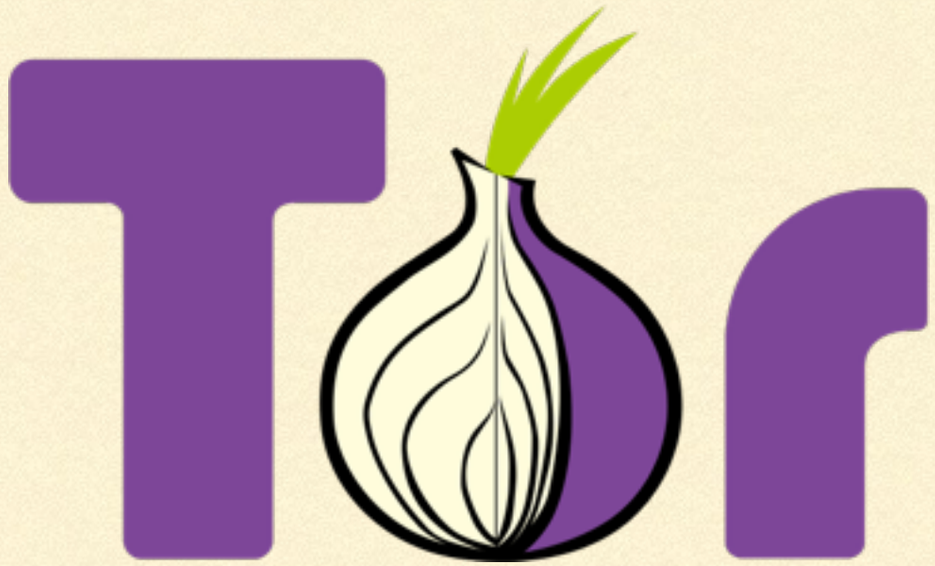
TOR PROJECT



www.torproject.org

INTRODUCTION

Το Tor αποτελεί συντομογραφία του *The Onion Router.* Στόχος του *Tor* είναι να εξασφαλίσει την ανωνυμία της δραστηριότητας στο δίκτυο.

Για να μπορέσουμε να χρησιμοποιήσουμε το δίκτυο του Tor, θα πρέπει να κατεβάσουμε πρώτα τον **Tor browser** και να το εγκαταστήσουμε.

link: https://www.torproject.org/download/download-easy.html.en

IS IT SAFE?

Σύμφωνα με δηλώσεις του Snowden TOR και PGP αποτελούν σοβαρό πρόβλημα για κάποιον που θέλει να υποκλέψει και να αποκρυπτογραφίσει μηνύματα.

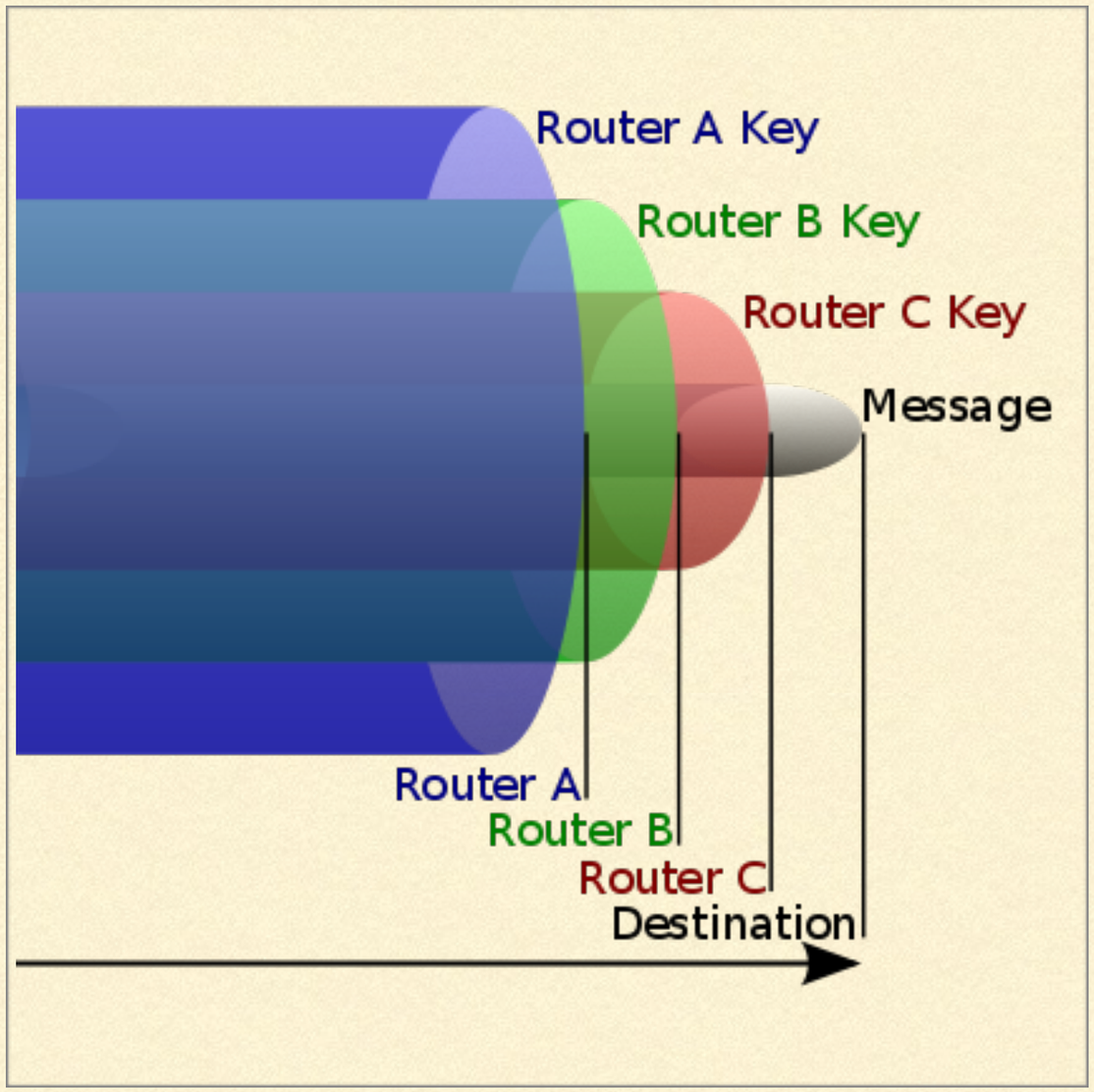
ABOUT TOR

- Πρώτη έκδοση: 20 Σεπτεμβρίου 2002 (αρχικά αναπτύχθηκε το 1990 από το αμερικανικό ναυτικό)
- Είναι γραμμένο σε C
- Δουλεύει στα περισσότερα λειτουργικά(unix, windows, os x, android)
- Τύπος άδειας: BSD
- Κρυπτογράφιση: AES, Elliptic Curve DSA, RSA (2014)

