeași conexiune la internet.

# Ce este OSI? (Open Systems Interconnection)

Modelul OSI (Open Systems Interconnection) este un model conceptual care caracterizează modul în care **componente de software și hardware** implicate în comunicarea în rețea ar trebui să împartă sarcinile și să interacționeze între ele.



**Rolul Tor**

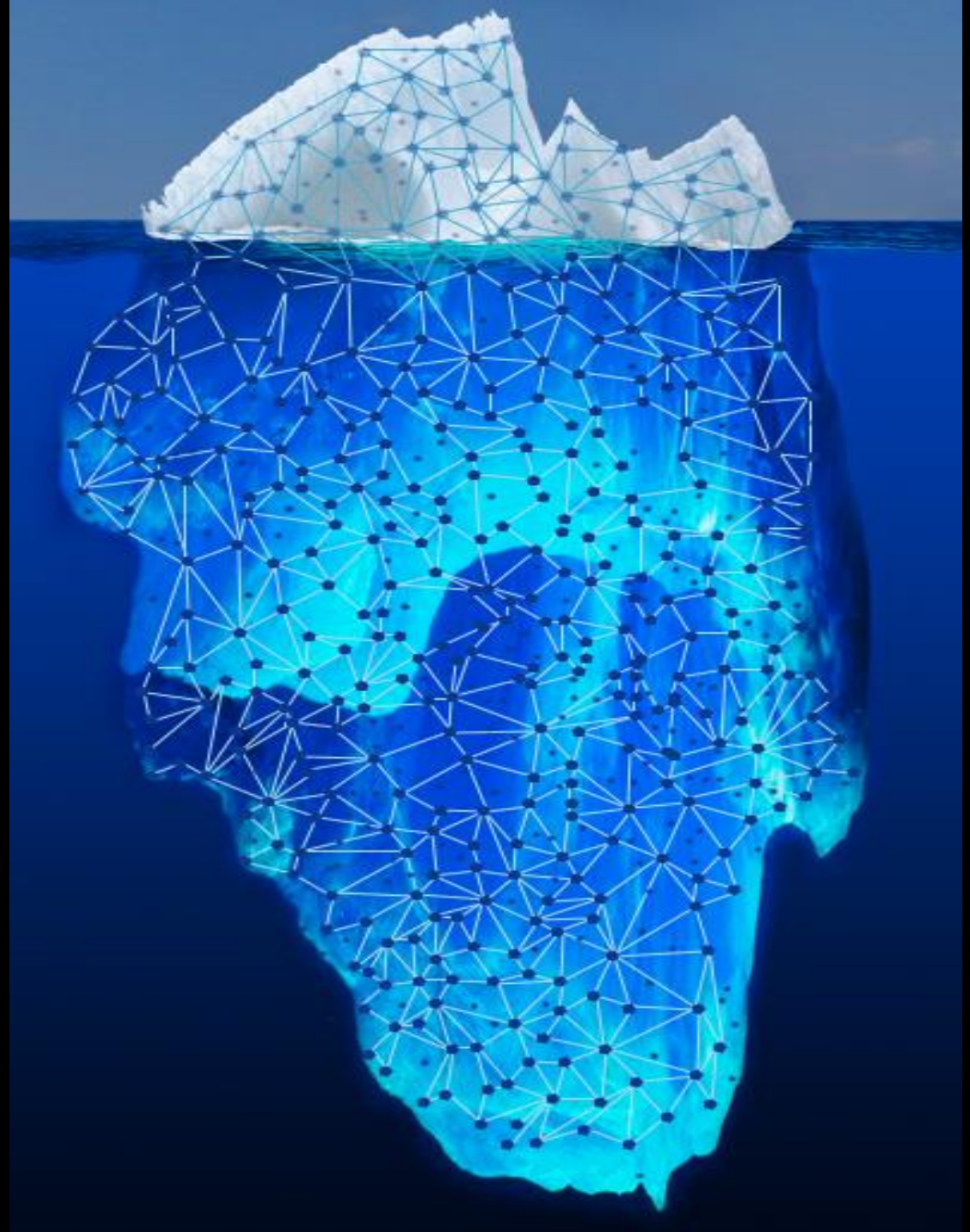
Tor, joacă un rol crucial în facilitarea **comunicării anonime** prin **redirecționarea** traficului de internet printr-o rețea **globală** de **voluntari**.

**E2EE (End to end encryption)**

Datele transmise prin rețeaua Tor sunt supuse unei criptari e2e , protejând confidențialitatea și integritatea informațiilor schimbate între utilizatori.

**Rezistență la cenzură**

Natura **descentralizată** a rețelei Tor **sporește** rezistența la **cenzură**, permițând utilizatorilor să acceseze informații fără **restricții impuse** de autorități sau terțe părți.



**Mecanismul de rutare prin straturi de ceapă**

Tehnica de rutare prin **straturi** de **ceapă** folosită de Tor **criptează** datele în mai multe **straturi**, asemănător cu straturile unei cepe, asigurând o confidențialitate și securitate sporită pentru utilizatori.

**Servicii Ascunse**

Platformele dark web utilizează **servicii ascunse** pentru a menține **anonimatul**, permițând site-urilor să fie găzduite pe servere în timp ce ascund **adresele** IP **reale**.

**Suport comunitar**

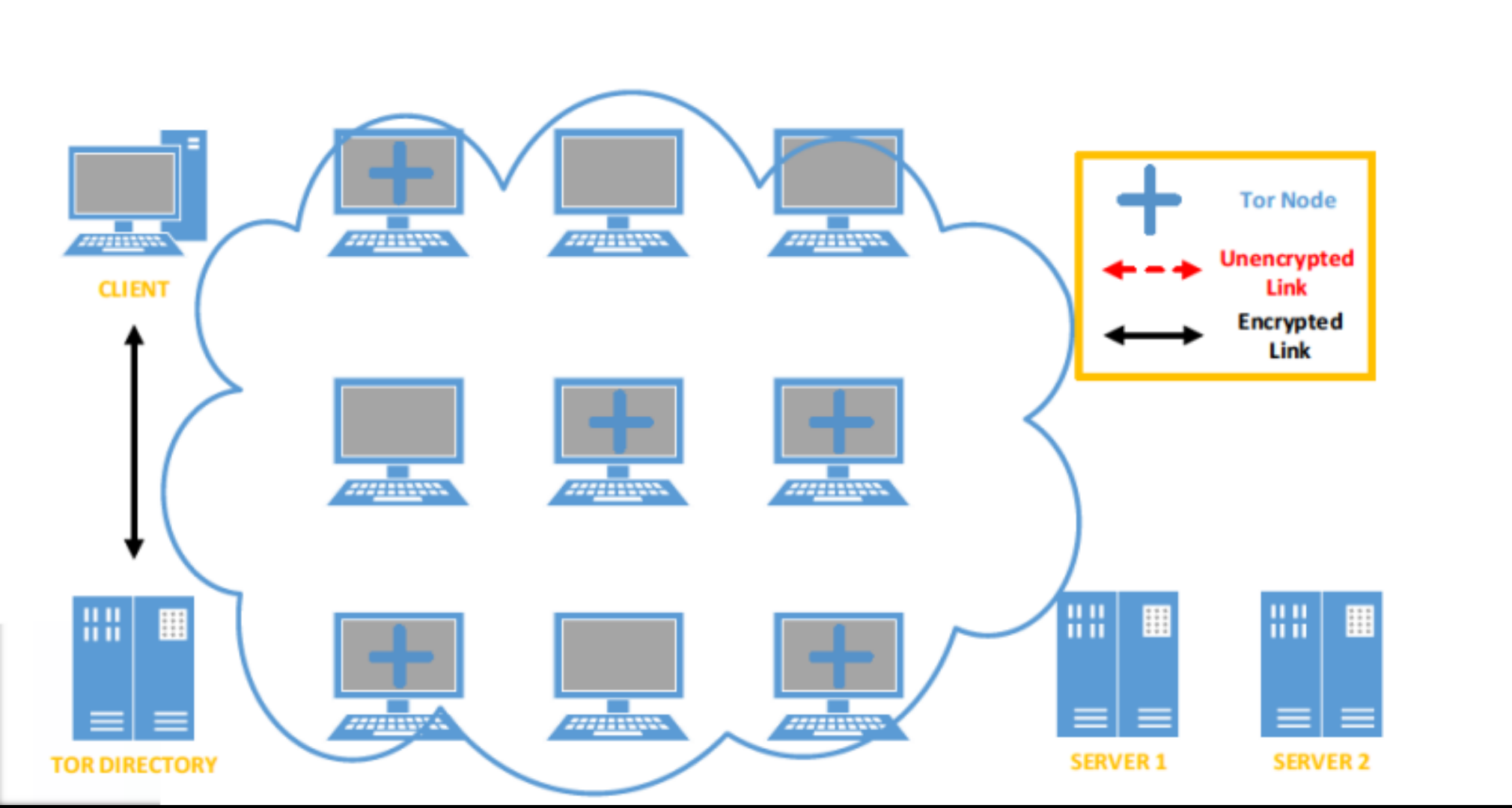
Suportul comunitar solid în spatele Tor și **operațiunilor** dark web creează un mediu sigur pentru persoanele care caută **confidențialitate** și **anonimitate** în activitățile lor online.

# Cum functioneaza?

Conexiunile regulate la internet urmează cea mai **scurtă**, **rapidă** și **eficientă** rută la transferul de pachete de rețea, în funcție de algoritmul folosit. Utilizatorii de internet nu trebuie să își facă griji în legătură cu acest aspect, deoarece furnizorii de servicii de internet (ISP) se ocupă de livrarea pachetelor de internet în cel mai eficient mod posibil.

