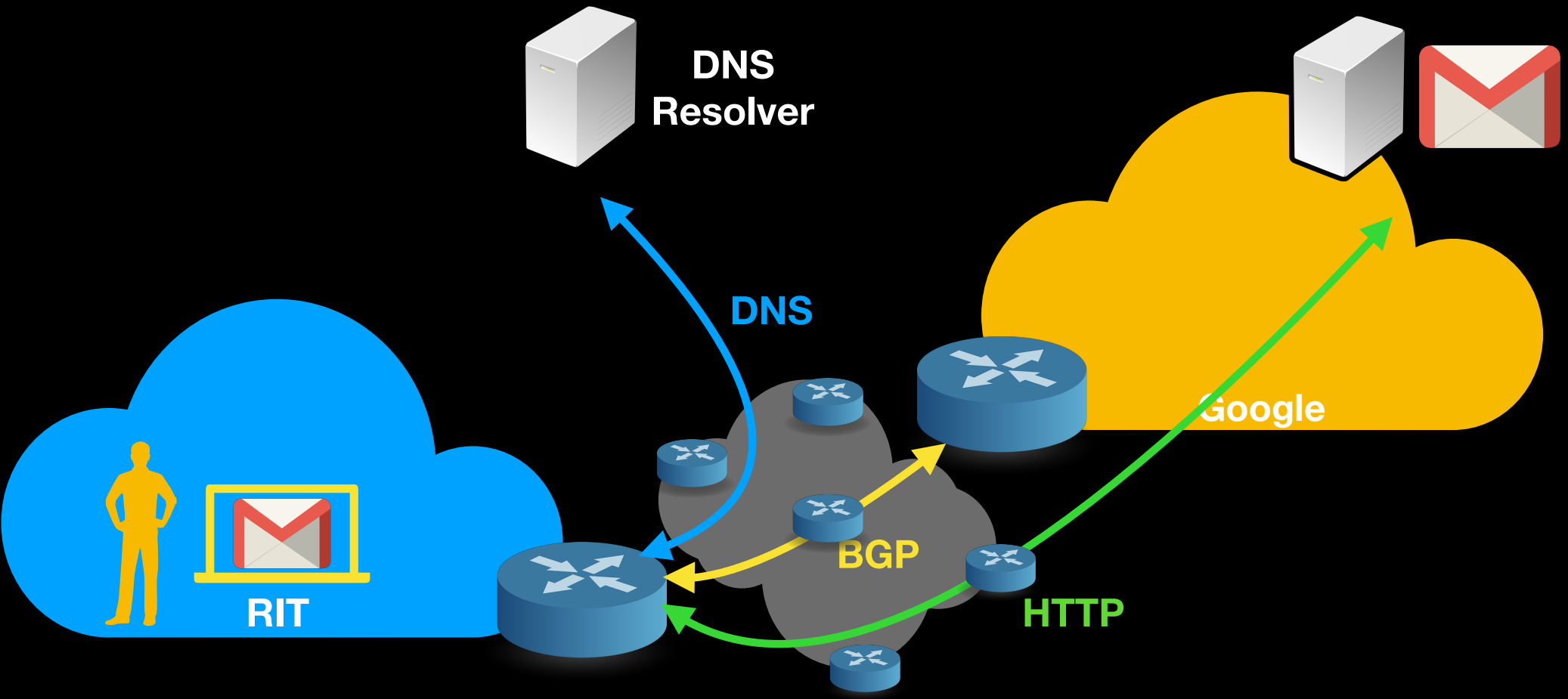
CSCI-759
Topics In Systems: Public Key Infrastructure and Network Security