TOR BASIC NODES

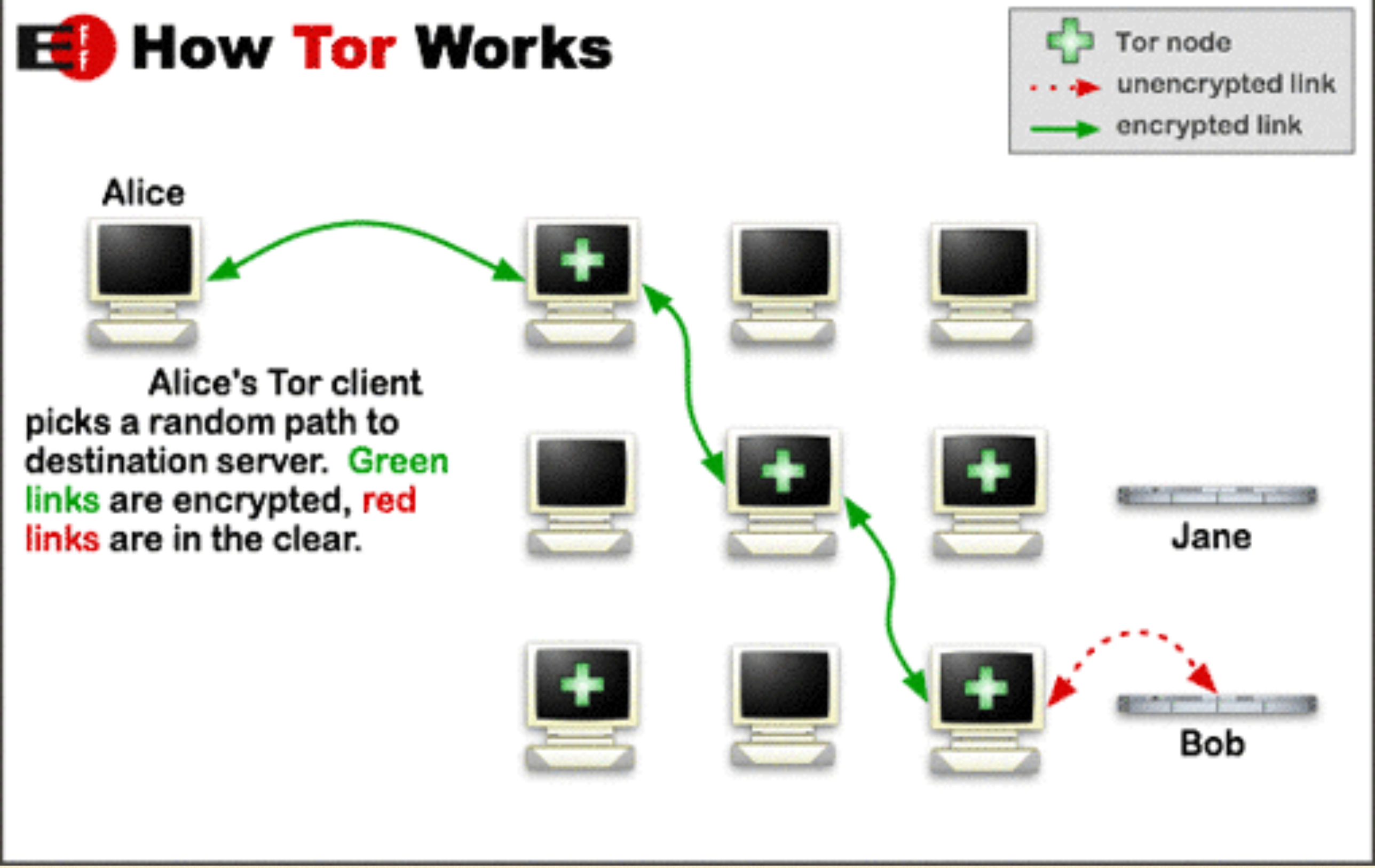
- **Entry node**: Είναι ο πρώτος κόμβος του δικτύου από τον οποίο εισέρχεται το πακέτο.
- **Relay**: Είναι ο ενδιάμεσος κόμβος (μπορεί να είναι και περισσότεροι) από τον οποίο θα περάσει το πακέτο μας
- **Exit node**: Είναι ο κόμβος στο οποίο αφαιρείται και το τελευταίο επίπεδο κρυπτογράφισης, και το πακέτο φτάνει στον τελικό προορισμό του.
- ***Bridge***: Αυτοί οι κόμβοι δεν περιέχονται στις λίστες με τους κόμβους του tor. Σε περίπτωση που έχει απαγορευτεί η πρόσβαση στους άλλους κόμβους μπορεί κανείς να χρησιμοποιήσει έναν τέτοιο για να έχει πρόσβαση στο δίκτυο του TOR.

HOW IT WORKS



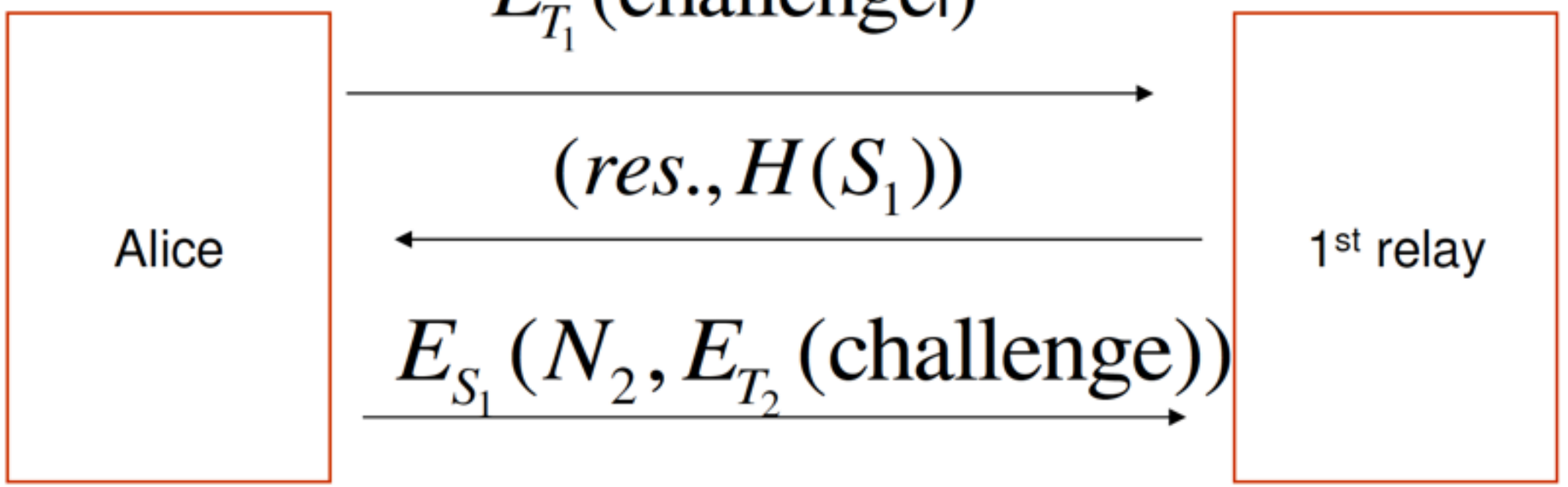
- Καθε μήνυμα προστατεύεται απο 3 επίπεδα κρυπτογράφησης
- Σε κάθε relay αφαιρείται και απο ένα
- Τελικά ο exit node διαβάζει το περιεχόμενο του μηνύματος

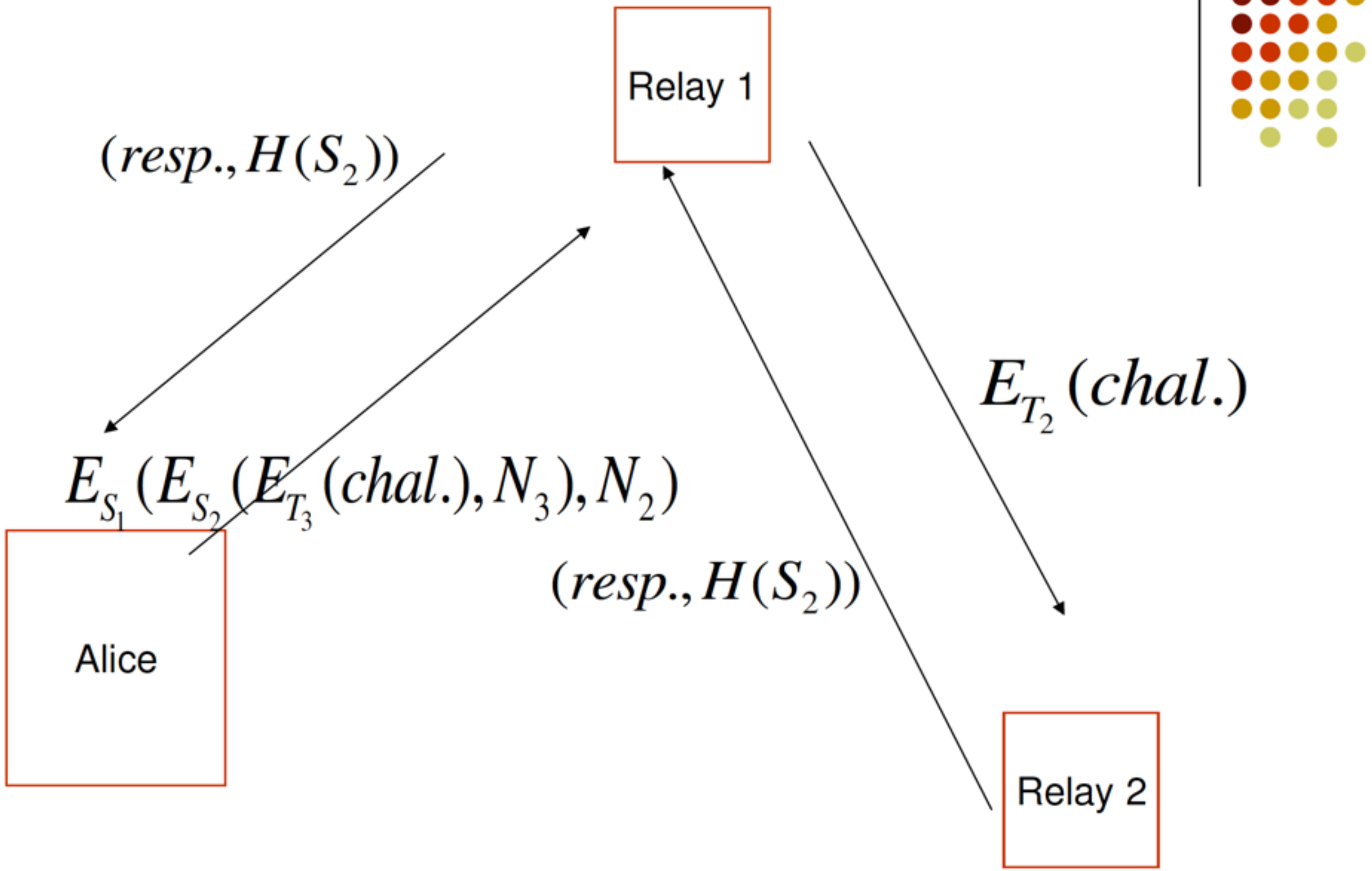
How Tor Works



PUBLIC KEY VERIFICATION

Έστω οτι η Alice θέλει να στείλει κάποιο μήνυμα μέσω του δικτύου tor. Έχοντας τα δημόσια κλειδιά των κόμβων από τους οποίους θα περάσει το μήνυμα, θα τους στείλει ένα μήνυμα επιβεβαίωσης του δημόσιου κλειδιού και θα πάρει ένα μήνυμα με το hash του δημοσίου κλειδιού. Στη συνέχεια θα το συγκρίνει με το hash από το δημόσιο κλειδί που ήδη έχει, και θα κάνει την επιβεβαίωση οτι είναι σωστό το κλειδί.