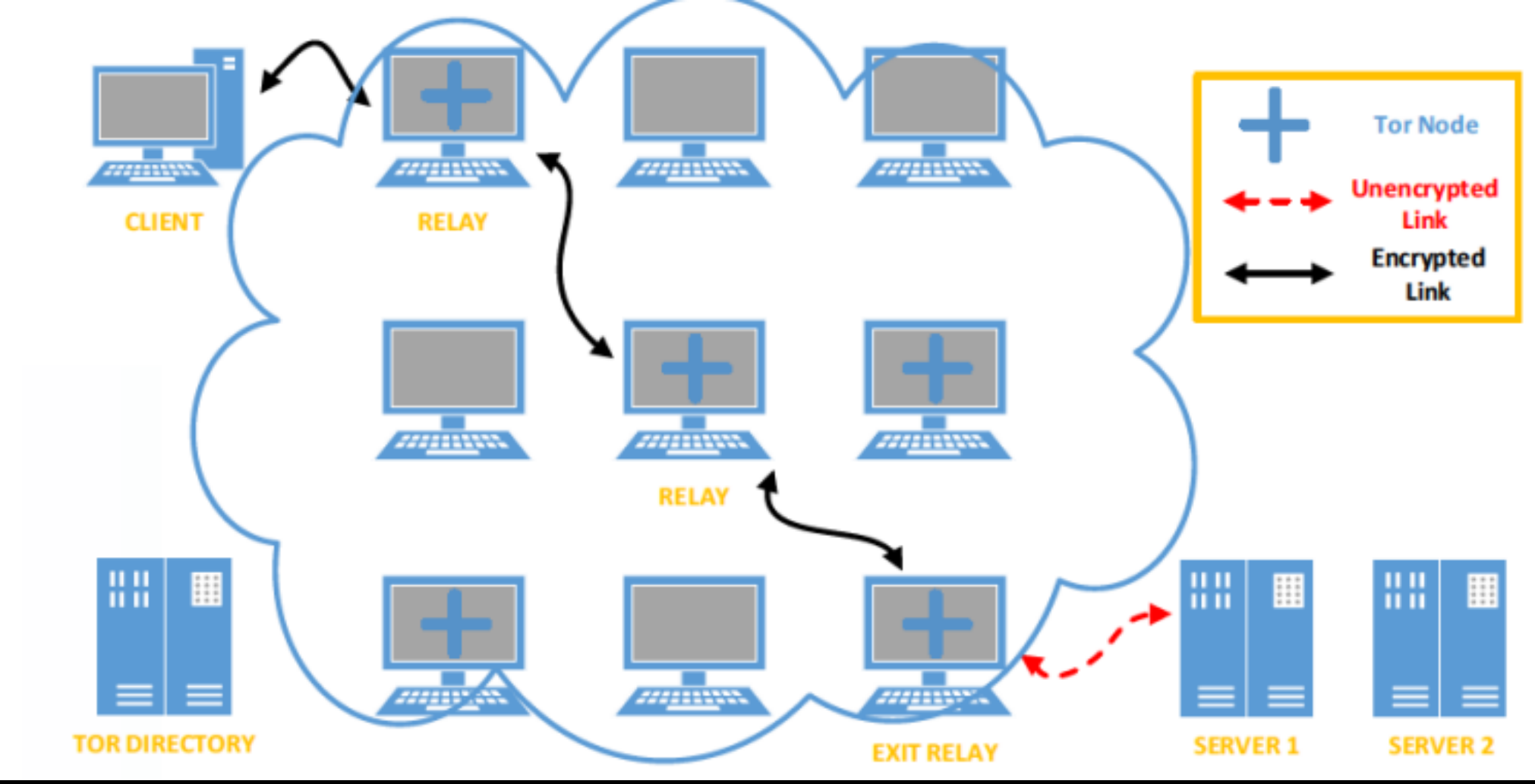
O rețea Tor urmează o abordare diferită. Ea creează o cale **privată** de rețea, numită **circuit**. Pornind de la end user, pachetele de rețea urmează diferite noduri intermediare, numite **relee**, până la ultimul nod al circuitului, releul de ieșire. Noduri de ieșire vor transmite apoi cererea către destinație (de exemplu, site-ul web pe care utilizatorul dorește să-l acceseze).

Toate conexiunile între **primul nod și nodul de ieșire sunt criptate**, iar fiecare nod de-a lungul traseului cunoaște doar **nodul anterior** și **următorul nod**. Nimeni nu cunoaște **întregul traseu în această arhitectură**, cu excepția atacurilor care pot dezvălui unele din aceste noduri.



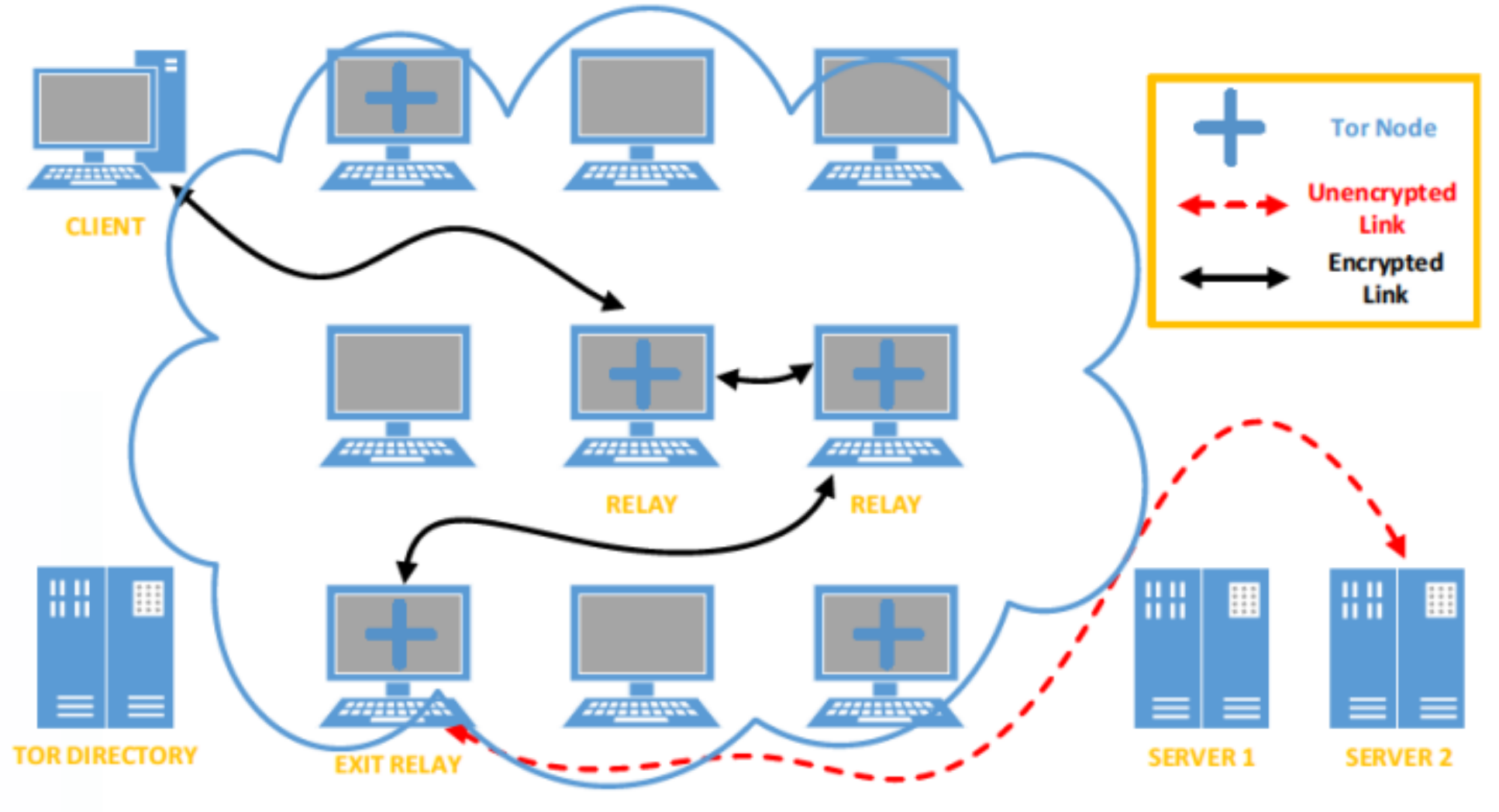

Serverele țintă sunt în partea dreaptă, nodurile Tor (releuri) sunt în mijloc, iar clientul și Directorul Tor sunt în stânga. În primul pas, un client care dorește să se alăture rețelei Tor trimite o cerere criptată către Directorul Tor pentru a obține o listă de noduri Tor disponibile.

Odată ce primește lista, clientul este pregătit să inițieze conexiuni cu acele releuri în norul internetului.




Dacă clientul trimite o cerere către un site HTTPS, cum ar fi "google.com", atunci întregul lanț ar fi criptat. Totuși, conexiunile criptate pot dezvălui și informații sensibile, în funcție de implementarea serviciului web. Această temă va fi detaliată mai târziu.

Clientul alege o rută aleatoare către destinație, Serverul 1 în acest exemplu. Se observă că toate conexiunile de rețea între client și ultimul releu (nod de ieșire) sunt criptate, cu excepția celei dintre Releul de leșire și Serverul 1. Aceasta se întâmplă atunci când clientul dorește să se conecteze la servicii necriptate cum ar fi site-urile web HTTP.