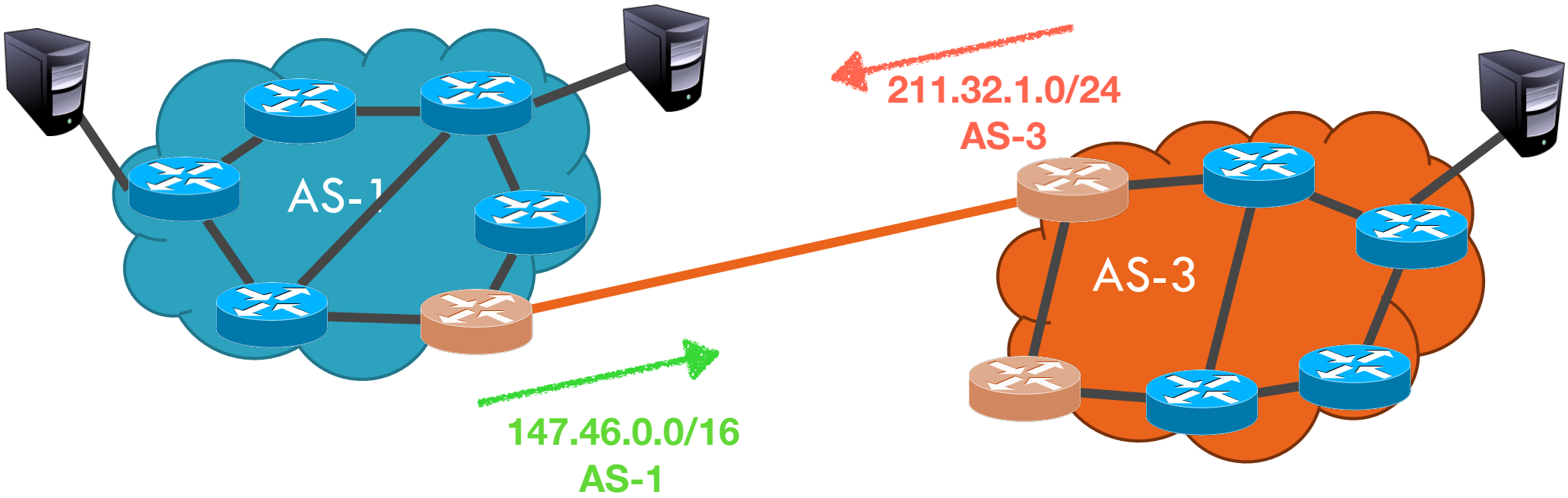
Lecture 1: Network protocols and PKI

CSCI-351 Data communication and Networking

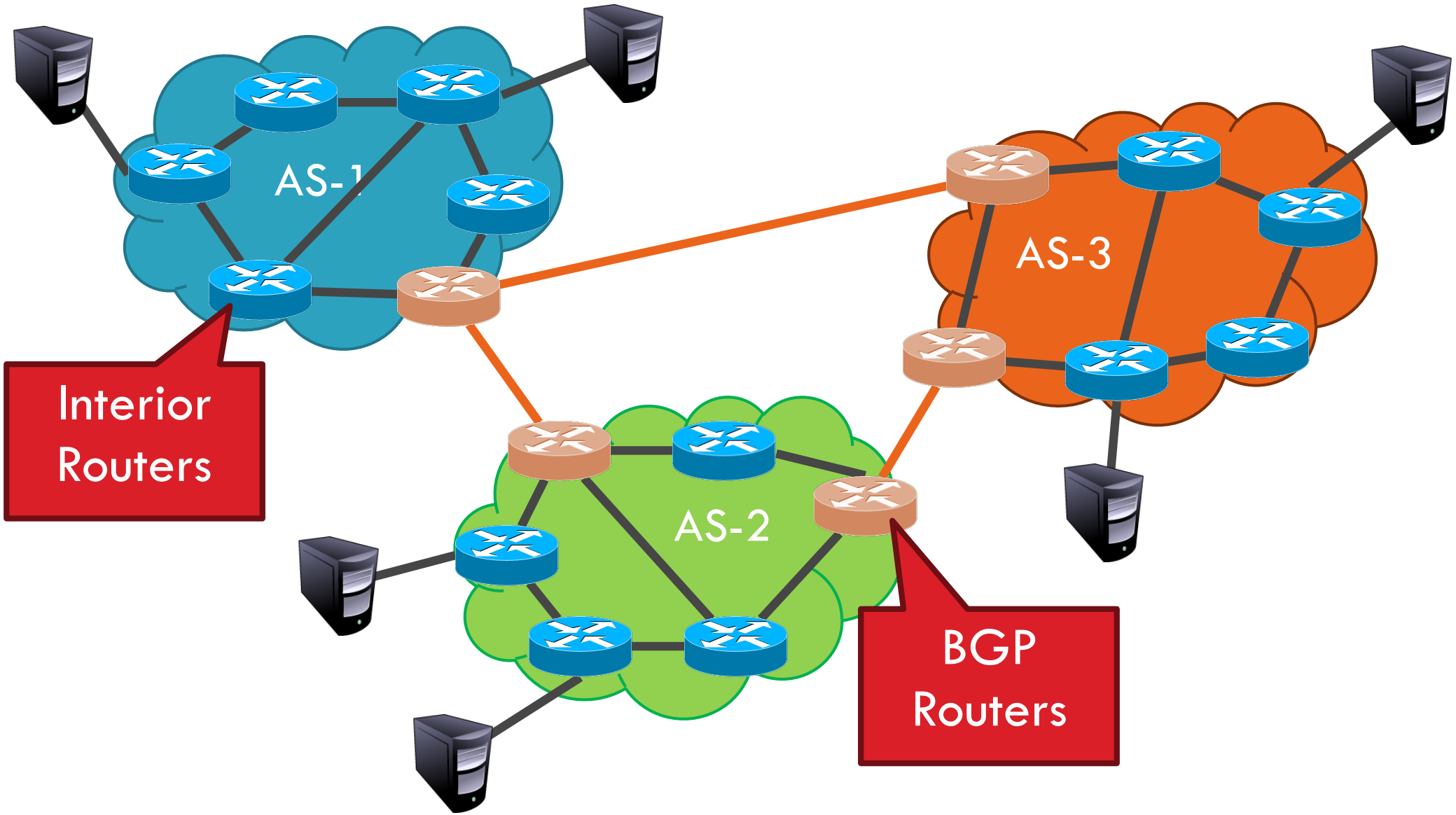


Recap BGP, HTTP, DNS from CSCI-351

Border Gateway Protocol



ASs, Revisited



AS Numbers

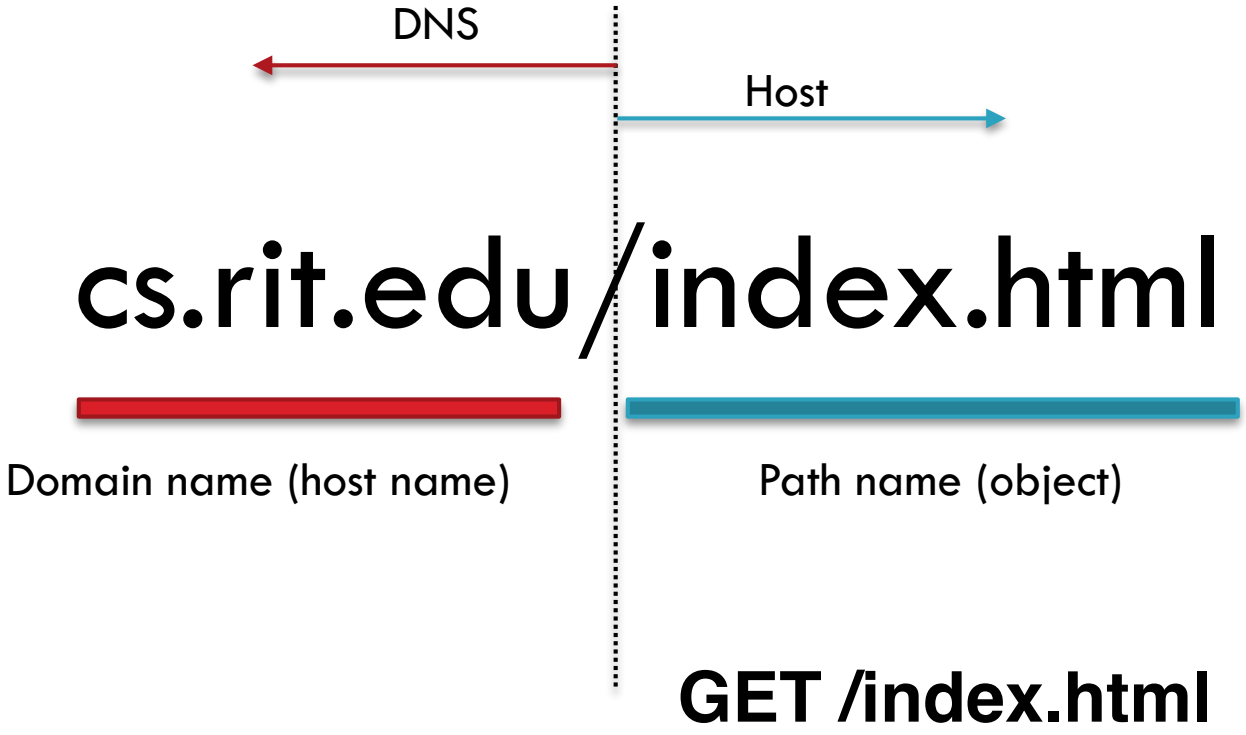
- Each AS identified by an ASN number
  - 16-bit values (latest protocol supports 32-bit ones)
  - 64512 – 65535 are reserved
- Currently, there are > 20000 ASNs
  - AT&T: 5074, 6341, 7018, …
  - Sprint: 1239, 1240, 6211, 6242, …
  - North America ASs → ftp://ftp.arin.net/info/asn.txt

Inter-Domain Routing

- Global connectivity is at stake!
  - Thus, all ASs must use the same protocol
  - Contrast with intra-domain routing
- What are the requirements?
  - Scalability
  - Flexibility in choosing routes
    - Cost
    - Routing around failures

Web and HTTP

- Web pages consist of objects
- Object can be HTML file, JPEG image, Java applet, etc.
- Each object is addressable by a URL



HTTP Basics

- HTTP layered over bidirectional byte stream
- Interaction
  - Client sends **request to server**, followed by **response from server** to client
  - Requests/responses are encoded in text
