

# CS558 Network Security

## Lecture 10: DNS Attacks and DNSSec

*hello*

# DNS

Domains:

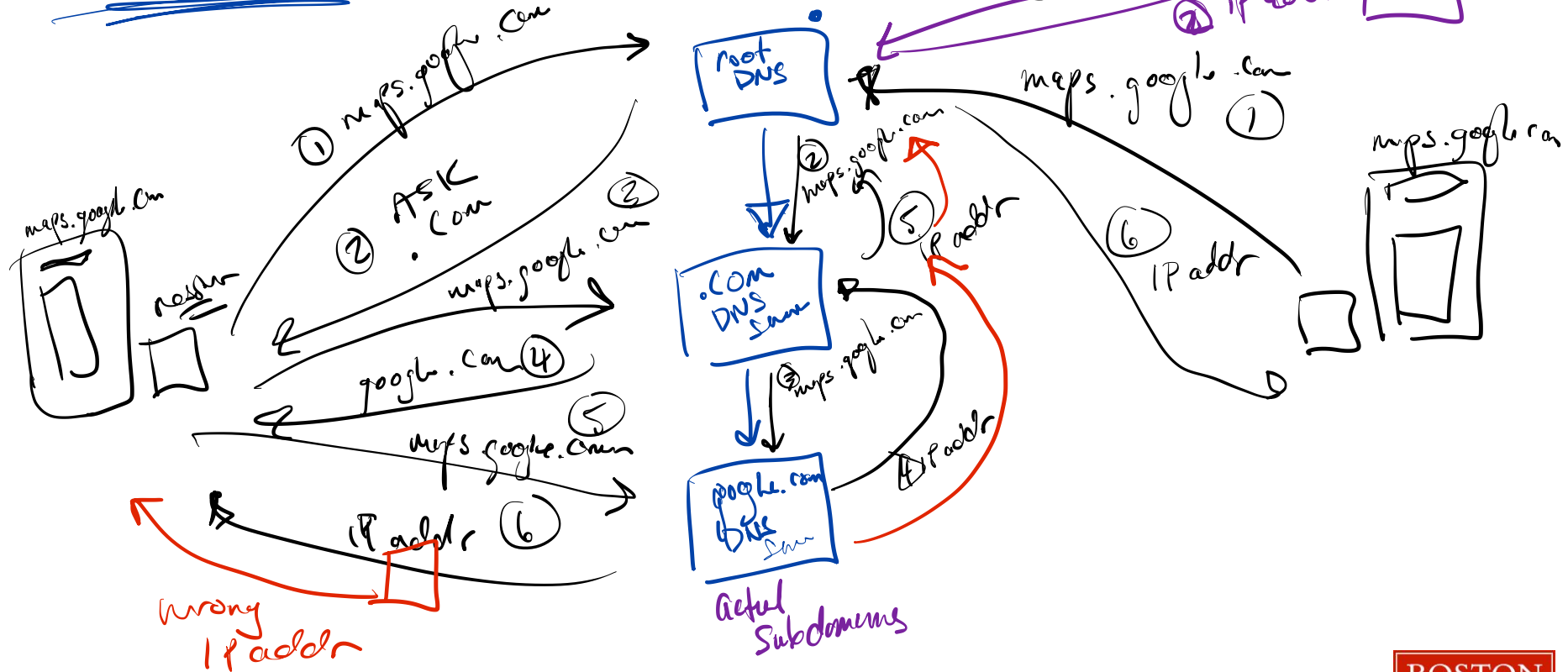
www.bu.edu.