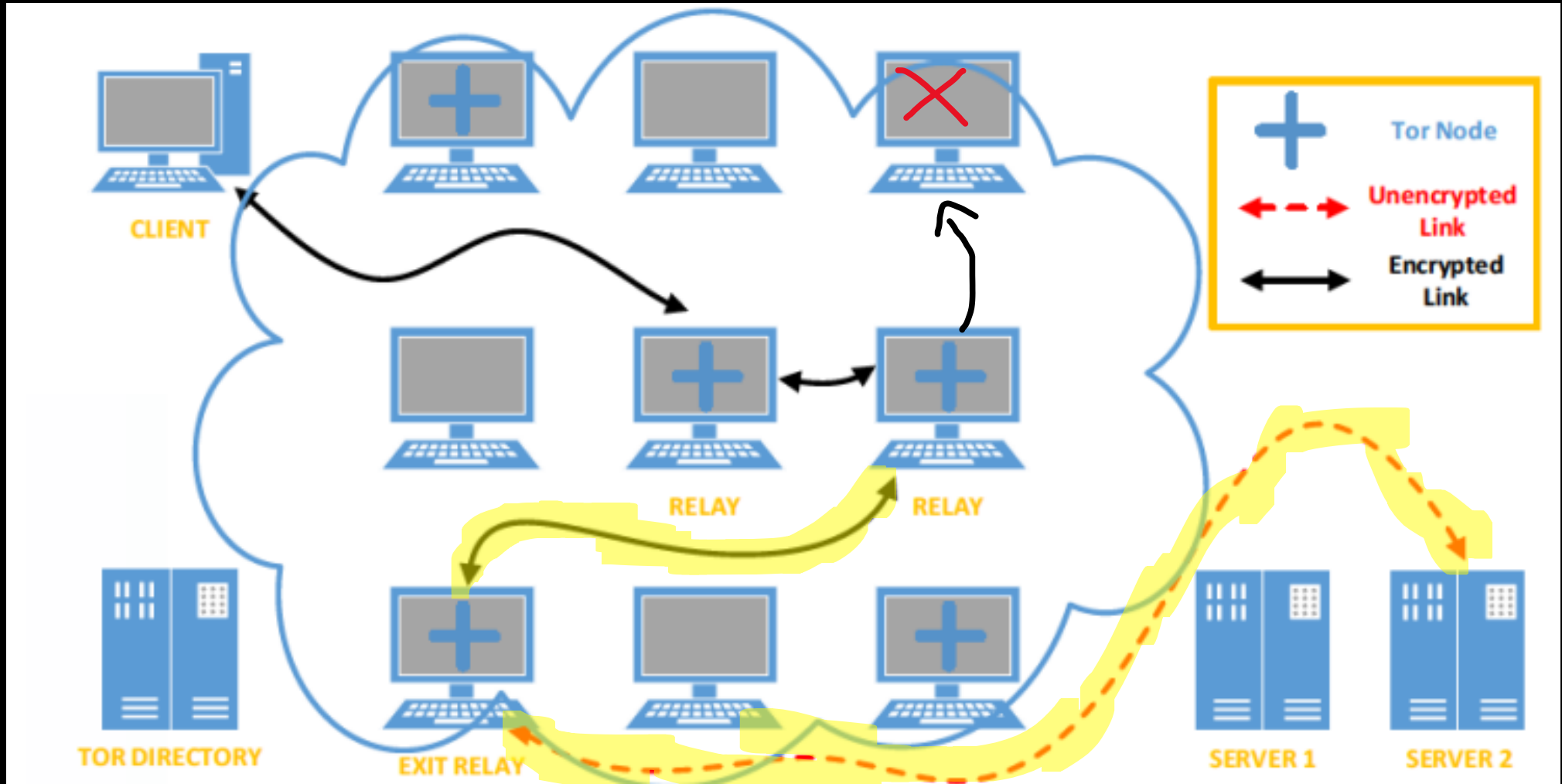



Clientul dorește să stabilească o conexiune nouă către un alt server, Serverul 2. În acest caz, **Tor furnizează o rută diferită către destinație pentru a preveni posibilele atacuri de corelație**. Există și alte modalități de a beneficia de Tor, cum ar fi Serviciile Ascunse. În Serviciile Ascunse, **traficul nu iese din releuri Tor**, ci rămâne în interiorul rețelei.

Tor oferă o funcționalitate numită Servicii Ascunse, care permite protejarea destinațiilor pe internet, cum ar fi serviciile web, utilizând un sistem de puncte de întâlnire distribuite.

În loc să se conecteze direct la serverul destinație, clienții Tor folosesc un identificator (cum ar fi xyz.onion) pentru a găsi și accesa serviciile ascunse. Acest sistem asigură confidențialitatea atât pentru clienți, cât și pentru servere.

Traficul în cadrul serviciilor ascunse rămâne în interiorul rețelei Tor, prevenind astfel problemele de securitate asociate cu monitorizarea traficului la nodurile de ieșire.



# Intrarea in TOR

Există diferite opțiuni de implicare activă în Tor, cum ar fi descărcarea aplicației browserului Tor și utilizarea sa ca client, **administrarea unui releu sau utilizarea unui bridge**. Majoritatea utilizatorilor preferă prima opțiune și se conectează la rețeaua Tor pentru uzul lor personal. Conform statisticilor de astăzi, există în jur de **2 milioane de conexiuni** directe în fiecare zi.

Cele mai frecvente 5 țări de utilizare și procentele sunt: Statele Unite (15,64%), Germania (8,90%), Franța (6,27%), Rusia (6,14%) și Brazilia (4,68%).
A doua opțiune este să administrezi un releu. Tor nu **este doar o rețea tehnică, ci și o rețea socială de voluntar**i care împart lățimea de bandă a rețelei cu alții.

# Intrarea in TOR - Bridge

Clienții Tor trebuie să obțină o listă de releuri active în rețea pentru a începe să creeze circuitul. Odată stabilit, fluxul de rețea va porni de la primul releu. Dar ce se întâmplă dacă acel **releu, sau chiar toate releurile din circuit, sunt inaccesibile utilizatorului**? Acest lucru ar face pur și simplu imposibilă conectarea la rețea. Aceasta este o tehnică comună pentru furnizorii de servicii internet în țările care blochează Tor.

Releurile pod (**Bridge**) sunt releuri **necomunicate**, **ascunse**, pe care utilizatorii le pot folosi ca prim pas pentru accesarea Tor. Chiar dacă un ISP blochează toate releelor, utilizatorii încă se pot conecta la Tor cu ajutorul podurilor. Există diferite **modalități** de a **afla adresa IP** a unui pod, cum ar fi trimiterea unui email la bridges@bridges.torproject.org cu linia „get bridges" în corpul emailului. Un răspuns automat va trimite instantaneu 3 adrese IP expeditorului.

# Nodurile de iesire

Administrarea unui releu de ieșire este un subiect puțin diferit și controversat. Există diverse motive în spatele acestui fapt, dar din punct de vedere tehnic și legal, unul iese în evidență: **releurile de ieșire sunt interfața rețelei Tor cu internetul.**

Orice ar face utilizatorii Tor, **oriunde s-ar conecta**, fie că este legal sau ilegal, **releurile de ieșire transportă acele mesaje către destinația finală**.

Principalele probleme nu apar din aplicația Tor în sine, ci din **mediul înconjurător**. Într-o **configurație adecvată**, ajustarea **setărilor** serverului pentru limitarea ratei și politici reduse de ieșire, **gestionarea relațiilor** cu furnizorii de servicii internet, obținerea unei **adrese IP separate pentru nod.**

# Nodurile de iesire

Deoarece Tor nu este utilizat doar pentru motive **nevinovate**, **activitățile spammerilor, încărcătorilor de fișiere Torrent și abuzatorilor** par a proveni toate de la **releurile de ieșire** Tor.

Comunitatea Tor **oferă o listă de ISP-uri** din **diferite țări** și evaluează răspunsul acestora dacă cineva **administrează un pod, un releu sau un nod de ieșire în infrastructura lor.**

Citirea **experiențelor anterioare colectate pe paginile Wik**i este una dintre **primele** lucruri pentru cei care iau în **considerare** să administreze un nod de ieșire pe cont propriu.

# Anonimizarea in TOR

**Asigurarea anonimatului** cuprinzător și fără erori pentru utilizatorii Tor este în centrul cercetării academice și a discuțiilor tehnice. **Din punct de vedere tehnic, designul arhitecturii To**r pare să poată atinge acest scop, însă există multe probleme care fac **sistemul susceptibil la eșecuri**.

Unele sunt legate de **greșelile utilizatorilor**, altele de problemele de rutare onion, iar altele sunt probleme indirecte care afectează rata de succes a sistemului.

**Nu fiecare utilizator poate fi de-anonimizat de fiecare dată**, dar unii utilizatori ar putea fi de-anonimizați la un moment dat.

# Anonimizarea in TOR

Lăsând la o parte toate problemele nelegate de Tor, subiectul principal al cercetării anonimatului provine din rezultatele monitorizării datelor transmise prin Tor. Apoi, **gradul de anonimat** poate fi măsurat prin diferite modele cum ar fi **probabilitatea, similaritatea, entropia** . Deoarece tot fluxul de rețea este criptat între releurile Tor cu ajutorul acestor modele, **ar putea fi posibil să se coreleze traficul și să se dezvăluie adresele IP** reale ale utilizatorilor.

**Colectarea datelor pentru analiza traficului**, care este în mare parte criptat, reprezintă un **pas crucial** și de cea mai mare importanță. Există studii anterioare care s-au concentrat pe analiza rețelei, colectarea URL-urilor traficului HTTP și altele asemenea. **Un releu de ieșire** Tor creează o altă posibilitate aici, deoarece oricine poate opera un releu de ieșire și releul transmite pachetele de internet într-un **format necriptat către destinație** dacă clientul a folosit **HTTP în loc de HTTPS** .

# Erori umane

Tor oferă o experiență de navigare diferită. Pentru a profita la maximum de aceasta și pentru a face ca sistemul să funcționeze corect, există câteva aspecte care necesită o atenție deosebită. **Primul aspect important este browser-ul Tor, deși există și alte soluții pentru a utiliza Tor cu un sistem de operare complet.**

Este foarte obișnuit să **vizualizăm un document**, să utilizăm un add-on în browser-ele internet obișnuite. În browser-ul Tor, **astfel de încercări** pot **perturba** mecanismul sistemului și ar putea **dezvălui adresa IP reală** a utilizatorului. Motivul este simplu. Tor este **conceput** să comunice doar cu alte **relee** înainte de **nodul de ieșire**. Cu toate acestea, unele **obiecte** sau **executabile** încorporate în **documente** pot forța ruptura acestei lanțuri și pot duce la o **scurgere**. Aceste capcane pot face, de asemenea, parte dintr-o **campanie** de **atac** împotriva unor utilizatori pentru a afla adresele lor IP reale.

# Erori umane

Utilizarea Torrent peste Tor **nu este recomandată**, deoarece logica este similară cu amenințările menționate anterior. Aplicațiile de partajare a fișierelor Torrent pot **ignora setările de proxy** ale browser-ului Tor și pot crea **conexiuni directe** cu alți **utilizatori**.

Un exemplu de atacuri legate de Tor **împotriva anonimatului** este faptul că se pretinde că plăți anonime pot fi făcute cu criptomonede precum Bitcoin. Utilizarea **Bitcoin** peste **Tor** se credea că îmbunătățește și mai mult acest lucru. Cu toate acestea, în octombrie 2014, cercetătorii de la Universitatea Luxemburg au demonstrat că **combinarea** lor permite atacuri de tip om în mijloc (**MitM**) pentru a obține **control** total asupra fluxurilor de informații între utilizatorii care folosesc **Bitcoin** peste **Tor**.

# Erori umane

Un ultim exemplu este utilizarea site-urilor web **HTTP** în loc de **HTTPS**. Nodurile de ieșire Tor pot **vizualiza pachetele** de internet care trec prin ele. Dacă clienții Tor folosesc **HTTP**, acest lucru ar face pur și simplu sistemul **vulnerabil** la supraveghere.

**Natura umană** este întotdeauna susceptibilă la **erori** în lumea **cibernetică**. Dacă un utilizator poate fi înșelat să **întreprindă** o acțiune **extraordinară** în timp ce folosește Tor, **identitatea** sa **reală** poate fi **dezvăluită**.

# Deep Packet Inspection

Inspecția profundă a pachetelor (Deep Packet Inspection - DPI) este o metodă de filtrare a pachetelor de rețea care analizează atât **antetul**, cât și **partea de date a unui pachet**. În cazul unui furnizor de servicii de internet (ISP), DPI implică **analizarea** întregii **conexiuni** și a **traficului** online al unui **utilizator**, nu doar a unor informații despre **conexiune**, cum ar fi numerele de **port**, adresele **IP** accesate și protocoalele.

ISP-urile folosesc în general DPI pentru a **aloca resursele disponibile** în scopul **fluidizării traficului**, pentru a-și optimiza serverele în vederea **detectării hackerilor**, **combaterii malware-ului** și **colectării datelor** comportamentale despre utilizatorii lor.

Deși DPI poate părea **inofensiv**, în realitate poate avea un **impact** foarte negativ asupra intimității tale online.

# Cum functioneaza DPI?

DPI este realizată în mod normal la nivel de **firewall**, în special la cel de-al **șaptelea strat** al (OSI) – Stratului de Aplicație. Metoda **evaluează** conținutul oricărui **pachet** de date care trece printr-un punct de control.