- Stateless
  - Server maintains no information about past client requests

HTTP Request

GET /foo/bar.html HTTP/1.1

- Request line
  - Method
    - GET – return URI
    - HEAD – return headers only of GET response
    - POST – send data to the server (forms, etc.)
    - …
  - URL (relative)
    - E.g., /index.html
  - HTTP version

HTTP Request

- Request headers (each ended with CRLF)
  - Acceptable document types/encodings
  - Etag - Cache Identifier
    - If-None-Match
  - Referrer – what caused this page to be requested
  - User-Agent – client software
  - Cookie - previously stored information
  - Content-Length - Size of data (only on POST)
- Blank-line (CRLF)
- Body

HTTP Header (www.example.com)

▼ **Request Headers** view source

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,
/;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9,ko;q=0.8

Cache-Control: max-age=0

Connection: keep-alive

Host: example.com

If-Modified-Since: Fri, 09 Aug 2013 23:54:35 GMT

If-None-Match: "1541025663+gzip"

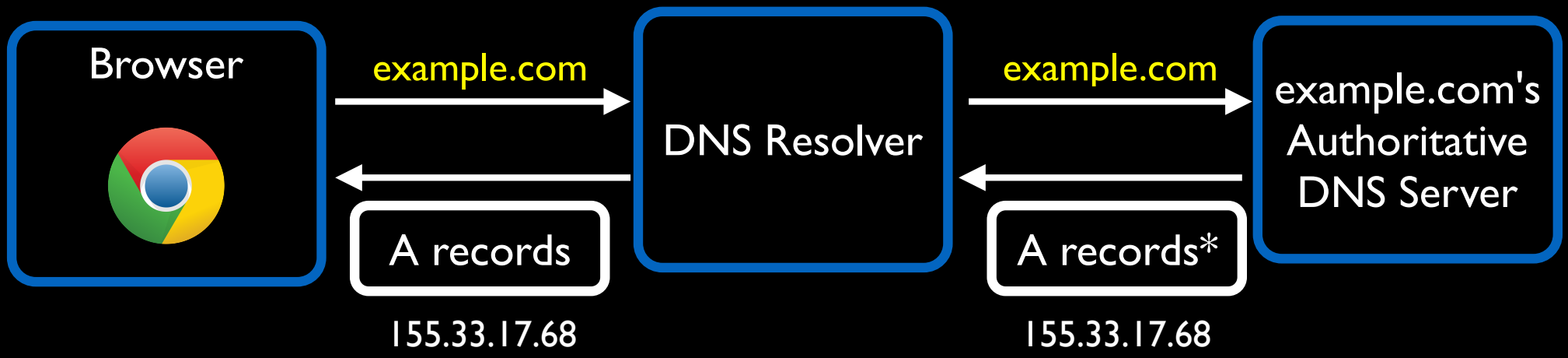
Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTM
L, like Gecko) Chrome/70.0.3538.77 Safari/537.36