→ TLD  
Top level domain

Domain Name Server

Domain Name ↔ IP address

# DNS Iterative/Recursive Resolving

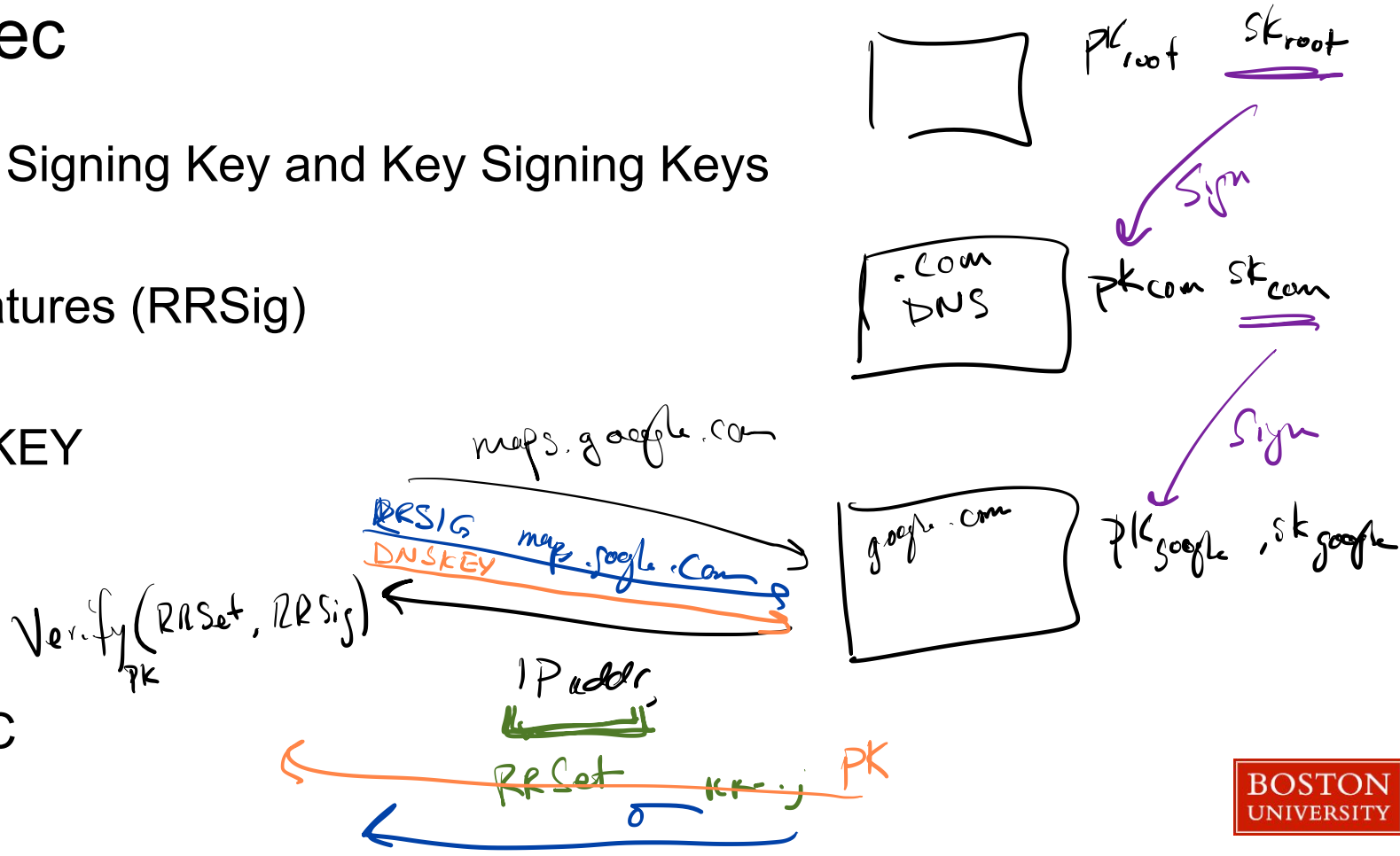


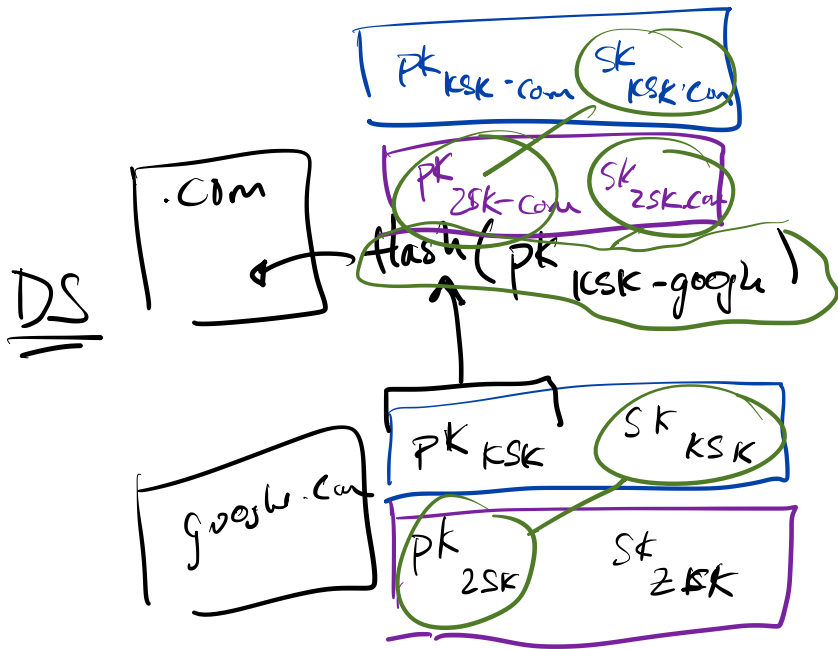
antitoxicity  
confidential



# DNSSEC

- Zone Signing Key and Key Signing Keys
- Signatures (RRSig)
- DNSKEY
- DS
- NSEC





root

DNS  
com

google.com

DS google.com, RRSIG

H

DNSKEY ZSK, KSK, RRSIG

PK<sub>ZSK-com</sub> PK<sub>KSK-com</sub>, σ

DNSKEY KSK  
PK<sub>KSK-google</sub>

maps.google.com

RRSET

RRSIG maps.google.com

σ

DNSKEY ZSK

PK<sub>ZSK-google.com</sub>

RRSIG PK<sub>ZSK-google.com</sub>

Hash(PK<sub>KSK-google</sub>) = H

# Core Internet Protocol Review

ARP → local routing  
no security → malicious routing of traffic in local network

BGP → global routing  
rerouting attack → RPKI → suspect hijack  
→ BGPsec → high effort one hop

DDOS → making "good traffic" useless → ~~policy~~ cloudflare  
→ be a responsible internet citizen

DNS → routing traffic to wrong place → fixed?