Modul în care DPI **evaluează** conținutul **pachetelor** de date se bazează pe **reguli stabilite** de **administratorul** rețelei. DPI efectuează evaluarea în timp **real** și poate **determina** de unde **provin pachetele** de **date** (de la ce aplicație sau serviciu, mai exact).

De asemenea, pot fi **stabilite filtre** pentru ca DPI să **redirecționeze** traficul de la **servicii online** (cum ar fi Facebook, de exemplu).

# DPI in diferite tari

Furnizorii de servicii de internet (ISP) au putut de mult timp să urmărească și să înregistreze fiecare mișcare a ta online. De asemenea, pot și vor **bloca** utilizatorii de la **accesarea anumitor** site-uri. Această practică este frecvent utilizată de anumite țări care au **impus interdicții** asupra **conținutului** de pe **internet**. SUA, Rusia, Coreea de Nord, China, Iran și alte țări folosesc DPI pentru a bloca accesul la site-uri în scopuri de **cenzură** și pentru a-și **monitoriza** cetățenii.

De exemplu, guvernul chinez folosește DPI pentru a **cenzura** conținutul considerat „**dăunător**" pentru cetățenii chinezi și interesele statului. În acest scop, ISP-urile chineze folosesc DPI pentru a urmări anumite **cuvinte cheie** care trec prin rețelele lor, **restricționând conexiunile** dacă se găsesc astfel de informații.

Un alt exemplu este Agenția Națională de Securitate a SUA, care folosește DPI pentru **supravegherea traficului** pe internet. De asemenea, se presupune că guvernul iranian folosește DPI pentru a colecta **informații** despre **indivizi** și a **bloca** comunicațiile.

# Cum Folosesc ISP-urile DPI?

Unul dintre principalele moduri în care ISP-urile folosesc DPI este pentru a căuta **conținut P2P** - în special în țările unde **torrenting**-ul nu este tocmai **legal**. Când găsesc conținut P2P, fie vor **încetini viteza** de **descărcare** a utilizatorului (în cel mai bun caz), fie vor **preda datele utilizatorului** autorităților și agențiilor de **copyright**.

În afară de aceasta, ISP-urile pot recurge la DPI dacă trebuie să **blocheze accesul** la anumite site-uri web. De obicei, fac acest lucru pentru a se conforma reglementărilor guvernamentale și, potențial, celor legate de copyright.

ISP-urile pot folosi DPI și pentru a **spiona conexiunile utilizatorilor** și pentru a compila **profiluri detaliate** bazate pe activitățile și preferințele lor online, pe care le-ar putea **vinde** apoi **agențiilor** de **publicitate terțe**. Este genul de lucru care poate avea loc legal în SUA și pe ascuns în alte țări. Deoarece **DPI** le oferă atât de multe informații despre ceea ce faci online și ce descarci, pot **potențial** să îți **încetinească viteza** dacă consideră că folosești „**prea multe date**" pentru o anumită activitate - cum ar fi **jocurile online**, **streaming**-ul online sau **descărcarea** de **fișiere**

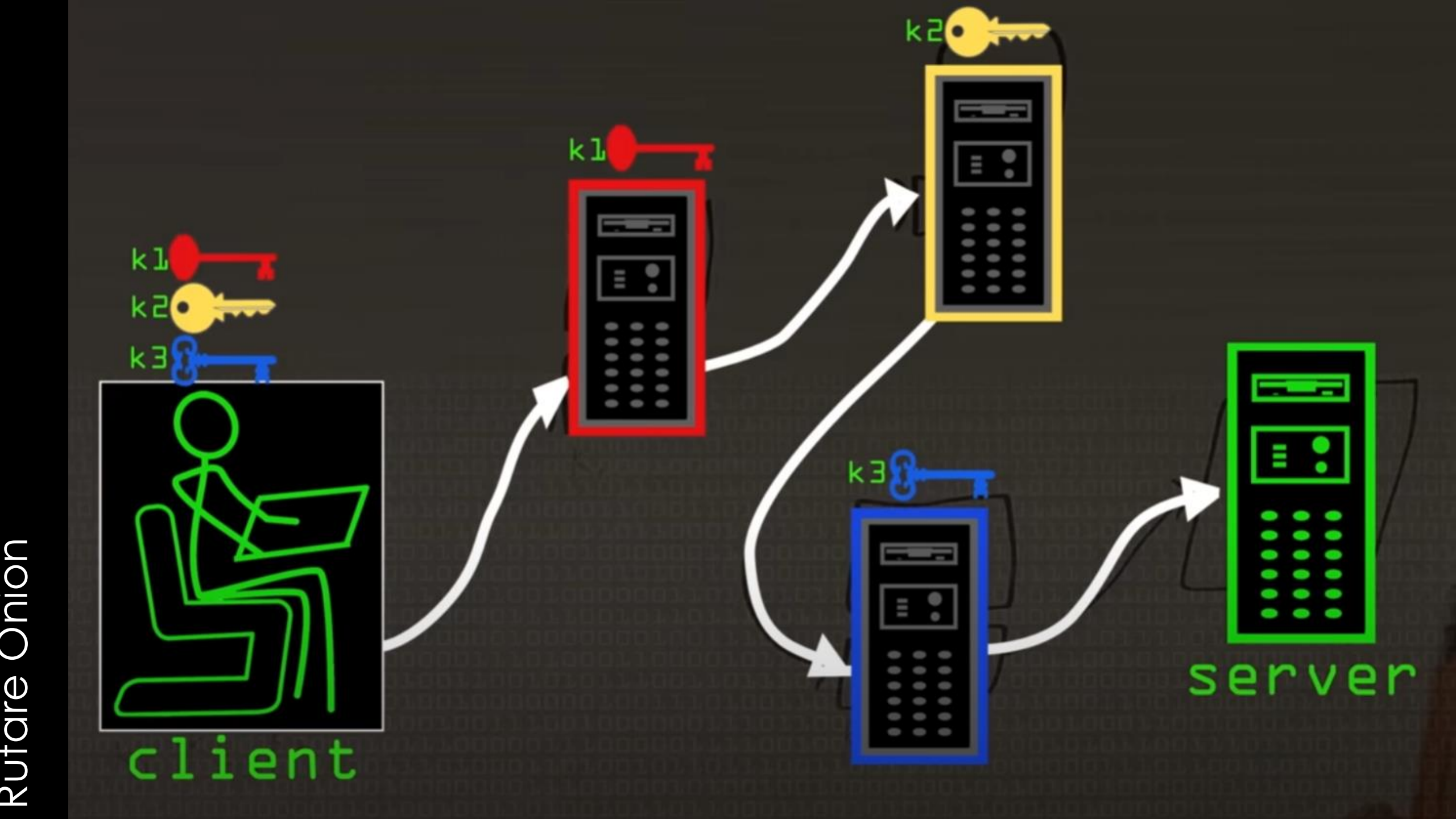
# Cum te Afectează DPI?

Deoarece toate informațiile pe care le trimiți și le primești online sunt compilate în mici pachete de date care sunt apoi scanate și analizate de ISP-ul tău, este destul de clar că DPI reprezintă o încălcare majoră a intimității tale.
Practic, dacă DPI nu este controlat și alegi să-l ignori, iată ce s-ar putea întâmpla:

- **Reclame Intruzive și Personalizate:** Este posibil să începi să primești o mulțime de reclame personalizate și intruzive dacă ISP-ul tău a împărtășit datele DPI cu agenții de publicitate.
- **Probleme Legale:** Ai putea avea probleme legale pentru descărcarea de torrente dacă trăiești într-o țară unde acest lucru este o problemă legală.
- **Încetinirea Vitezei Conexiunii:** Vitezele conexiunii tale ar putea fi intenționat încetinite ca o modalitate de a te „convinge" să plătești pentru un abonament mai scump sau un plan de date mai costisitor.
- **Lipsa Intimității:** Va trebui să trăiești cu gândul că tot ceea ce faci online nu este niciodată privat – va exista întotdeauna cineva care îți urmărește obiceiurile de navigare și conversațiile.
- **Acces Restricționat:** S-ar putea să nu poți accesa anumite site-uri web dacă ISP-ul tău este forțat să folosească DPI pentru a le bloca.

# Cum putem prevenii DPI?

- **Utilizează un VPN (Virtual Private Network)**
- **Folosește Tor**
- **Activează HTTPS Everywhere**
- **Utilizează un Proxy**