HTTP Response

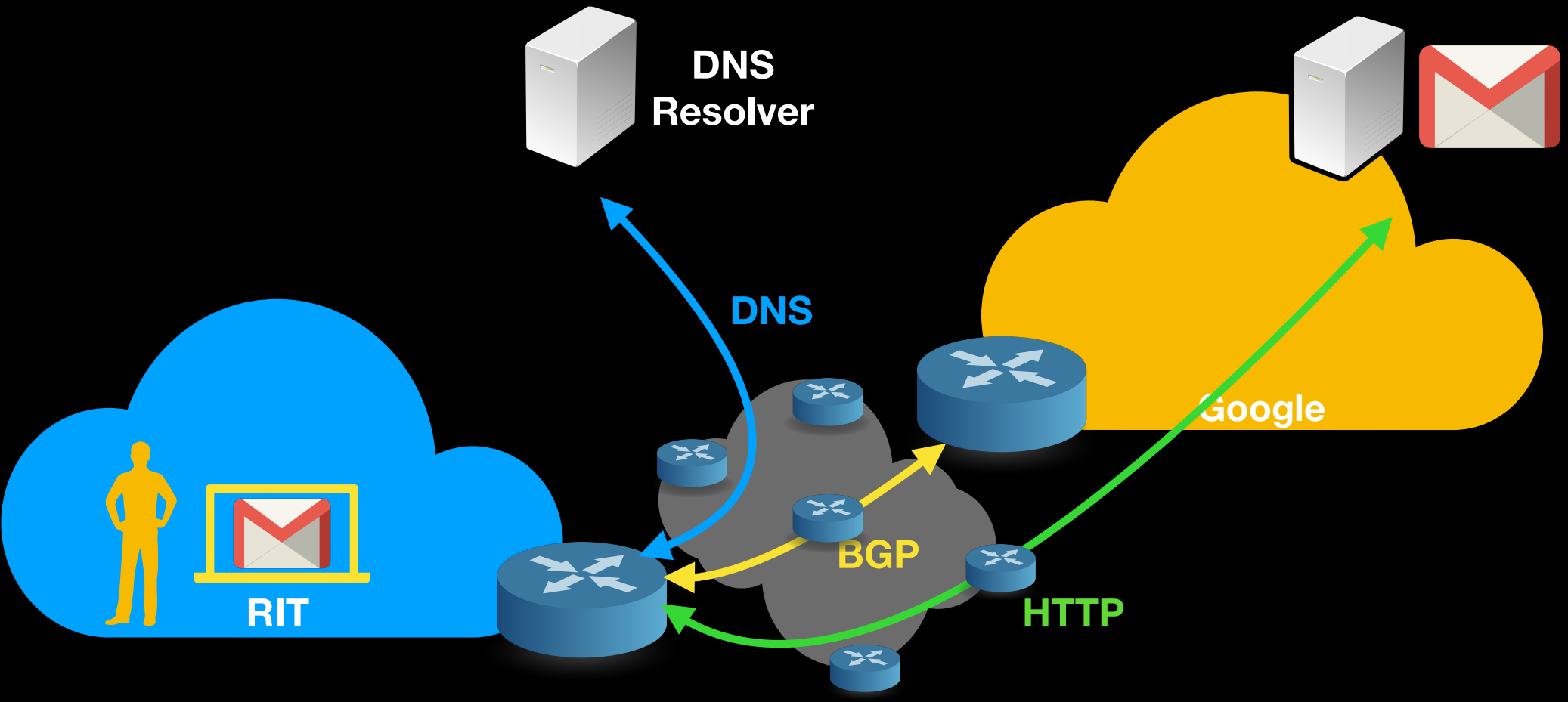
- Status-line
  - HTTP version
  - 3 digit response code
    - 1XX – informational
    - 2XX – success
      - 200 OK
    - 3XX – redirection
      - 301 Moved Permanently
      - 303 Moved Temporarily
      - 304 Not Modified (for etag)
    - 4XX – client error
      - 404 Not Found
    - 5XX – server error
      - 505 HTTP Version Not Supported
  - Reason phrase

Domain Name System (DNS)



*A record: one of the DNS records that contains IP addresses of a domain name

CSCI-351 Data communication and Networking



Security Problems

http://

OpenDNS

Google's Malaysian Domains Hit with DNS Cache Poisoning Attack

PREVIOUS CONTRIBUTORS

OCT 11, 2013 | LATEST SECURITY NEWS

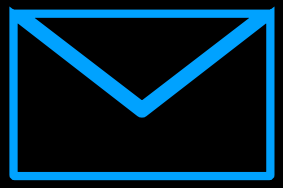
MESSAGE FROM BANK OF AMERICA

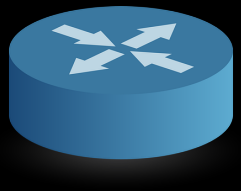
Bank of America <info@boa.com>

to

Be careful with this message. Many people marked

Bank of America
115 W 42nd St, New York, NY 10036, USA
From Desktop of Mr. Jeff Anderson
Our Ref: BOF-0XX2/987/20
E-mail:jeffandersonbnk@gmail.com