E_{T_1}(challengel)
$(res., H(S_1))$
Alice
1st relay
$E_{S_1}(N_2, E_{T_2}(\text{challenge}))$

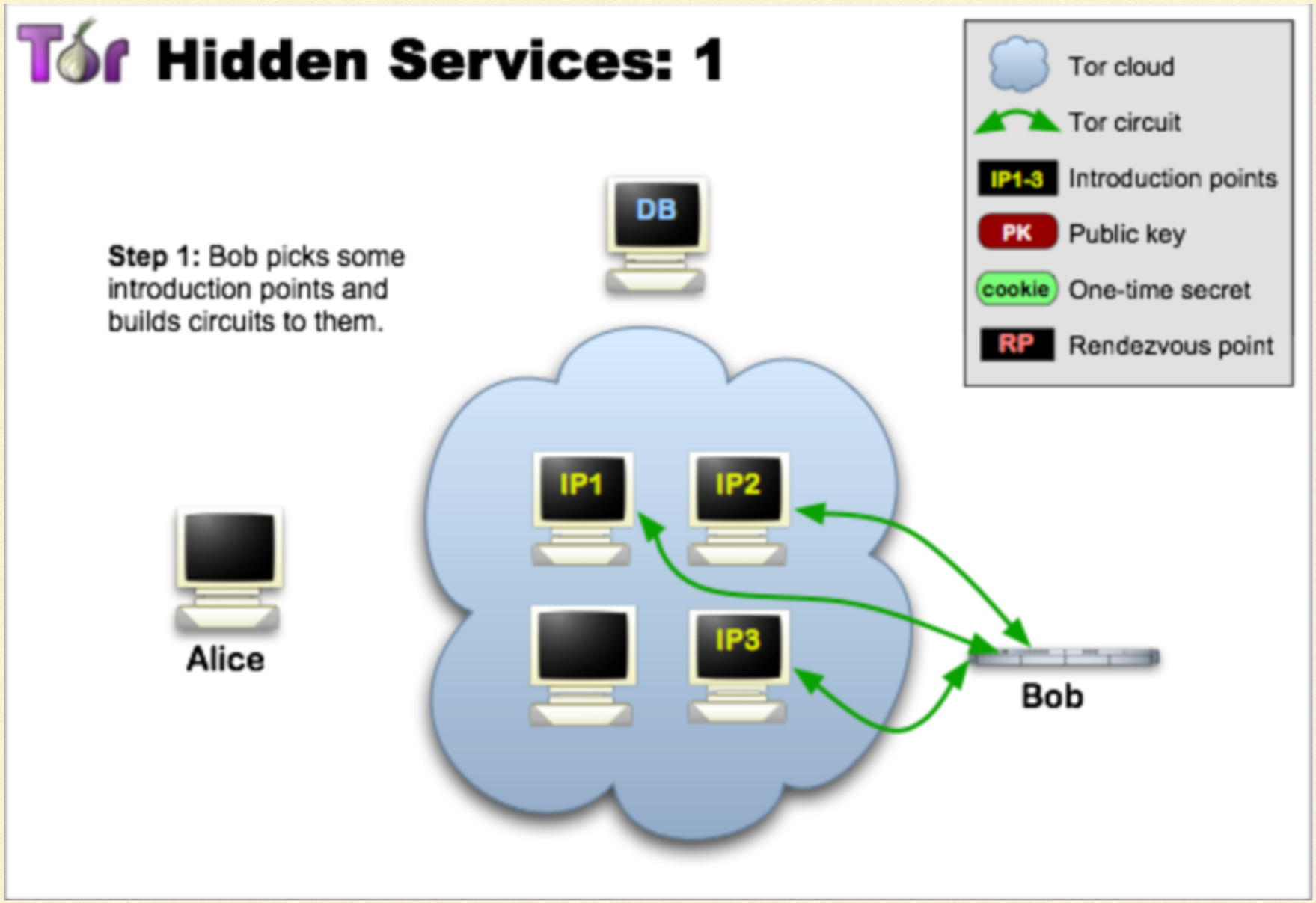

Relay 1
$(resp., H(S_2))$
$E_{T_2}(chal.)$
$E_{S_1}(E_{S_2}(E_{T_3}(chal.), N_3), N_2)$
$(resp., H(S_2))$
Alice
Relay 2

HIDDEN SERVICES

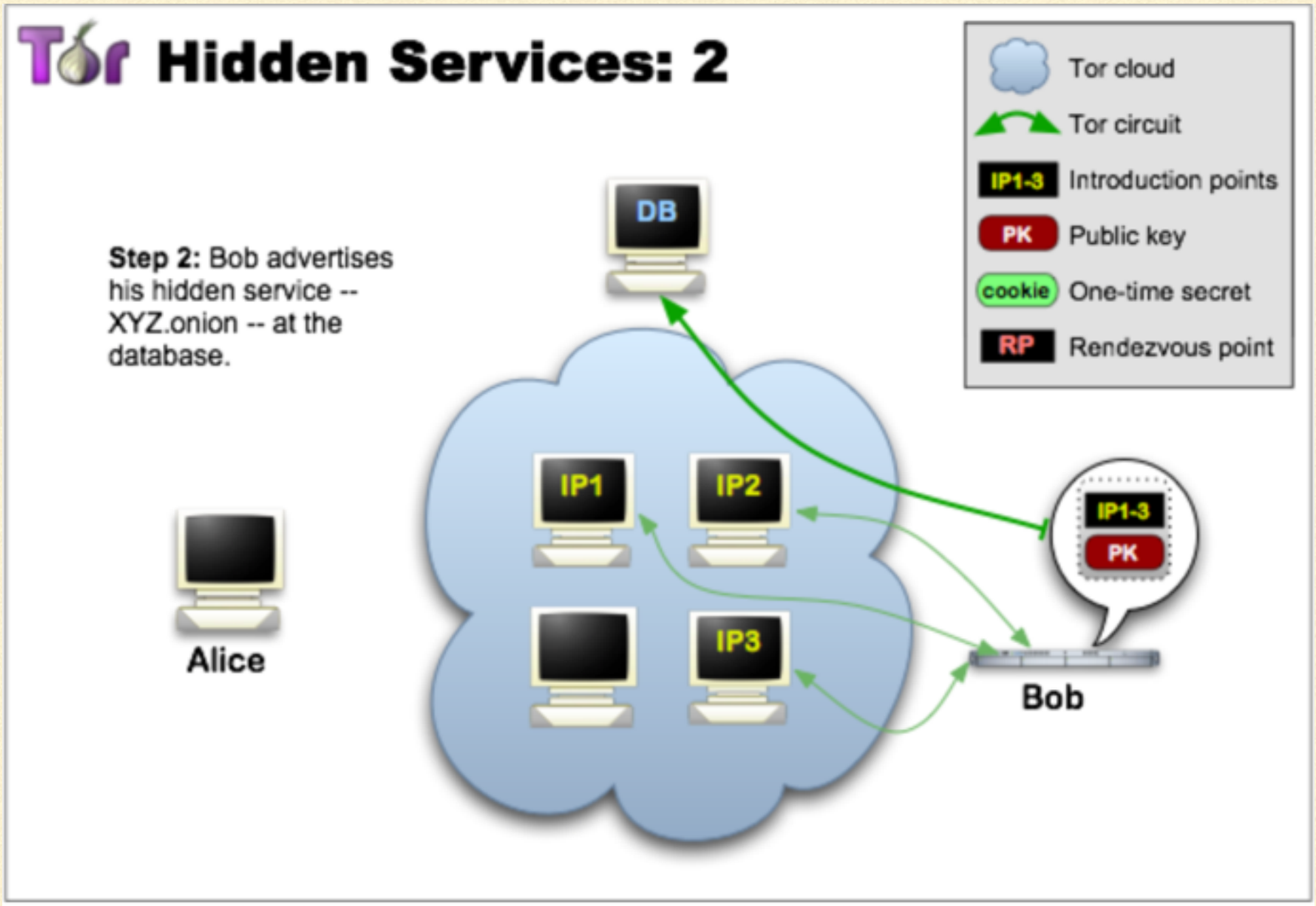
Υπάρχουν site τα οποία έχουν κατάληξη .onion, τα οποία μπορεί να τα επισκεφτεί κανείς μόνο μέσω του tor browser. Επίσης, οι διευθύνσεις δεν μοιάζουν με τις διευθύνσεις των άλλων browsers.