Rutare Onion

# Symmetric encryption

Bob

Alice

$(a, g, p)$

$(A, g, p)$

$(b)$

$A = g^a \bmod P$

$B = g^b \bmod P$

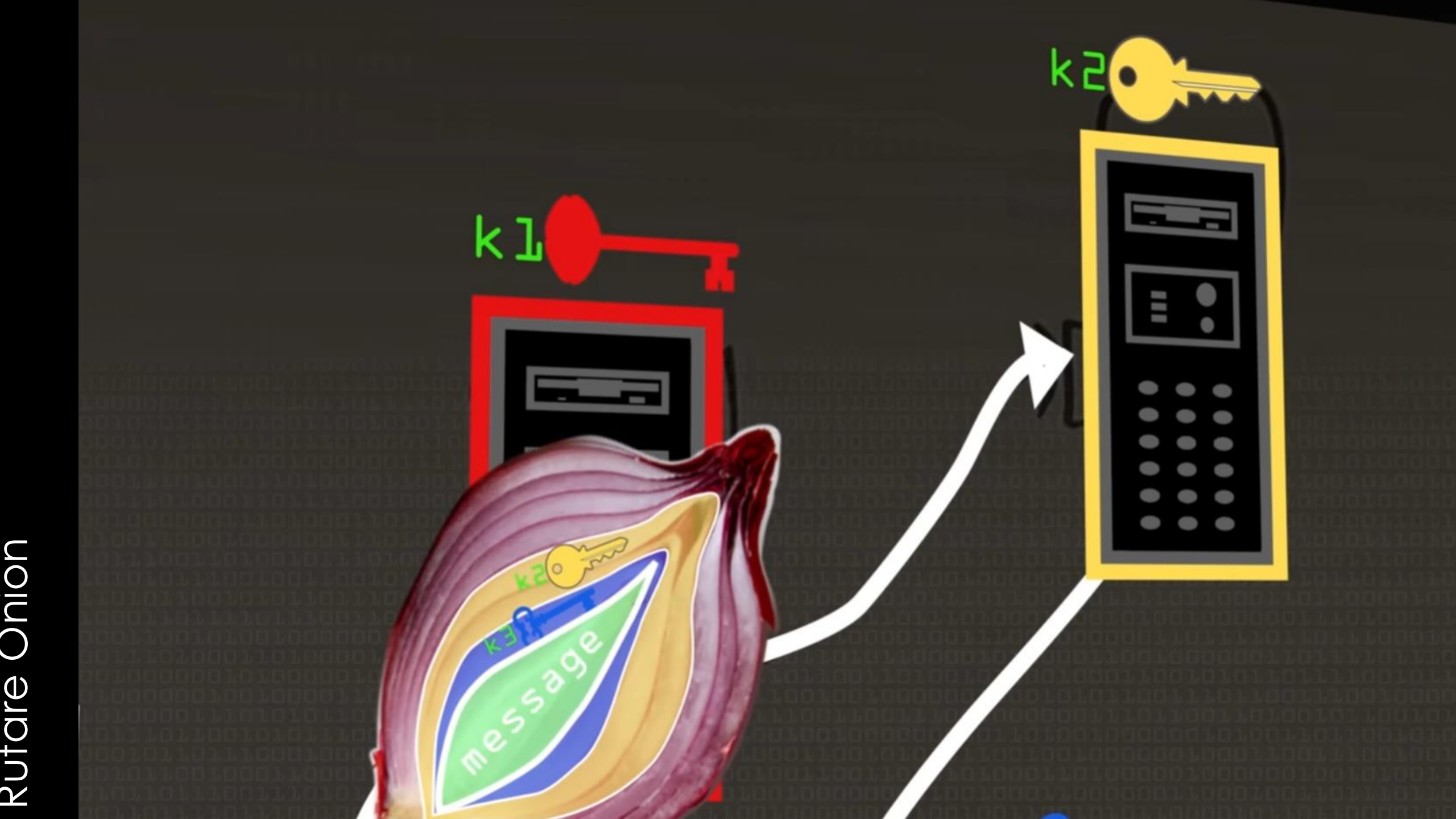
$(B)$

$K = B^a \bmod P$

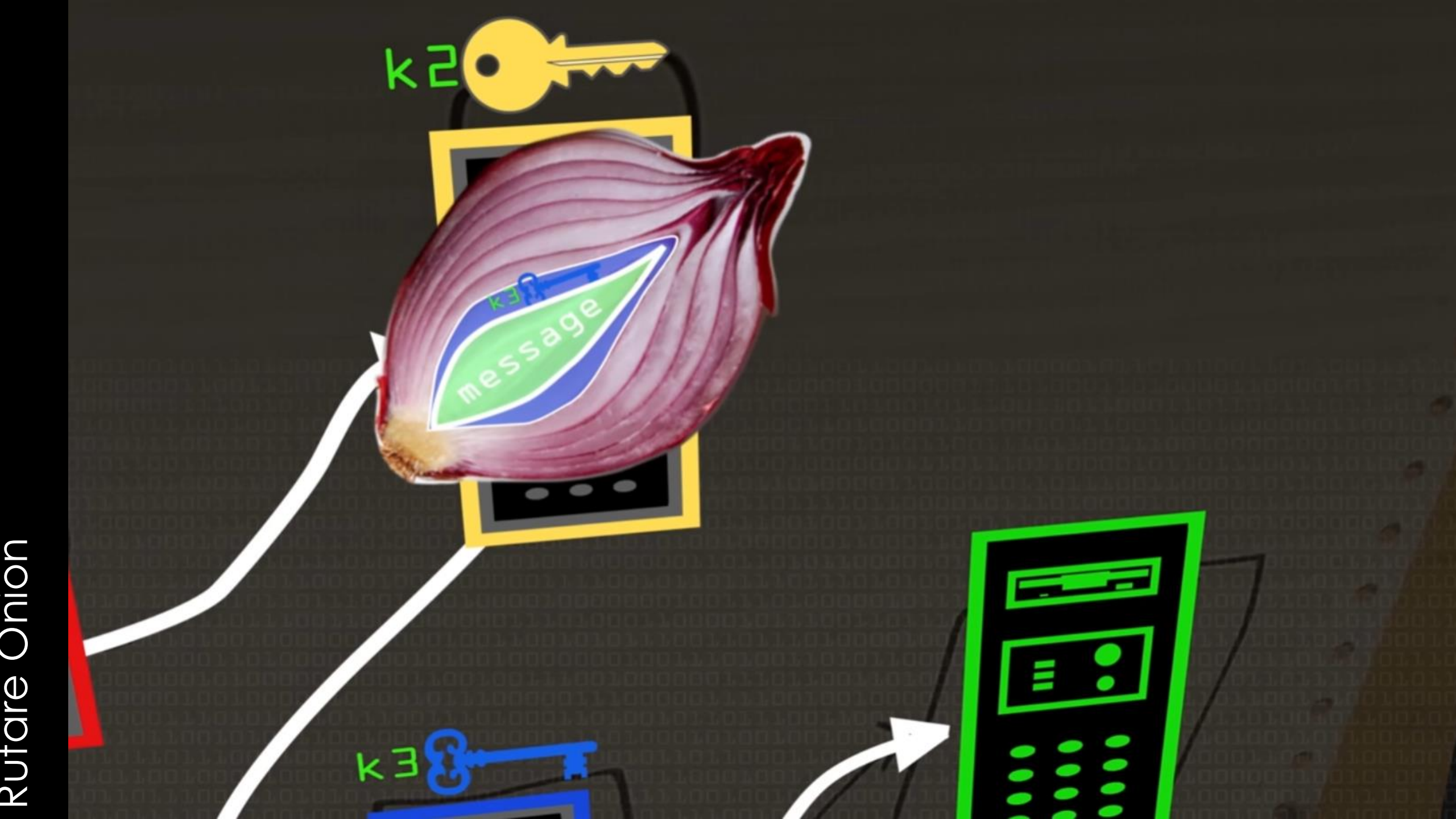
$K = A^b \bmod P$

Rutare Onion

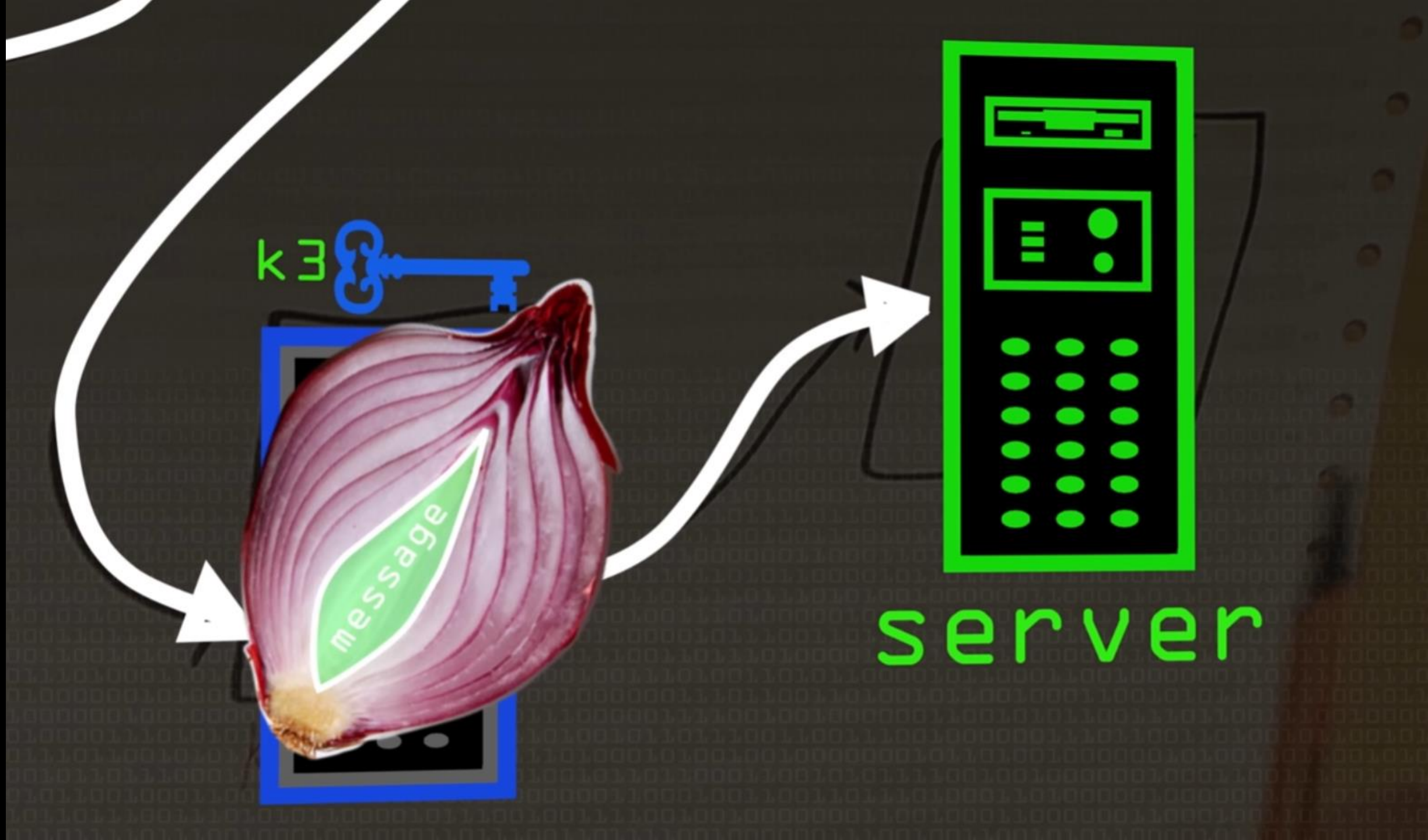

Rutare Onion



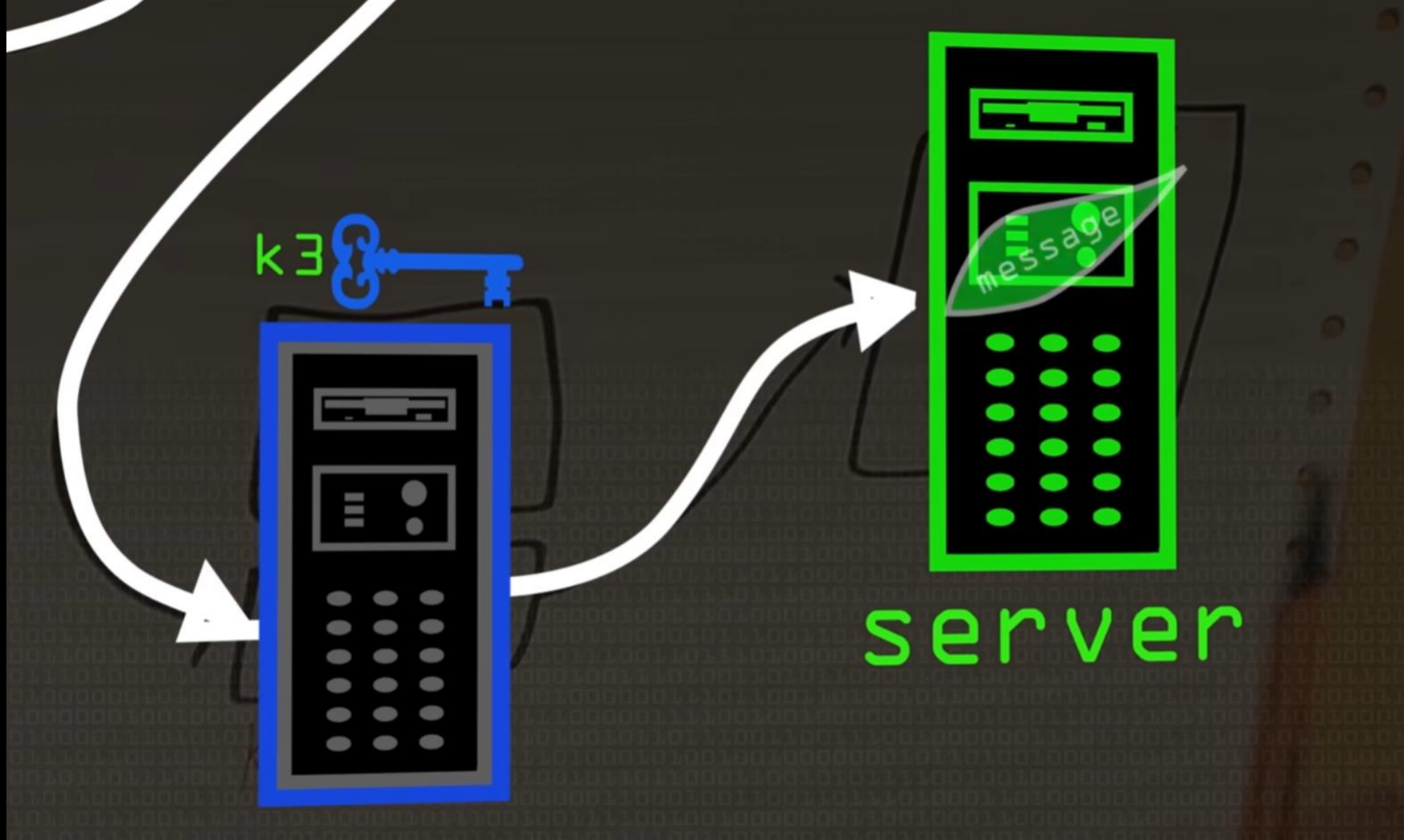

Rutare Onion




Rutare Onion



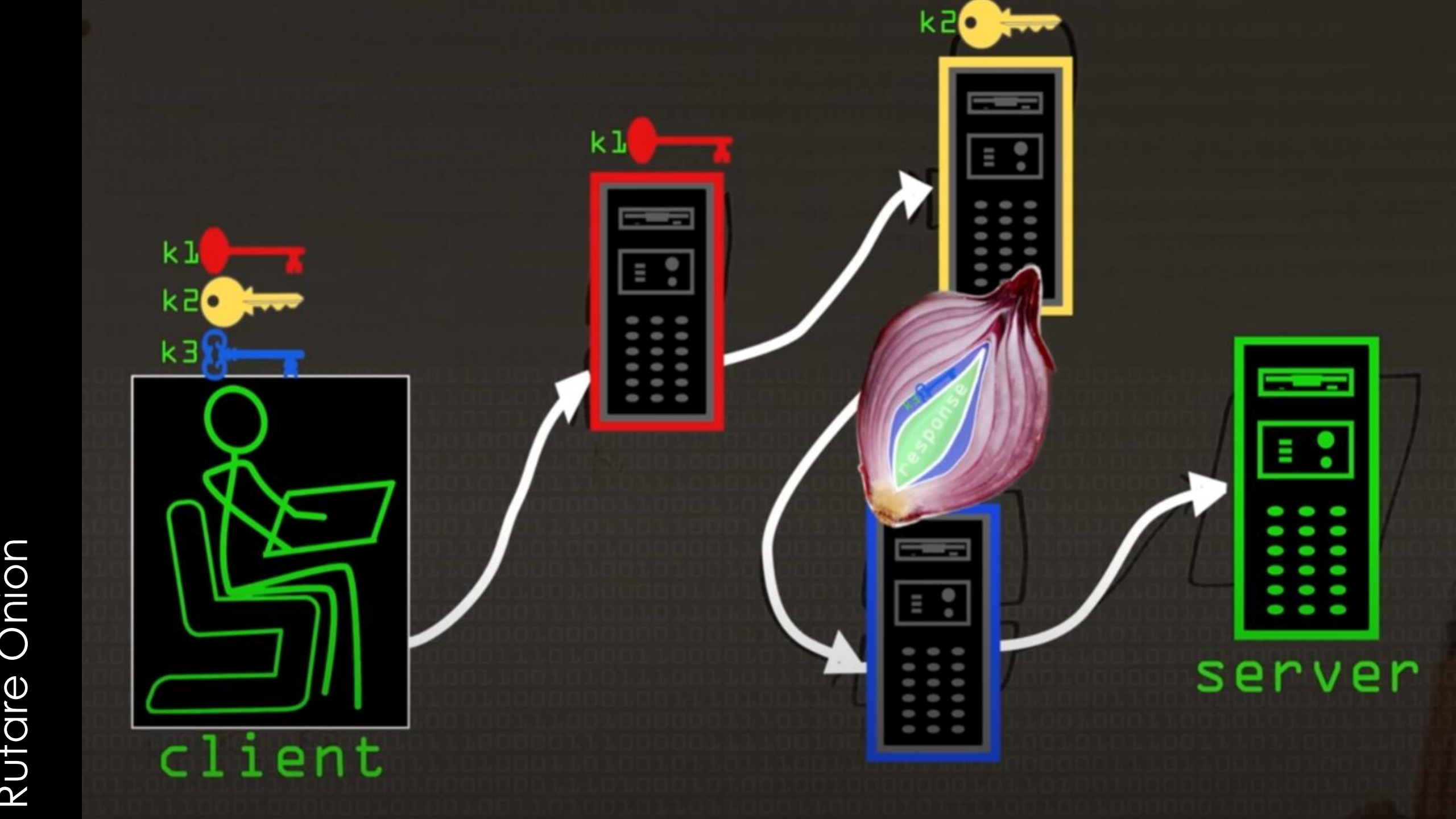

Rutare Onion



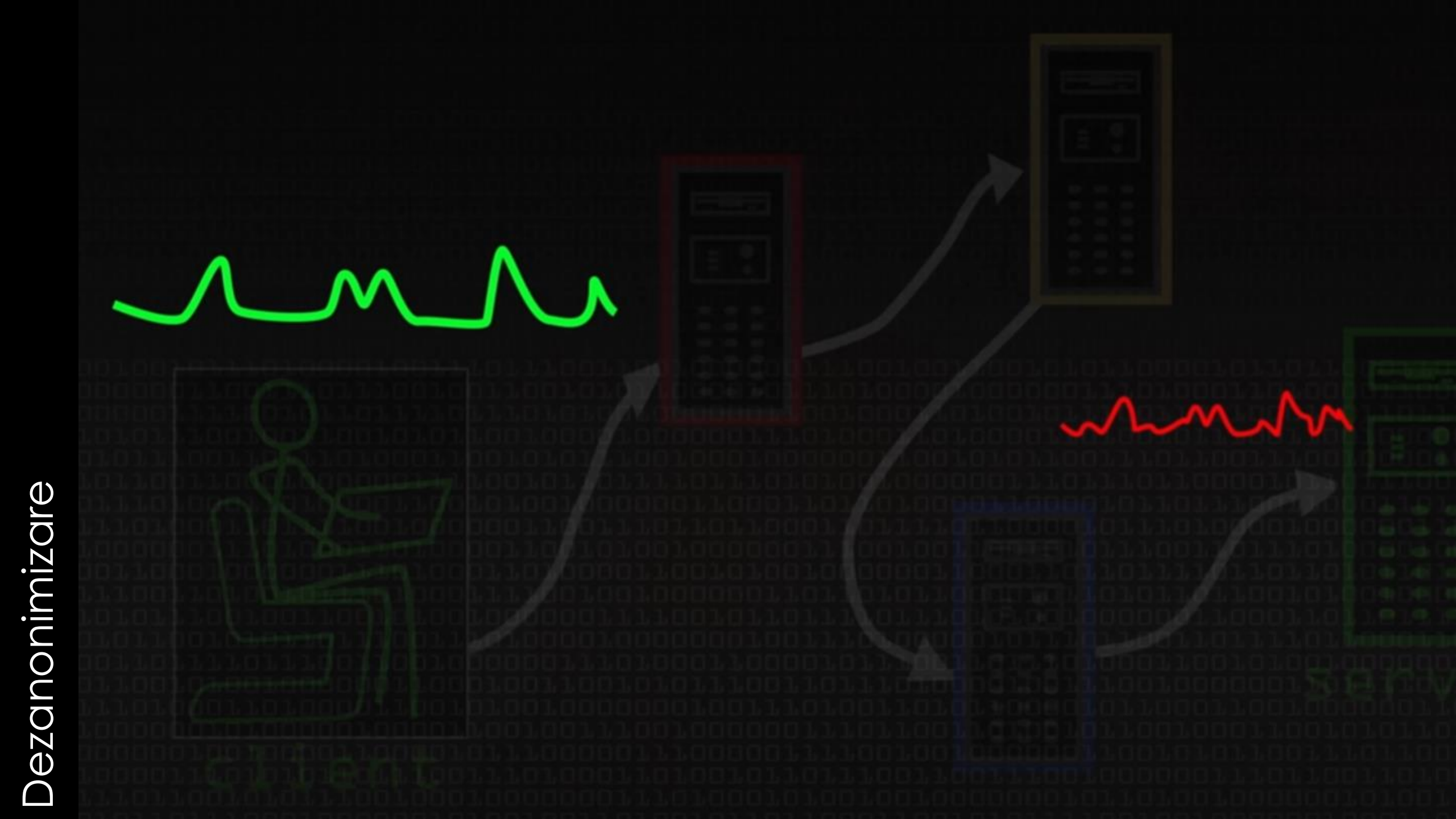

Rutare Onion


Rutare Onion

Rutare Onion




Rutare Onion


Dezanonimizare

# Guvernul in Tor

Deși nu confirmat oficial, se raportează că **NSA** a făcut încercări repetate de a dezvolta **atacuri împotriva persoanelor care utilizează Tor**. În 2013, s-a sugerat că documentele scurse confirmă faptul că NSA **operează** și **colectează** trafic de la unele noduri din rețeaua Tor, fără a exista informații suplimentare cu privire la câte noduri sunt controlate și dacă tehnica propusă de de-anonimizare a fost vreodată implementată.

Unele surse susțin că „NSA **urmărește** utilizatorii care se presupune că locuiesc în afara SUA și care **solicită informații despre punțile** Tor prin e-mail sau care caută sau descarcă **Tor** sau sistemul de operare **TAILS** live".