ars TECHNICA SUBSCRIPTIONS

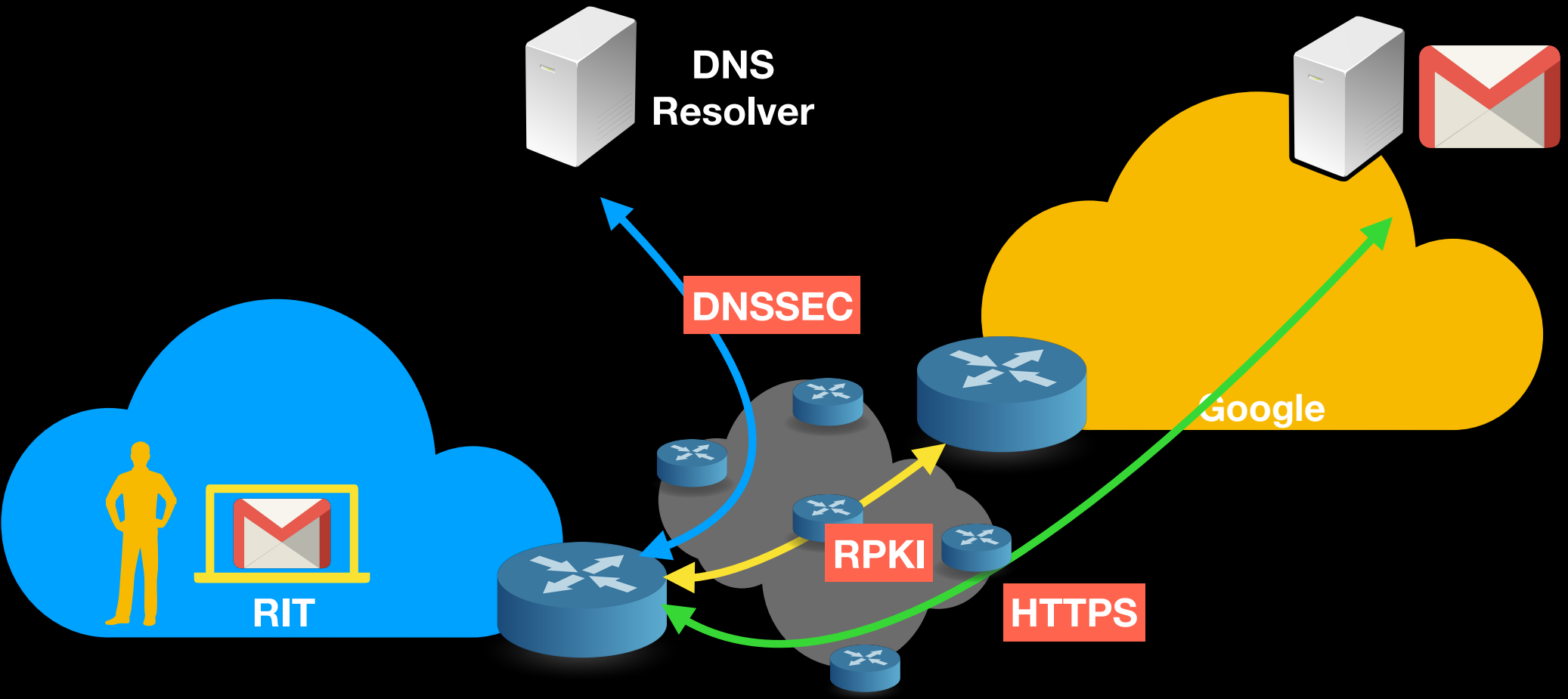
THE POWER OF FALSE ADVERTISING —

How an Indonesian ISP took down the mighty Google for 30 minutes

Internet's web of trust let a company you never heard of block your Gma

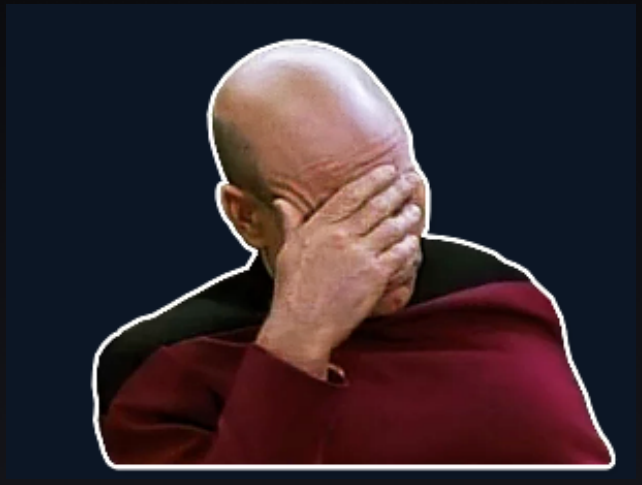
SEAN GALLAGHER - 11/6/2012, 11:07 AM

Security Internet Protocols



All of them use “PKI"

Are we safe now?



TECH | CYBERSECURITY | CRYPTOCURRENCY

Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet

26

By Russell Brandom | @russellbrandom | Apr 24, 2018, 1:40pm EDT

SHARE

MOST READ

Keurig launches a cocktail-making pod machine

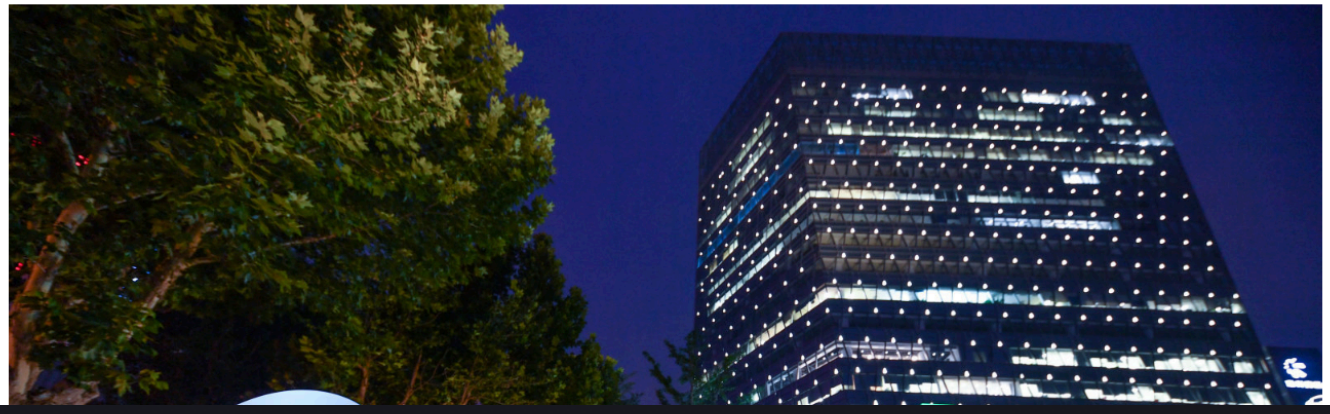
Google went down after traffic was routed through China and Russia