wikileaks url: http://gjlng65kwikileax.onion

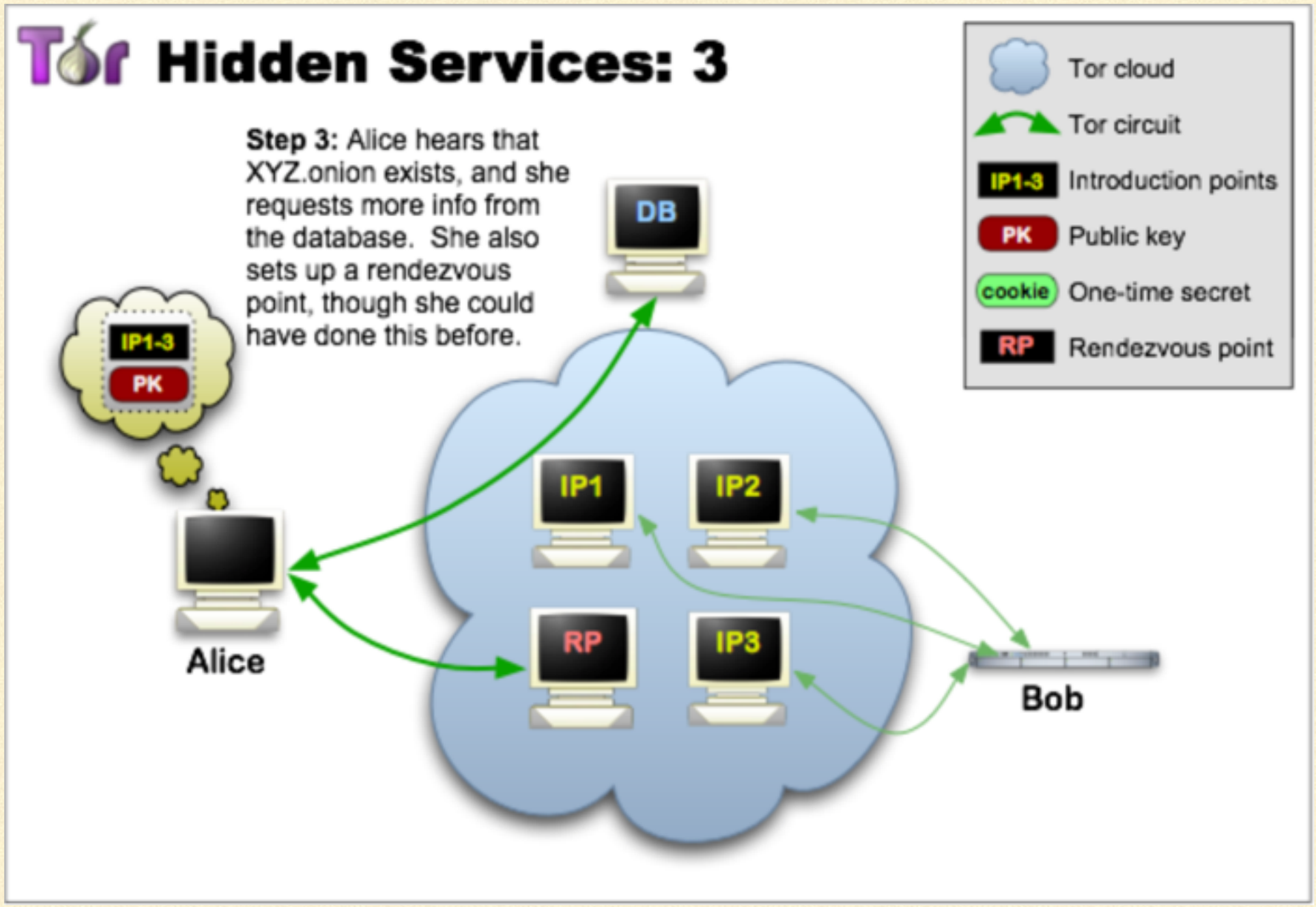
HOW THEY WORK (1/6)



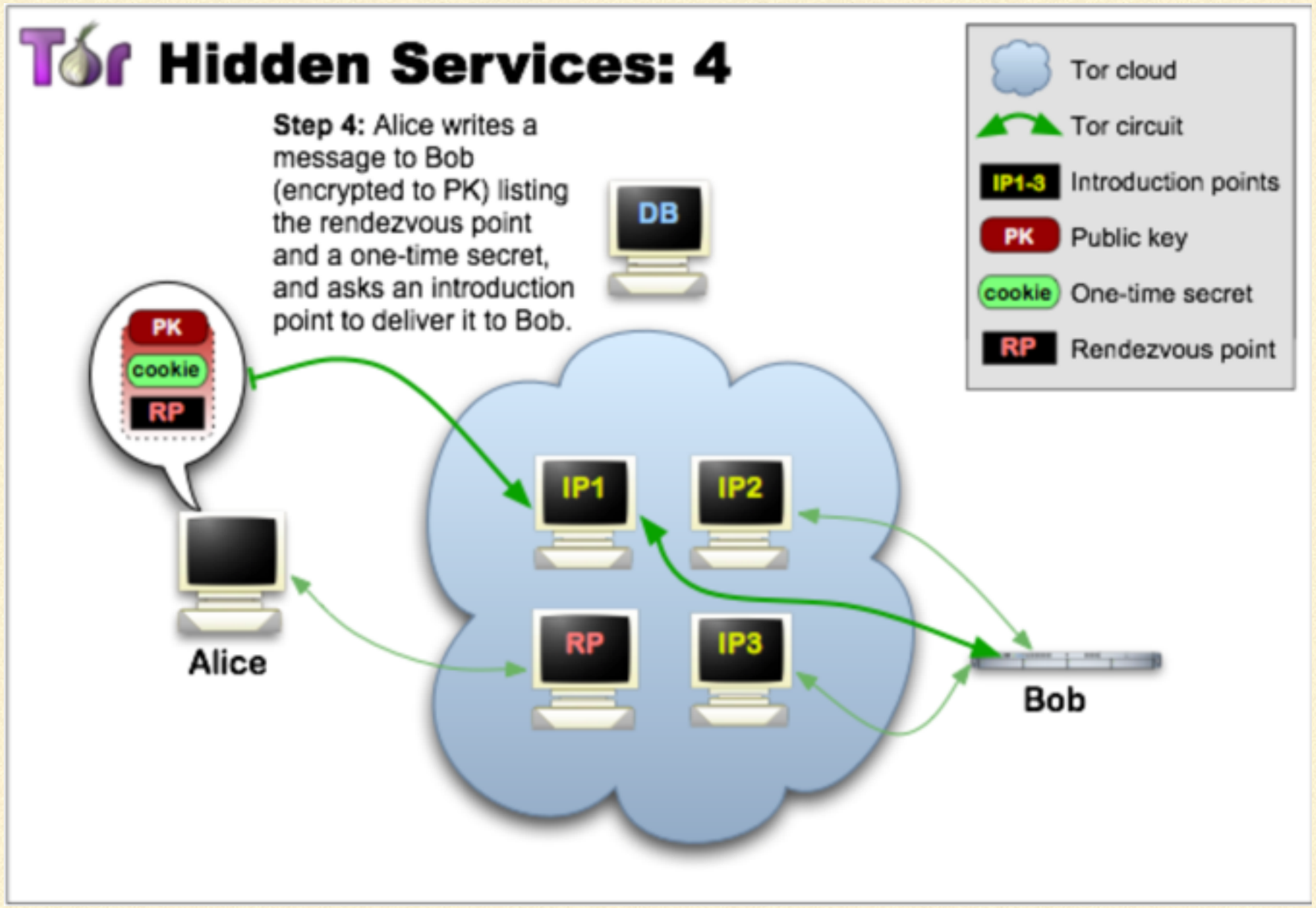
HOW THEY WORK (2/6)