# Guvernul in Tor

Alte țări au propus, de asemenea, **măsuri** pentru a contesta **anonimitatea** oferită de Tor. Un exemplu este **Rusia**, care, cu scopul „de a asigura **apărarea** și **securitatea** țării”, a oferit deschis o recompensă de **110.000** de **dolari** oricui poate **sparge identitățile** utilizatorilor rețelei Tor.

Într-o dezvoltare recentă, **EUROPOL** a anunțat în 2014 închiderea „a peste **410** servicii ascunse”, numărul fiind ulterior corectat la **27** de site-uri web.

# Fortele de ordine in investigatiile criminale

Astăzi, Tor este o unealtă comună pentru autoritățile de aplicare a legii naționale. Proiectul Tor rezumă trei activități principale pentru utilizarea de către forțele de ordine:

- **Supravegherea online**: Tor permite oficialilor să navigheze pe site-uri web suspecte și servicii fără a lăsa urme evidente. Dacă administratorul unui site **ilegal** de **jocuri** de **noroc**, de exemplu, ar observa mai multe conexiuni de la **adrese IP** ale **guvernului** sau ale forțelor de ordine în jurnalele de utilizare, **investigațiile** ar putea fi **împiedicate**.
- **Sting Operations**: Similar, **anonimatul** permite **ofițerilor** de **poliție** să participe la operațiuni „**sub acoperire**" online. Indiferent cât de credibile pot fi acoperirile ofițerilor sub acoperire, dacă **comunicările** includ IP-uri de la adrese de poliție, acoperirea poate fi **compromisă**.
- **Anonymous tip lines**: În timp ce **liniile de informații anonime** online sunt populare, fără software de anonimat sunt mult mai puțin utile. Sursele sofisticate înțeleg că, deși un **nume** sau o **adresă** de email **nu** este atașată **informațiilor**, **jurnalele serverului** pot să le **identifice** foarte repede.

# Folosirea nodurilor de iesire pentru colectarea de dovezi

Au existat rapoarte care pretind că unele guverne au control și rulează anumite de ieșire .

În ciuda diferențelor dintre sistemele legale din diferite țări, supravegherea poate fi în mod general împărțită în două categorii:

-**supravegherea țintită** (de obicei 'interceptarea')

-**supravegherea non-țintită** ('monitorizarea' sau 'filtrarea') nu vizează persoane sau date specifice, ci mai degrabă tipuri generale de conținut nedorit în scopuri generale de **'securitate'**

Din perspectiva autorităților de aplicare a legii, ar fi dificil, dacă nu imposibil, să se determine că datele care trebuie interceptate ar trece printr-un anumit nod de ieșire, deoarece Tor **își schimbă ruta în medie** la **fiecare 10 minute**, ceea ce ar face **dificilă** determinarea **scopului** și detaliilor **mandatului necesar** pentru accesarea acestor date.

# Cine foloseste TOR si in ce scopuri?

- **Jurnaliști și activiști**:
- **Scopuri**: Protejarea surselor, comunicarea sigură, și accesarea de informații cenzurate în anumite țări. Jurnaliștii și activiștii folosesc TOR pentru a evita supravegherea guvernamentală și pentru a comunica în siguranță în regimuri opresive.

- **Informatori (whistleblowers)**:
- **Scopuri**: Dezvăluirea de informații sensibile și protejarea identității lor. Informatorii folosesc TOR pentru a trimite informații mass-mediei sau organizațiilor fără a-și compromite siguranța personală.

- **Utilizatori obișnuiți preocupați de confidențialitate**:
- **Scopuri**: Protejarea datelor personale și navigarea anonimă. Mulți utilizatori obișnuiți aleg să folosească TOR pentru a-și proteja intimitatea online și pentru a evita urmărirea și colectarea de date de către terți.

# Cine foloseste TOR si in ce scopuri?

- **Cercetători și academicieni**:
- **Scopuri**: Accesarea de materiale și baze de date restricționate sau cenzurate. Cercetătorii pot folosi TOR pentru a accesa informații necesare studiilor lor, care ar putea fi blocate sau filtrate în anumite regiuni.

- **Utilizatori din țări cu cenzură strictă**:
- **Scopuri**: Ocolirea cenzurii și accesarea liberă a internetului. În țările unde guvernul cenzurează internetul, cetățenii folosesc TOR pentru a accesa site-uri și servicii care sunt blocate.

# Cine foloseste TOR si in ce scopuri?

- **Infractori cibernetici**:
- **Scopuri**: Activități ilegale, cum ar fi vânzarea de droguri, arme, informații furate, și alte activități ilicite. Din păcate, TOR este folosit și pentru a desfășura activități ilegale pe Dark Web, datorită anonimatului pe care îl oferă.

- **Organizații și corporații**:
- **Scopuri**: Protejarea comunicărilor interne și a datelor sensibile. Unele companii și organizații folosesc TOR pentru a proteja datele confidențiale și pentru a evita **spionajul industrial**.

# Caz – NSA Whistleblower

Edward Snowden, un fost asistent tehnic de 29 de ani la CIA și angajat al Booz Allen Hamilton, este responsabil pentru dezvăluirile semnificative privind supravegherea NSA.

El a divulgat documente strict secrete pentru a expune amploarea activităților de supraveghere ale NSA, sperând să declanșeze o dezbatere globală despre intimitate și puterea guvernului.

- **PRISM**: Un program care permite NSA să colecteze direct date de la serverele unor mari companii de internet, precum Google, Facebook, Microsoft și Apple. Aceste date includ **e-mailuri, chat-uri video și voce, fotografii, fișiere transferate** și alte informații de comunicație.

- **XKeyscore**: Un sistem de analiză care permite agenților NSA să caute și să analizeze vaste **baze de date** de internet. Prin intermediul acestui program, NSA poate **urmări activitățile online ale utilizatorilor**, inclusiv istoricul de navigare, e-mailuri și căutări pe internet.

# Caz – NSA Whistleblower

**CO-TRAVELER**: Un program care **analizează locațiile telefoanelor mobile** pentru a urmări **mișcările** și **întâlnirile** oamenilor. Acesta ajută la **identificarea tiparelor** de **mișcare** și **asociații** între **indivizi**.

**Dishfire**: Un program care colectează "**aproape toate**" mesajele ***SMS*** trimise zilnic la nivel global. Aceasta include nu doar **conținutul mesajelor**, ci și **informațiile asociate** precum **locațiile** și **contactele**.

# Caz – Wikileaks

Julian Assange este un jurnalist, programator și activist australian cunoscut pentru fondarea WikiLeaks, o organizație non-profit dedicată publicării de informații secrete, documente clasificate și scurgeri de informații.

**Vault 7**: În 2017, WikiLeaks a publicat documente ale **CIA** care dezvăluie detalii despre capabilitățile **agenției** de a **desfășura** operațiuni de **hacking** și **supraveghere cibernetică**, inclusiv **compromiterea** dispozitivelor electronice.

**Guantanamo Files**: Documentele despre **deținuții** de la Guantanamo Bay au expus detalii despre **reținerea** și **interogarea prizonierilor**, evidențiind problemele legate de justiția militară americană.

**Collateral Murder**: Tot în 2010, WikiLeaks a publicat un videoclip militar clasificat care arată un **atac aerian american** în Bagdad, Irak, în care au fost **uciși civili** și doi **jurnaliști Reuters**. Videoclipul a provocat un val de critici la adresa tacticilor militare ale SUA.

# Caz – Silkroad

Silk Road a fost un magazin online ilegal, cunoscut pentru facilitarea vânzării de droguri și alte bunuri și servicii ilicite. A funcționat pe dark web, utilizând rețeaua Tor pentru a anonimiza **locația utilizatorilor** și **tranzacțiile**, și a **acceptat** plăți în **Bitcoin** pentru a asigura **anonimitatea financiară**.

Silk Road a fost creat de **Ross Ulbricht**, un fost student american în fizică, cunoscut online sub pseudonimul „**Dread Pirate Roberts**”. Ulbricht a lansat site-ul în **februarie 2011** și a operat până la arestarea sa în **octombrie 2013**.

# Caz – Silkroad

**Operațiunile Silk Road**

- **Platformă anonimă**: Silk Road a fost construit pe rețeaua Tor pentru a ascunde locațiile serverelor și identitățile utilizatorilor.
- **Plăți în Bitcoin**: Tranzacțiile au fost realizate în Bitcoin, o criptomonedă care oferă un anumit grad de anonimitate.
- **Vânzarea de bunuri ilicite**: Site-ul permitea vânzarea și cumpărarea de droguri, falsuri, date de carduri furate și alte bunuri și servicii ilegale.

•**Arestarea și procesul**

•**Arestarea**: Ross Ulbricht a fost arestat pe 1 octombrie 2013 într-o bibliotecă din San Francisco, în timp ce era conectat la Silk Road.

•**Acuzarea și condamnarea**: Ulbricht a fost acuzat de conspirație pentru trafic de droguri, conspirație pentru spălare de bani și alte infracțiuni. În 2015, a fost găsit vinovat și condamnat la închisoare pe viață fără posibilitatea de eliberare condiționată.

# Caz – Silkroad

**Impactul** Silk Road

Silk Road a avut un impact **semnificativ** asupra **pieţelor online ilegale**, demonstrând cum tehnologiile **anonime** şi **criptomonedele** pot fi folosite pentru **activităţi ilicite**. A creat precedentul pentru multe alte piețe negre online, chiar dacă a fost închis după arestarea lui Ulbricht.

# Caz – The Pirate Bay

The Pirate Bay este unul dintre cele mai cunoscute și controversate site-uri de torrente din lume, cunoscut pentru facilitarea distribuției ilegale de conținut protejat de drepturile de autor, cum ar fi filme, muzică, software și jocuri video.

- **Platformă de torrente**: The Pirate Bay este un site web care permite utilizatorilor să descarce fișiere torrent, care sunt folosite pentru partajarea de conținut digital.

- **Anonimizare și rezistență**: Site-ul operează pe baza tehnologiilor de anonimizare și rezistență, ceea ce îi permite să evite închiderile și blocările de către autorități.

# Caz – The Pirate Bay

Istoric și Fondatori

- **Fondatori**: The Pirate Bay a fost fondat în 2003 de către Gottfrid Svartholm, Fredrik Neij și Peter Sunde, din Suedia.

- **Misiune**: Inițial, **platforma** a fost creată pentru a **facilita** schimbul liber de **informații** și conținut, dar a devenit cunoscută în principal pentru **descărcarea ilegală** de **conținut protejat** de **drepturi** de **autor**.

# Siteurile de torente

Folosesc adesea mai multe strategii pentru a evita acțiunile legale și pentru a-și menține operațiunile în ciuda eforturilor autorităților de a le închide.