Google said it wasn't malicious, but the timing is odd.

Steve Dent, @stevetdent
11.13.18 in Internet

15
Comments

1759
Shares

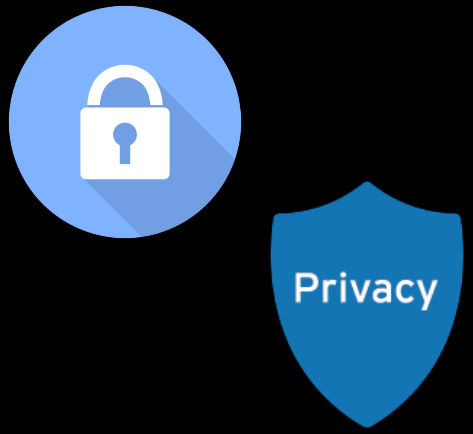


Why are we still in trouble?

- Discrepancies between how they are designed and actually used
  - Economic or technical reasons
- Lots of different versions of protocols and different ways of implementation
- Vulnerabilities are typically found by luck rather than by systematic means.

We need a data-driven approach to security

About this class



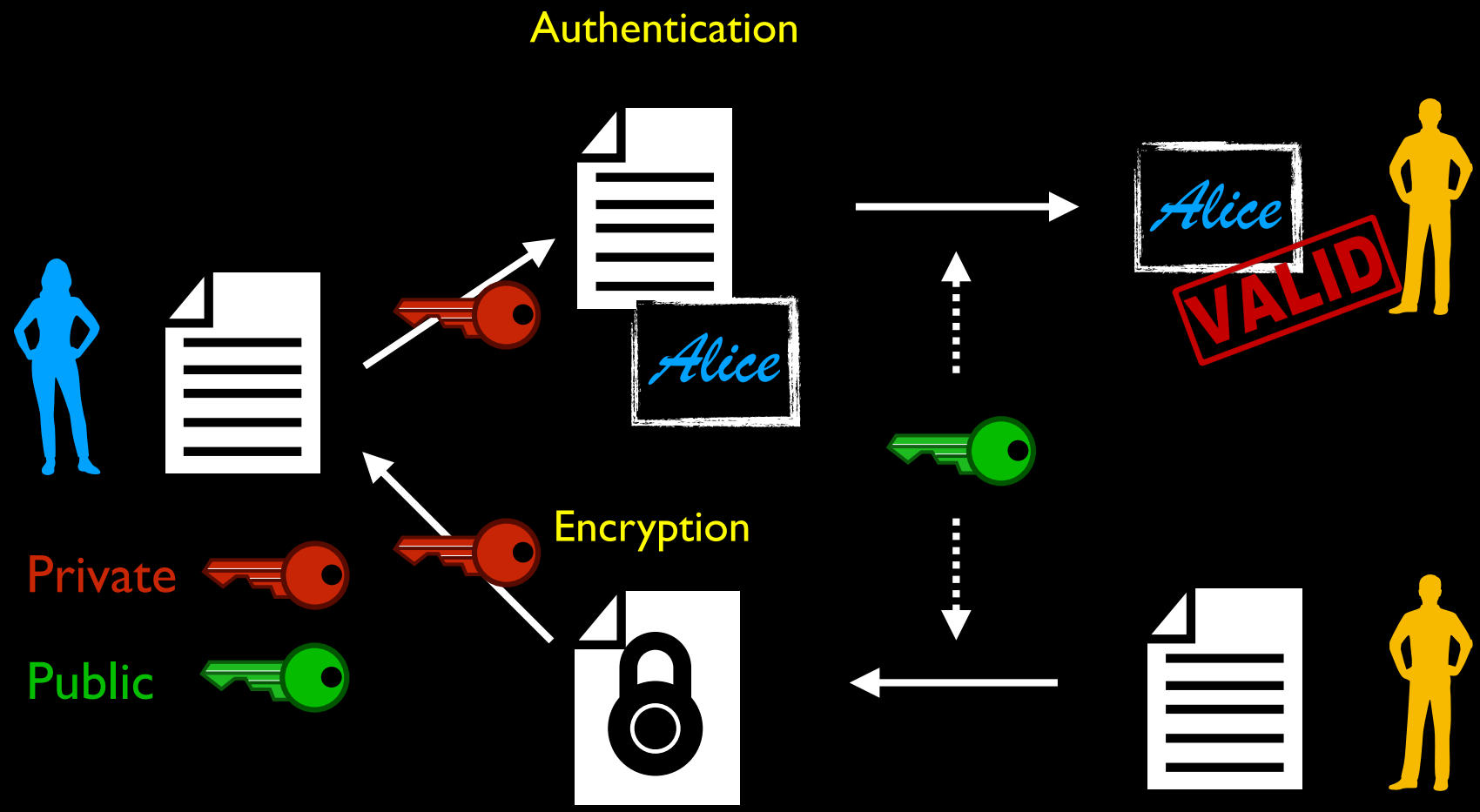
Measurement + **Security & Privacy**

Goal: better understand how secure protocols work, are actually used in practice, and they could be improved