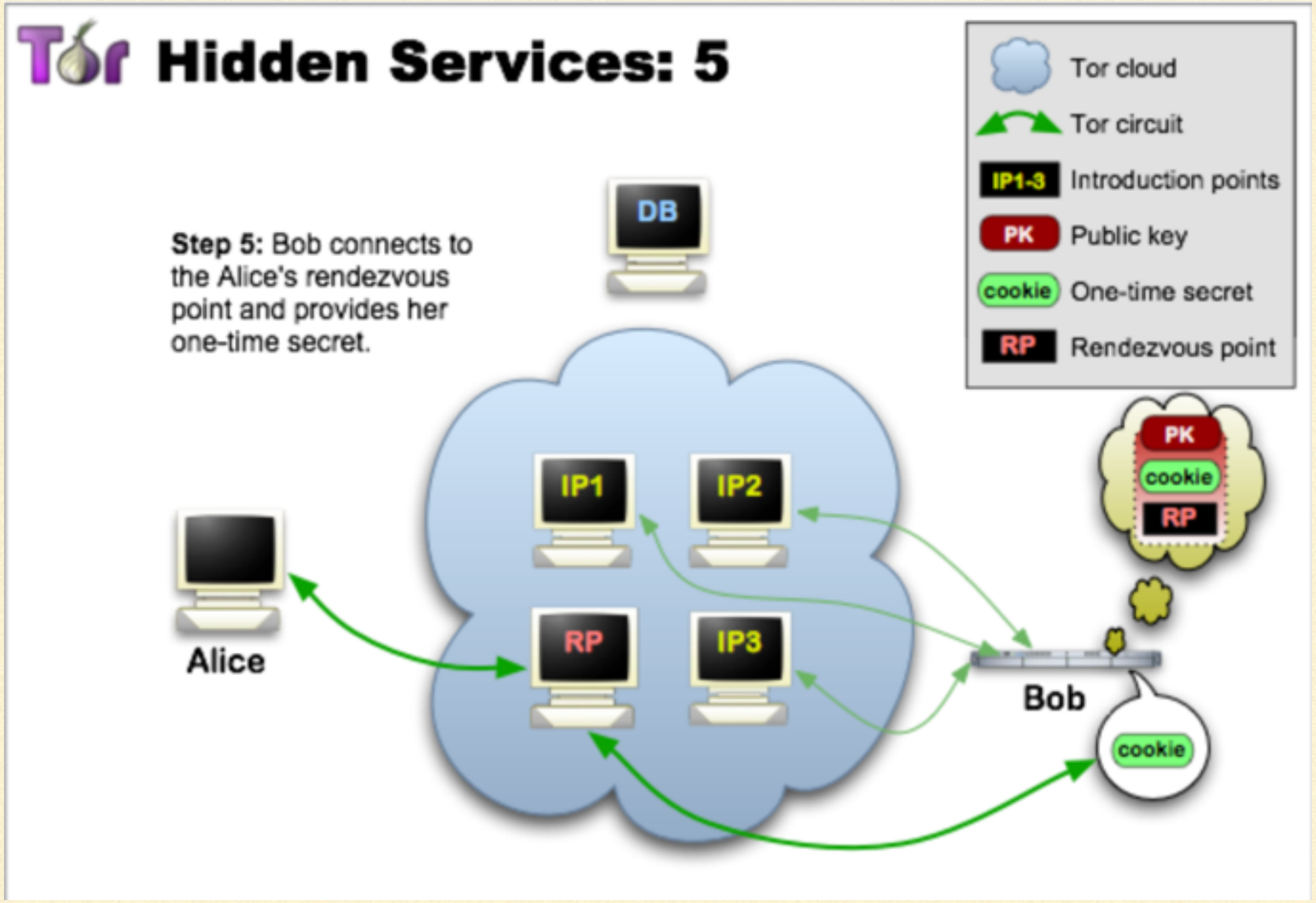
HOW THEY WORK (3/6)



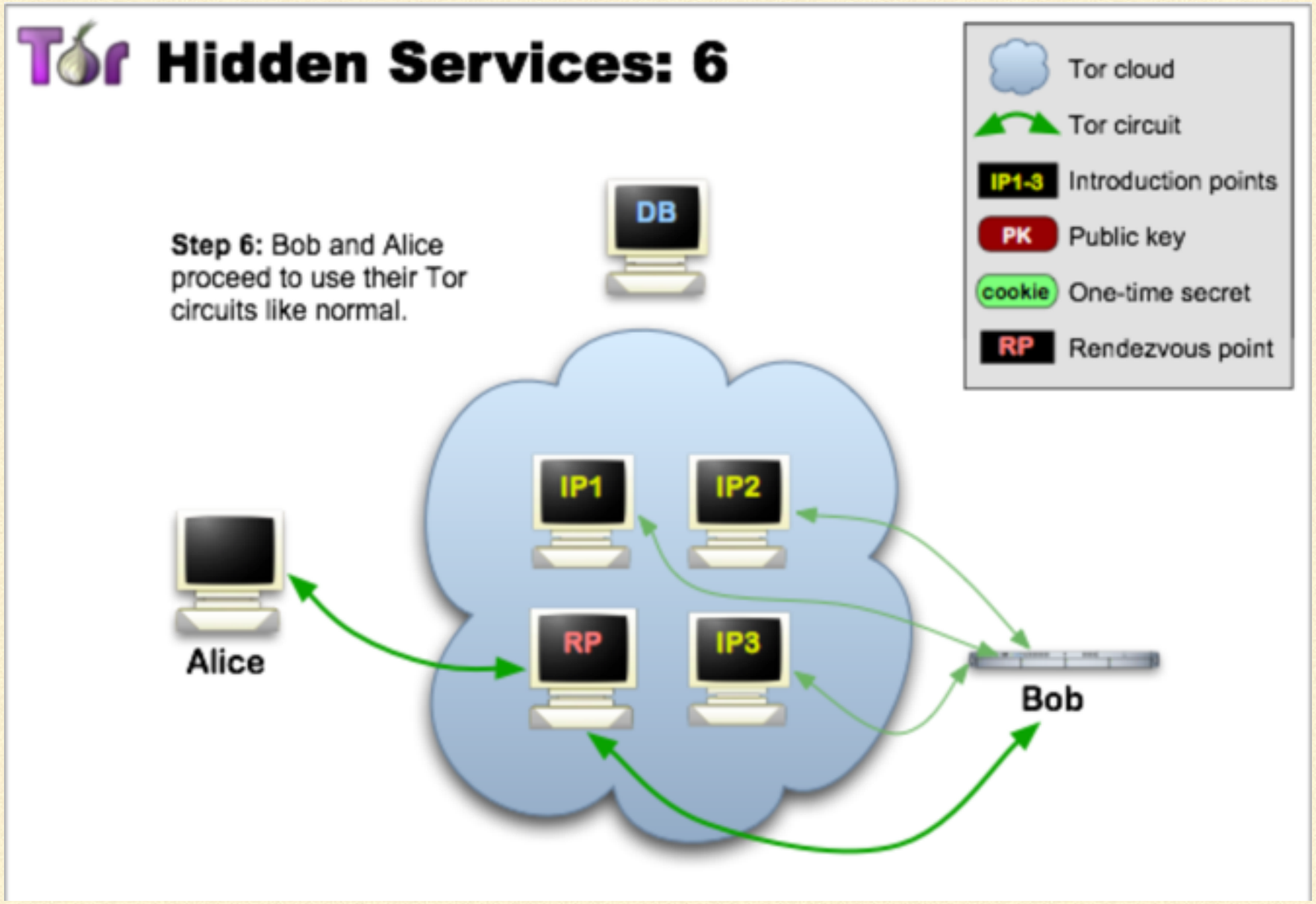
HOW THEY WORK (4/6)



HOW THEY WORK (5/6)



HOW THEY WORK (6/6)



CONSTRUCTION OF .ONION URLS

Έστω οτι η Alice θέλει να επισκεφθεί την τοποθεσία z.onion. Το z είναι αποτέλεσμα ενός base 32 encoding του hash (SHA1) μίας 10-octet από το public key της υπηρεσίας.