- **Schimbarea Domeniilor**: Site-urile de torrente **schimbă frecvent** numele **domeniilor** sau folosesc o rețea de site-uri mirror. Aceasta le permite să treacă **rapid** la un **nou domeniu** în cazul în care cel actual este **confiscat** sau **blocat** de **autorități**. Aceste **domenii** pot fi găzduite în țări cu **legi slabe** în ceea ce privește **drepturile** de **autor** sau aplicarea acestora.

- **Găzduire Offshore**: Multe site-uri de **torrente** sunt găzduite pe servere situate în țări unde nu **există legi stricte** privind drepturile de autor sau unde aplicarea acestora este **minimă**. Aceasta face **dificilă** pentru **autorități** să **confiște** fizic **serverele** din alte țări.

# Filme & Documentare

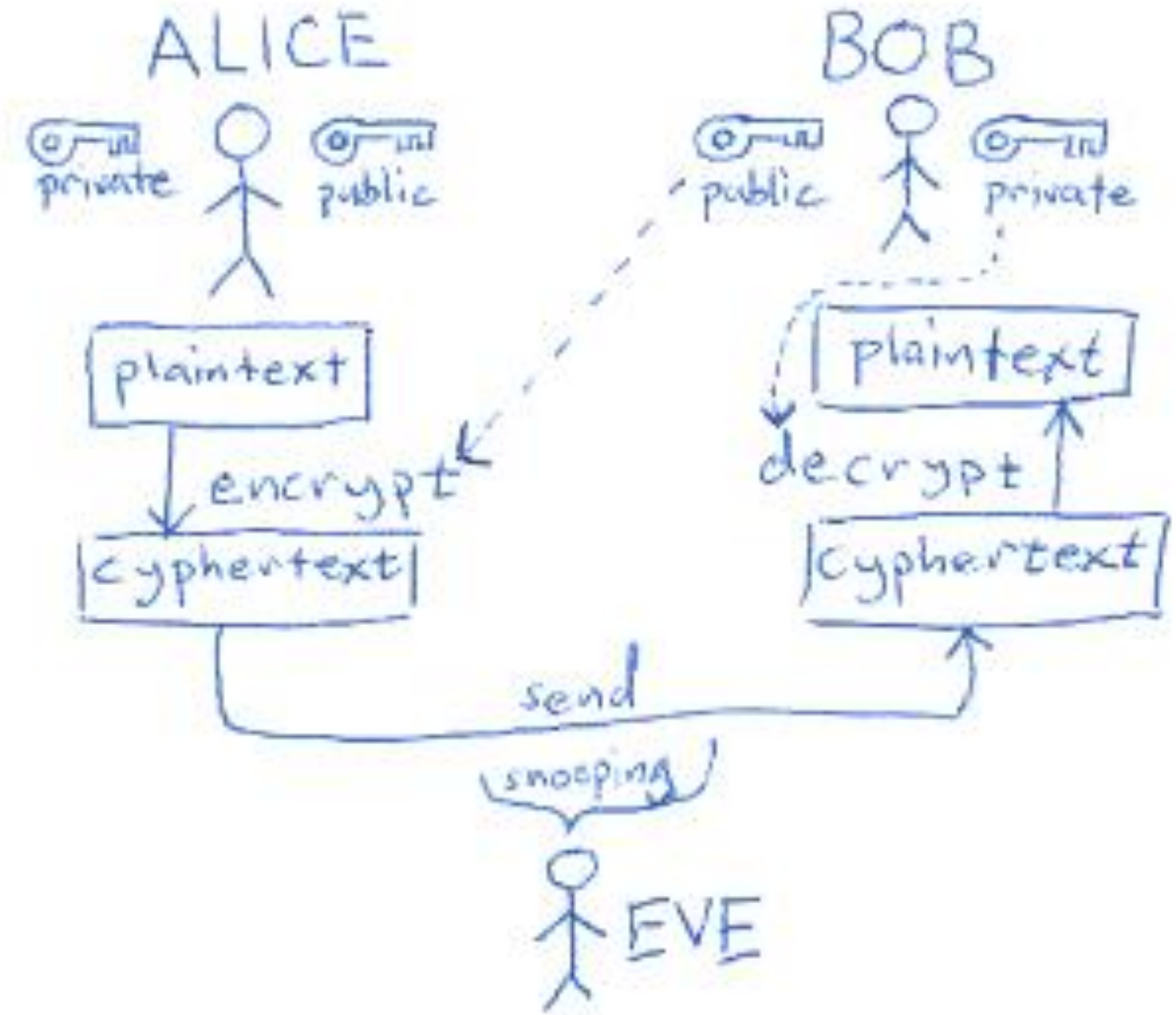
Snownden (2016)

Silk Road (2021)

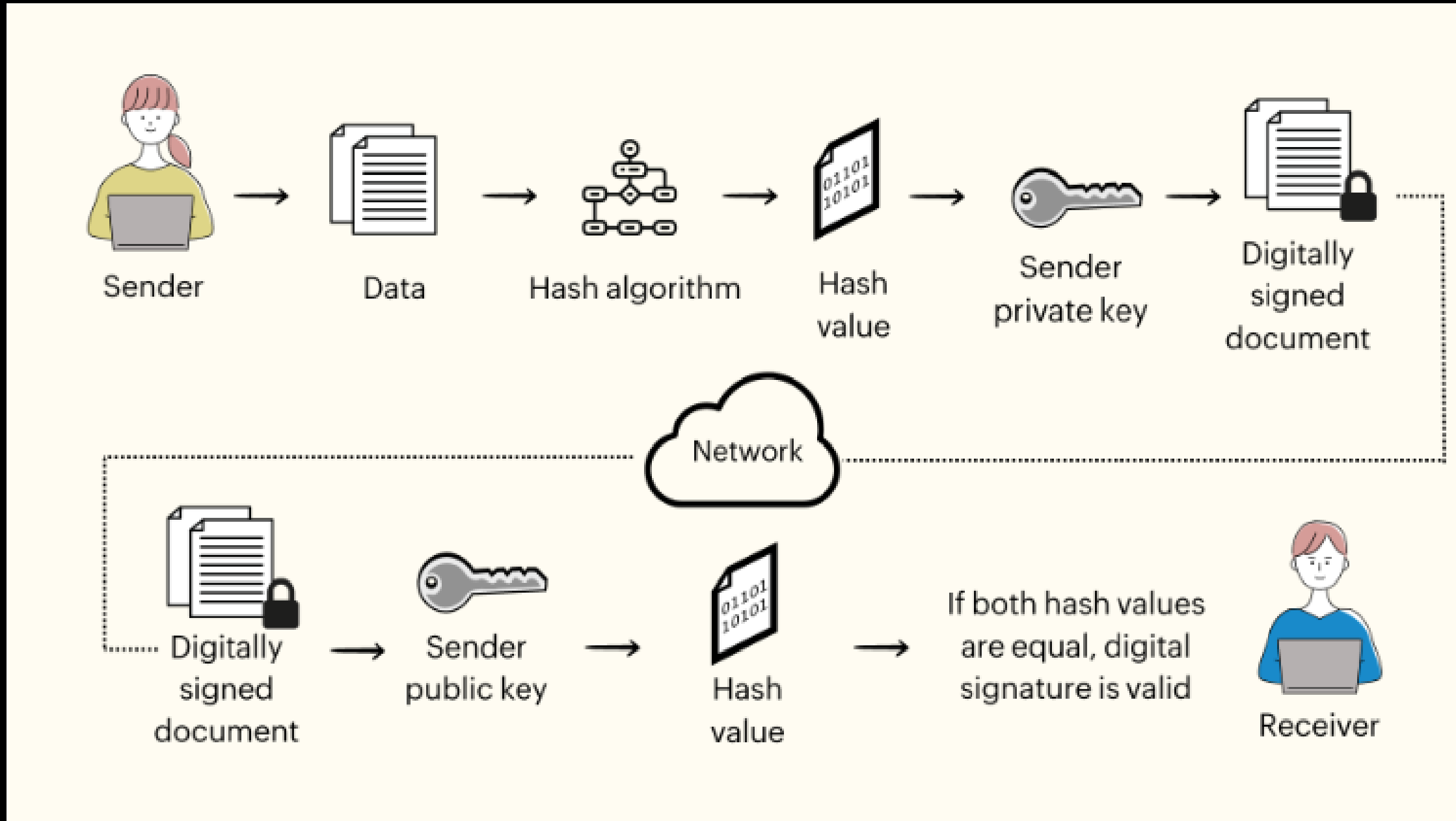
The Fifth Estate (2013) - Wikileaks

TPB AFK – The Pirate Bay Away From Keyboard (2013)

# Criptare Asimetrica



# Semnatura digitala



# Concluzii

Dark web-ul este o parte ascunsă și enigmatică a internetului, accesibilă prin rețele anonime și criptate cum ar fi Tor. În concluzie, iată câteva puncte cheie despre dark web:

- **Anonimat și Confidențialitate**: Dark web-ul oferă utilizatorilor un grad mare de anonimat, permițându-le să navigheze și să interacționeze fără a fi ușor de urmărit sau identificat.
- **Activități Ilegale și Controverse**: Este cunoscut pentru activități ilegale, cum ar fi vânzarea de droguri, arme, date personale și alte bunuri ilegale sau servicii. Aceasta a generat controverse și preocupări legate de securitate și aplicarea legii.
- **Platformă pentru Libertatea de Expresie**: În ciuda reputației sale negative, dark web-ul servește și ca un spațiu unde activiștii pentru drepturile omului, jurnaliștii și alți indivizi vulnerabili pot comunica în siguranță și evita cenzura.
- **Tehnologii Avansate și Riscuri**: Utilizează tehnologii avansate pentru a asigura confidențialitatea, dar adesea este asociat și cu riscuri de securitate, inclusiv atacuri cibernetice, phishing și fraudă.
- **Monitorizare și Reglementare**: Guvernele și agențiile de aplicare a legii monitorizează activitățile pe dark web și iau măsuri pentru combaterea criminalității, ceea ce ridică întrebări despre echilibrul dintre securitate și respectarea drepturilor individuale.

# Referinte


https://ccdcoe.org/uploads/2018/10/TOR_Anonymity_Network.pdf

https://www.cactusvpn.com/beginners-guide-to-online-privacy/what-is-deep-packet-inspection/

https://www.youtube.com/watch?v=6eWkdyRNfqY

https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#/media/File:DiffieHellman.png

https://www.sangfor.com/glossary/cybersecurity/what-is-cia-triad

https://community.fs.com/article/tcpip-vs-osi-whats-the-difference-between-the-two-models.html

https://www.clickssl.net/blog/what-is-symmetric-encryption

# Referinte


https://uk.norton.com/blog/emerging-threats/deep-web-vs-dark-web

https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

https://www.bbc.com/news/world-us-canada-68282613

https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

https://en.wikipedia.org/wiki/The_Pirate_Bay

https://coindesk.com/markets/2014/10/29/bitcoin-over-tor-anonymity-can-be-busted-for-2500-a-month/