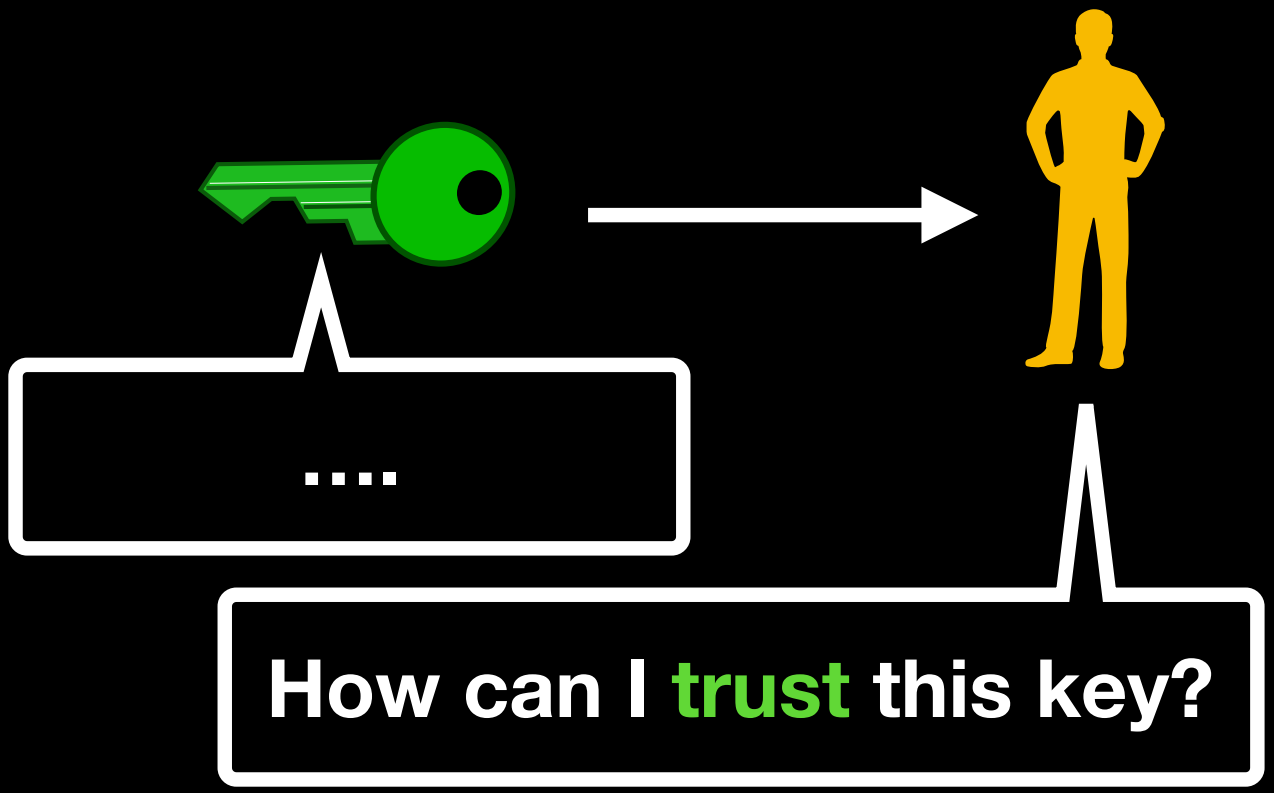
Goals of PKI:
Authentication, Authorization and Encryption

- Authentication
  - verifying the identity of a user or process
- Authorization
  - the action or fact of authorizing or being authorized.
- Encryption