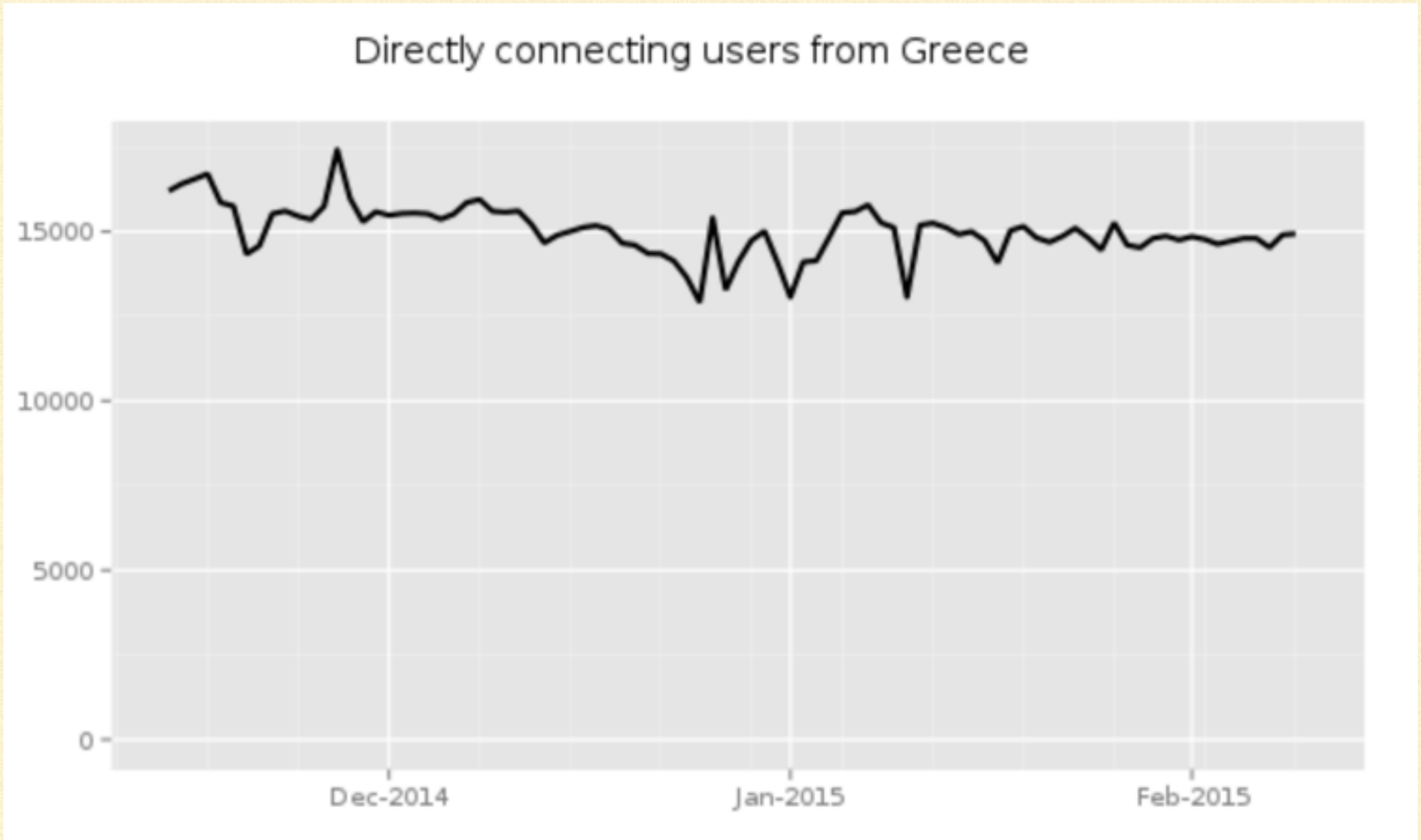
Αναλυτικά:

1. Let H = H(PK).
2. Let H' = the first 80 bits of H, considering each octet from most significant bit to least significant bit.
3. Generate a 16-character encoding of H', using base32 as defined in RFC 4648.

CORRELATION ATTACK

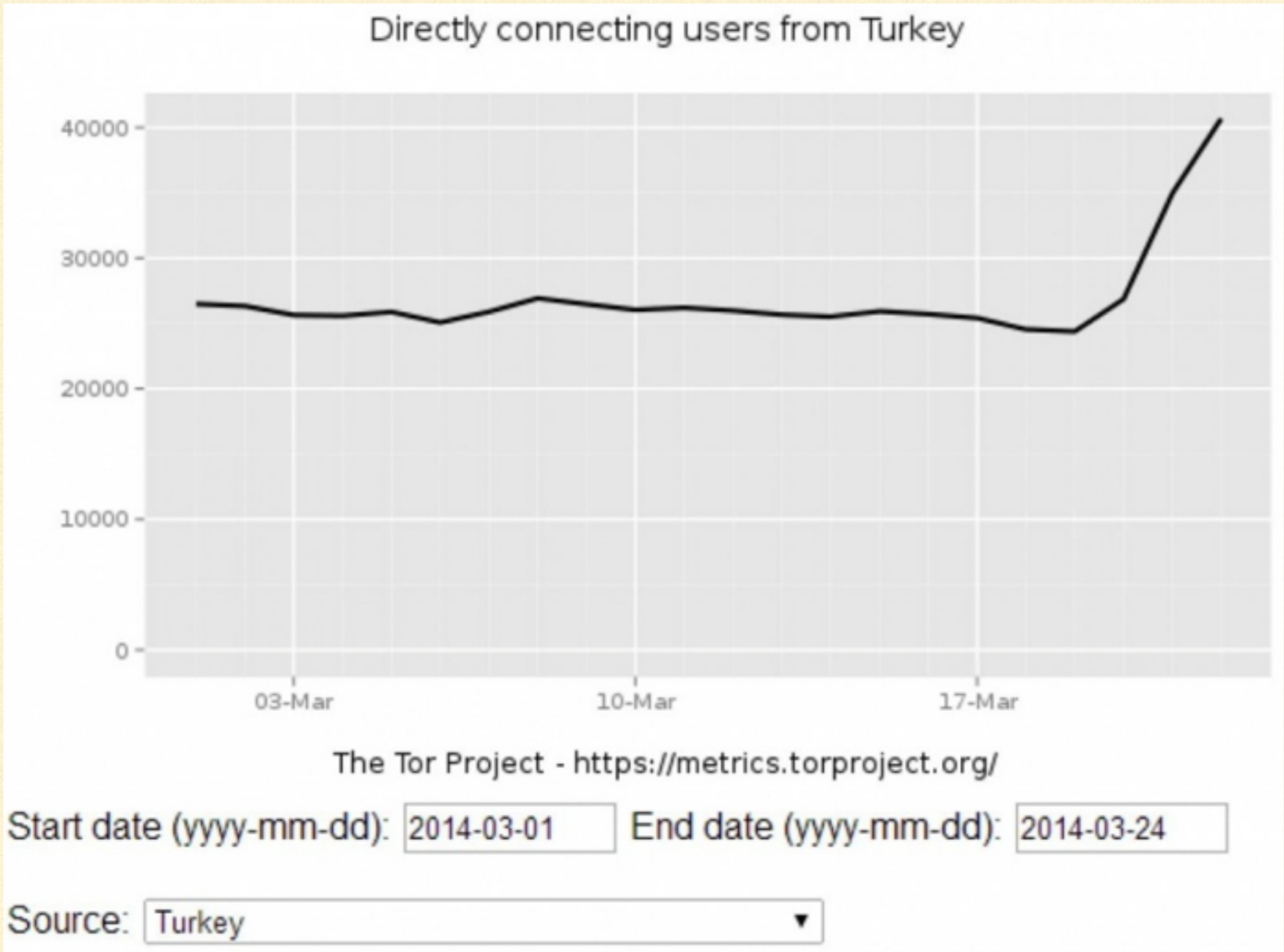
Στην περίπτωση που είναι compromised ο 1ος και ο 3ος κόμβος είναι πιθανό να μπορεί να βρεί κάποιος πληροφορίες για εμάς.
Αυτό μπορεί να γίνει εντοπίζοντας ένα πακέτο που εισέρχεται στο δίκτυο, και μετά απο λίγο εντοπίζοντας ένα λίγο μικρότερο (καθώς αφαιρέθηκαν 2 στρώματα κρυπτογράφησης) πακέτο στον exit node. Με τον τρόπο αυτό μπορεί να γίνει μια συσχέτιση των πακέτων που εισέρχονται στο δίκτυο, με τα πακέτα που εξέρχονται.