Public Key Cryptography



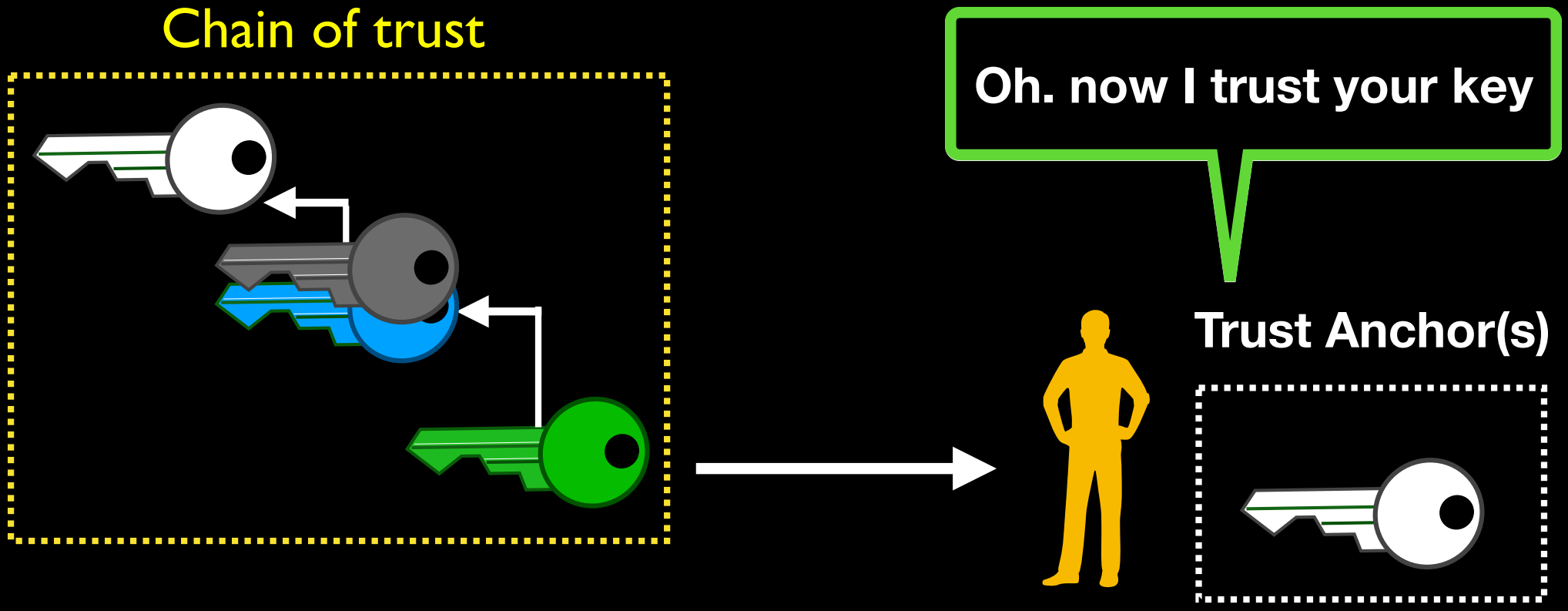
Public Key Infrastructure



PKI

Public Key Infrastructure (PKI) supports
the (1) distribution and (2) identification of public key

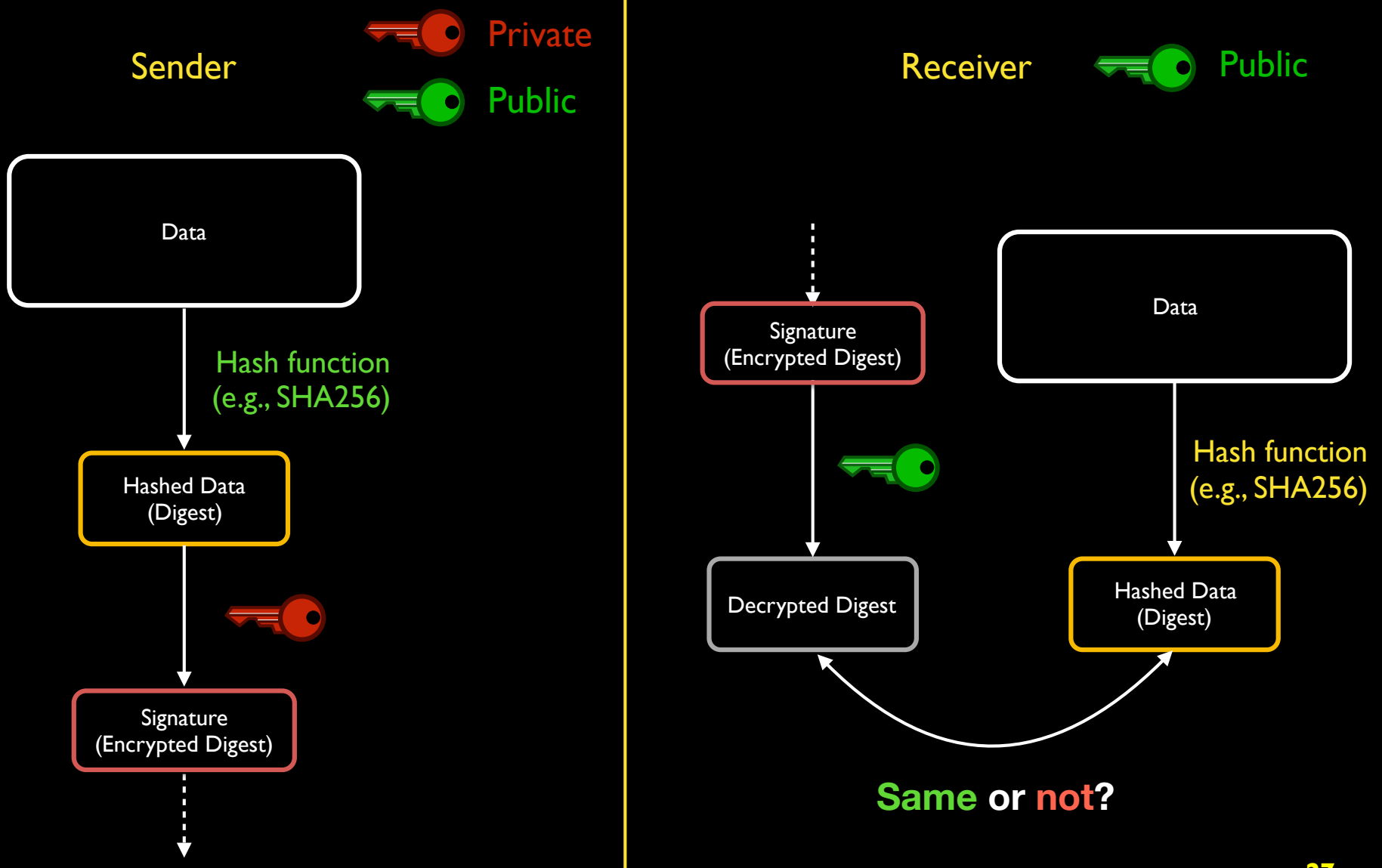
Hierarchical Public Key Infrastructure



Hierarchical PKI

Many secure protocols in the Internet rely on hierarchical PKI

Again,
Signing and verification process



Hash (Digest)

- Originally is used to index the original value or key
- A one-way operation
- Time complexity
  - Obtaining a hash value is O(1)
  - Conjecturing keys from the hash is….
    - In case of sha256,
    - it takes 10**57 minutes (theoretically)