TOR METRICS



https://metrics.torproject.org

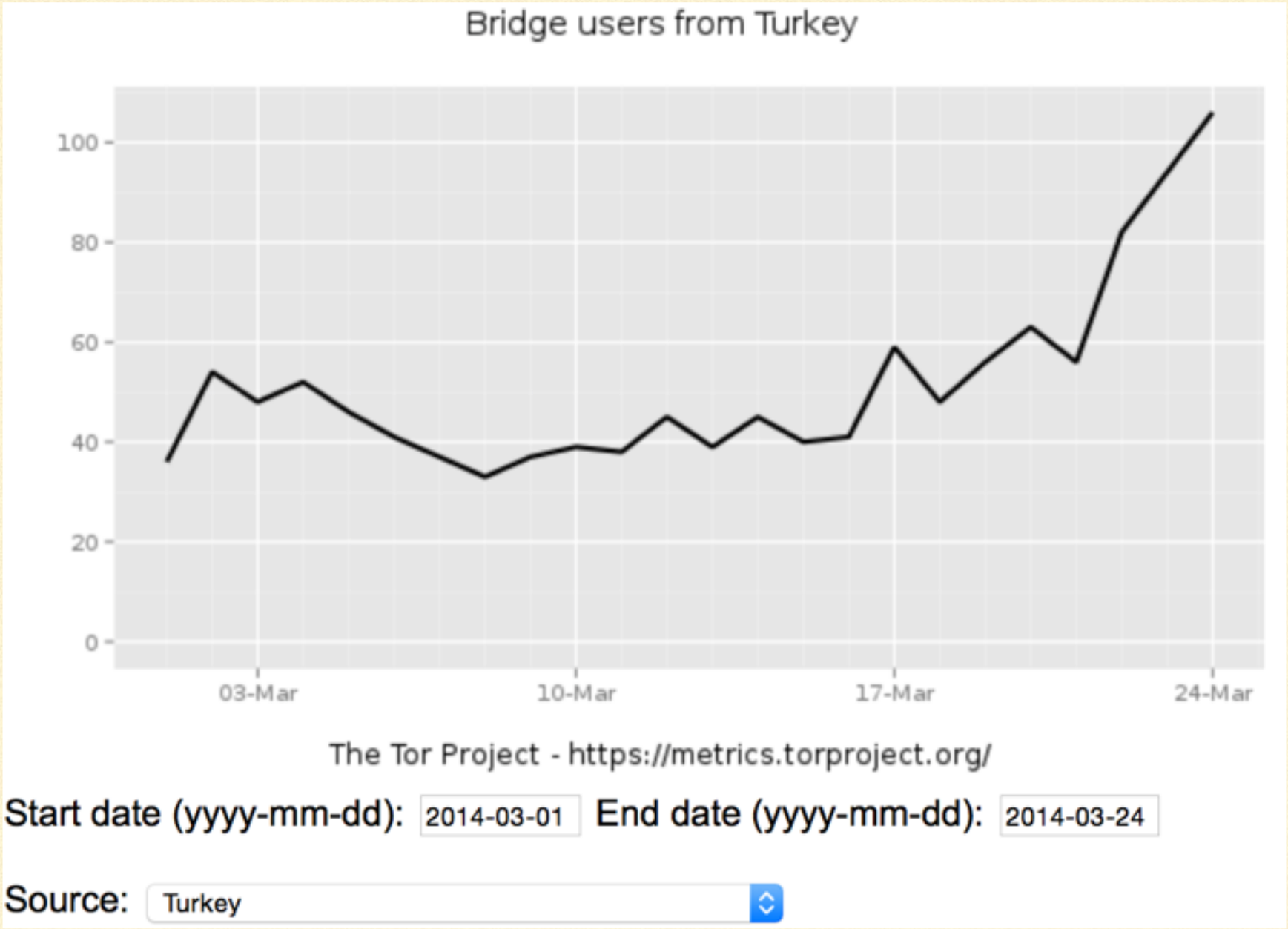
ΑΥΞΗΣΗ ΧΡΗΣΗΣ ΤΟΥ TOR



TURKEY BANS TWITTER

Αρχικά οι ISPs εφάρμοσαν την απαγόρευση σε επίπεδο DNS redirection. Αυτό όμως μπορούσε να παρακαμφθεί εύκολα, διαλέγοντας έναν DNS server εκτός της χώρας. Στην συνέχεια όμως η απαγόρευση έγινε σε επίπεδο IP. Τότε πολλοί χρήστες επέλεξαν εναλλακτικές μεθόδους πρόσβασης του twitter όπως π.χ. τη χρήση VPN και φυσικά το TOR.

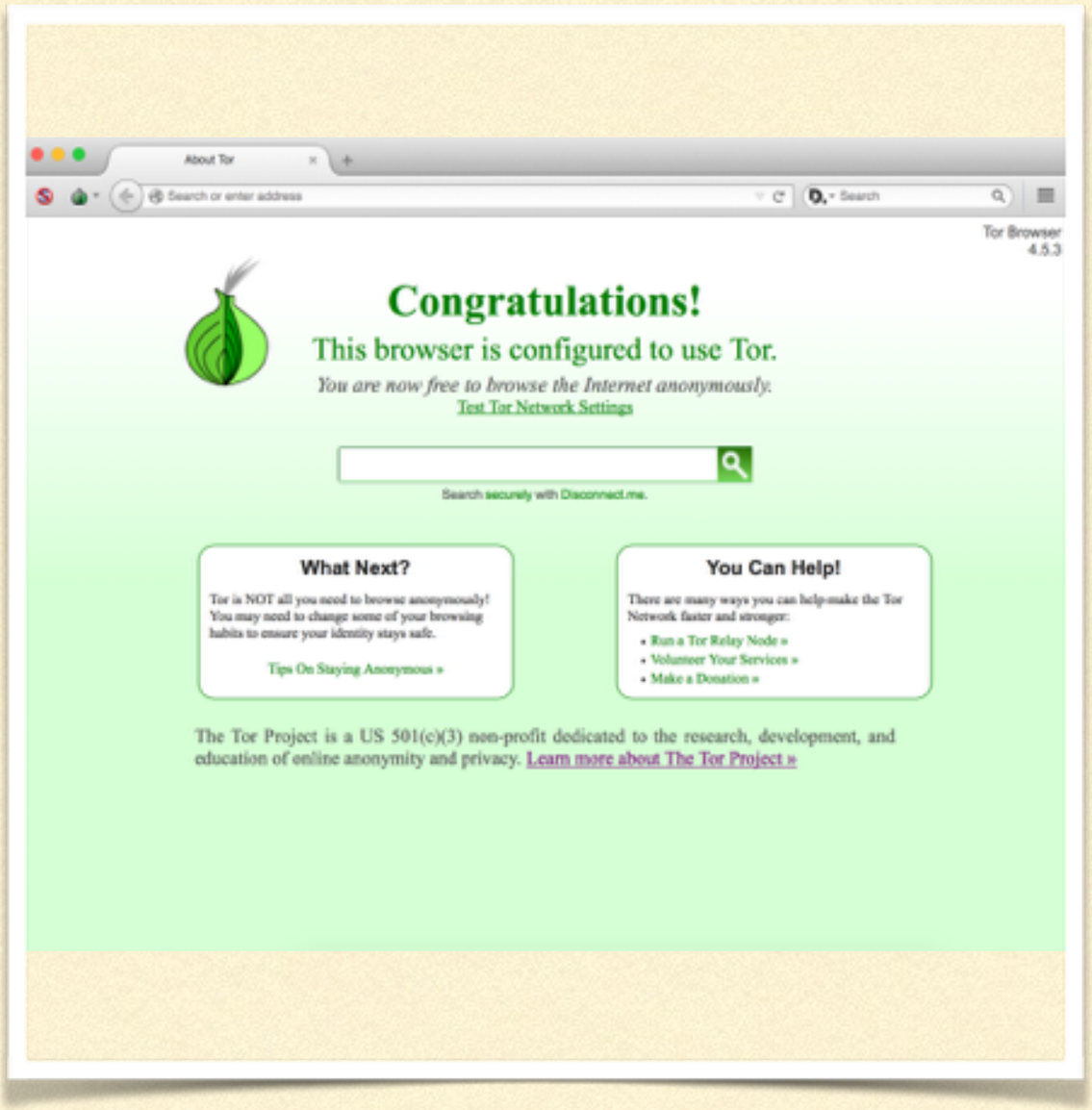
BRIDGE USAGE INCREASE



TIPS TO STAY SECURE

- Χρησιμοποιούμε tor browser
- Δεν κατεβάζουμε torrent *
- Δεν χρησιμοποιούμε plugins (i.e. flash player)
- Χρησιμοποιούμε HTTPS
- Δεν ανοιγουμε doc και pdf αρχεία που κατεβάσαμε μεσω tor, όσο είμαστε ακόμα συνδεδεμένοι

TOR BROWSER

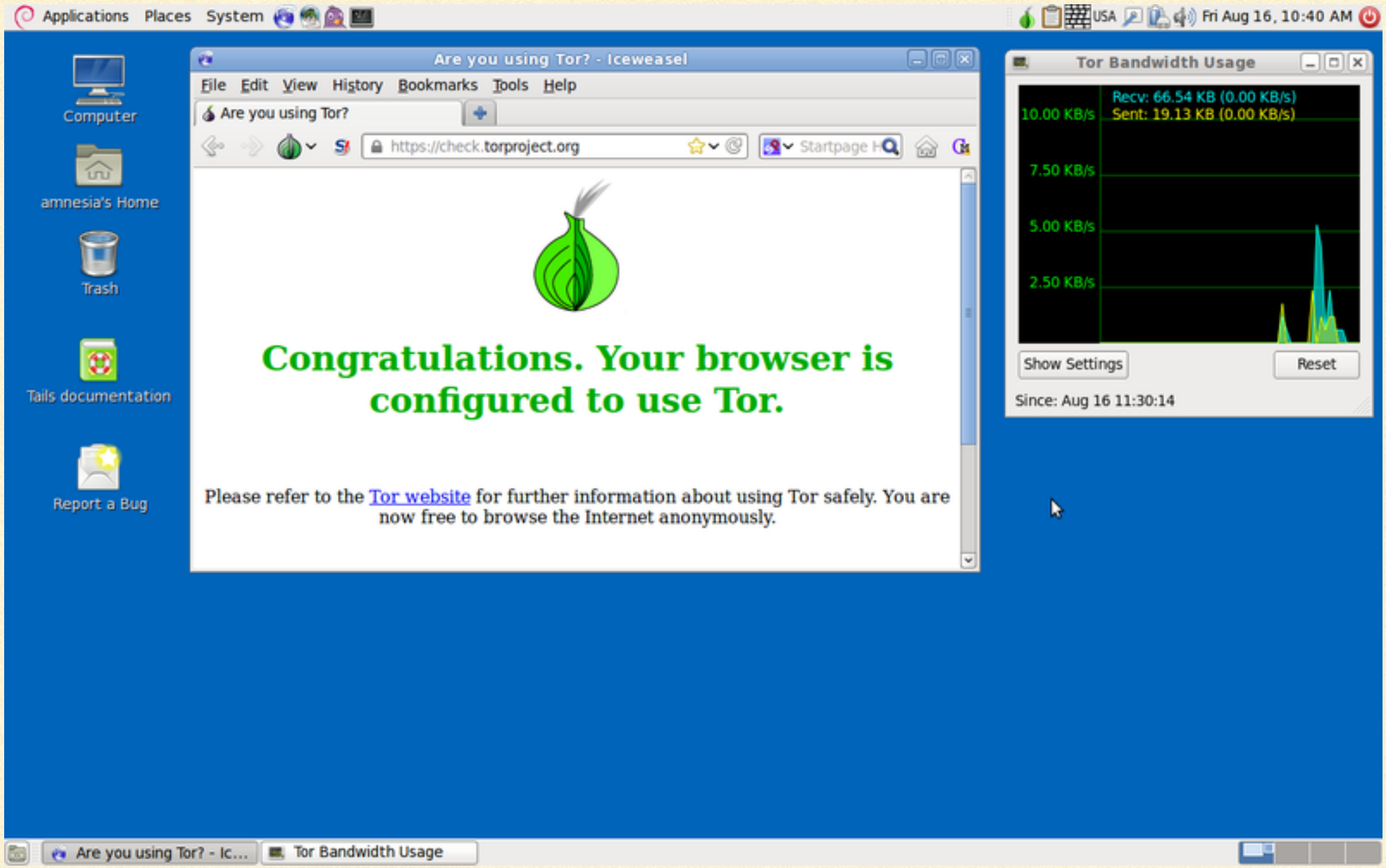


Ο Tor browser (παλαιότερα γνωστός ώς Tor Browser Bundle TBB), αποτελεί μια διαφορετικη έκδοση του firefox και αποτελεί τη ναυαρχίδα των προϊόντων της κοινότητας του Tor

TAILS OPERATING SYSTEM

Το λειτουργικο σύστημα tails είναι ένα debian-based linux distribution, το οποίο κάνει όλες τις συνδέσεις μόνο μέσω TOR και είναι σχεδιασμένο ώς ένα bootable live-DVD το οποίο δεν αφήνει καθόλου ίχνη (digital footprints) στο μηχάνημα το οποίο βρίσκεται.

TAILS DESKTOP

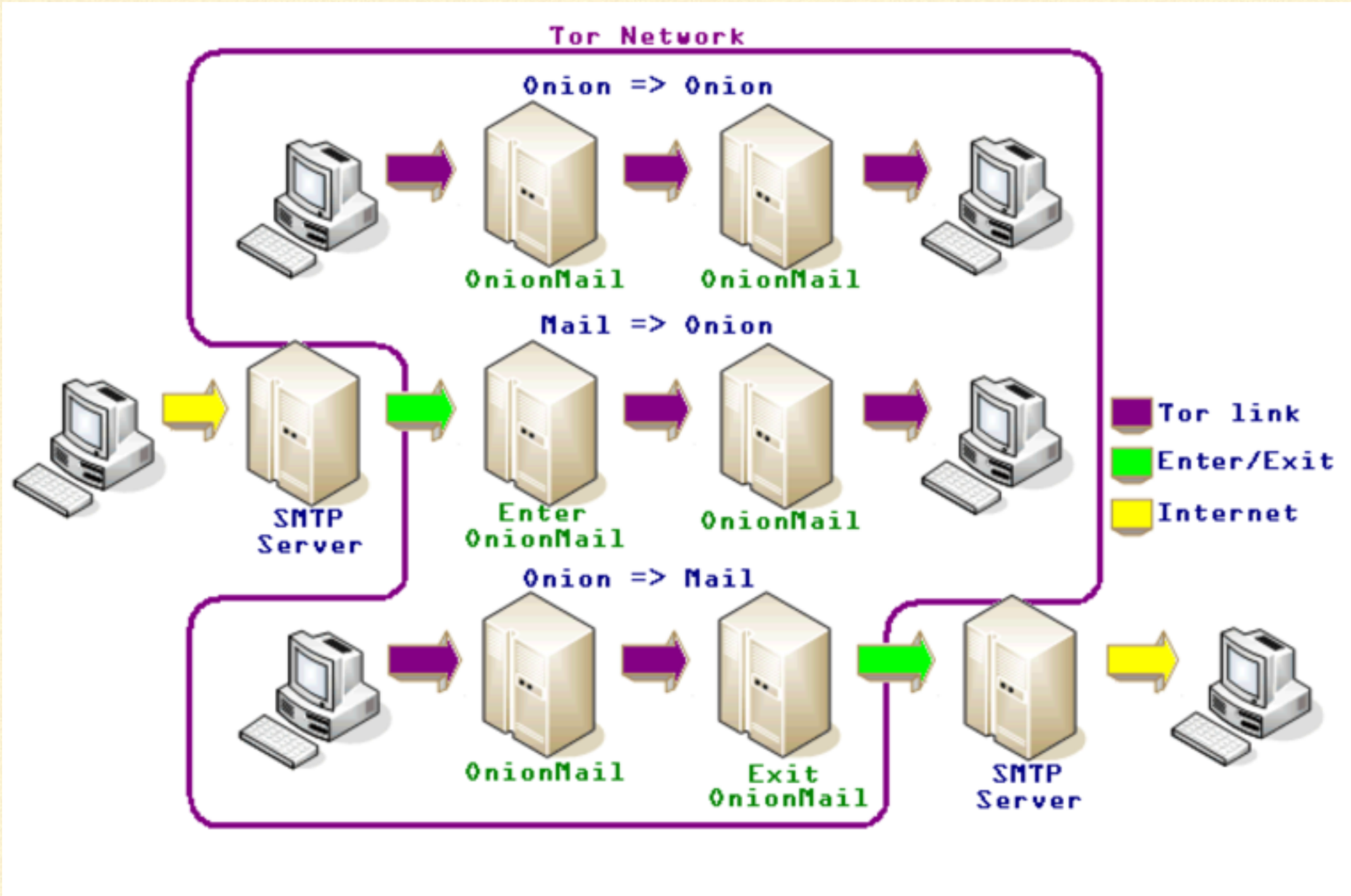


ONION-MAIL

Εκτός από το browsing υπάρχει και η δυνατότητα χρήσης του δικτύου αυτού για την αποστολή email. Αυτή η μέθοδος ονομάζεται OnionMail. Μας εξασφαλίζει οτι η σύνδεση θα είναι πάντα κρυπτογραφημένη, καθώς και οτι ο server δεν αποθηκεύει αρχεία στον δίσκο.

http://onionmail.info/paper.html

ONION-MAIL DIAGRAM



TORBIRDY

Το TorBirdy είναι ένα extension του thunderbird το οποίο κάνει τις συνδέσεις μεσω του tor και μπορεί να χρησιμοποιηθεί για την διατήρηση της ανωνυμίας μας. Υπάρχουν βήμα-βήμα οδηγίες για την χρήση του TorBird στο thunderbird.

https://addons.mozilla.org/en-us/thunderbird/addon/torbirdy/

WHO USES TOR?

- Δημοσιογράφοι
- Αστυνομία και σώματα ασφαλείας
- Ακτιβιστές
- Bloggers
- Στρατός
- IT professionals
- Καθημερινοί άνθρωποι που θέλουν ανώνυμη περιήγηση

https://www.torproject.org/about/torusers.html.en

STEM

Το stem είναι μια βιβλιοθήκη python με την οποία μπορούμε να γράψουμε scripts για το TOR. Από το site μπορεί κανείς να το κατεβάσει, αλλά και να δεί tutorials σχετικά με την χρήση του.

https://stem.torproject.org/index.html

ORBOT (ANDROID)

ΕΥΧΑΡΙΣΤΩ!

Last but not least: https://www.eff.org/pages/tor-and-https

e-mail: ksdimkas@csd.auth.gr

Λοιπές πηγές: en.wikipedia.org