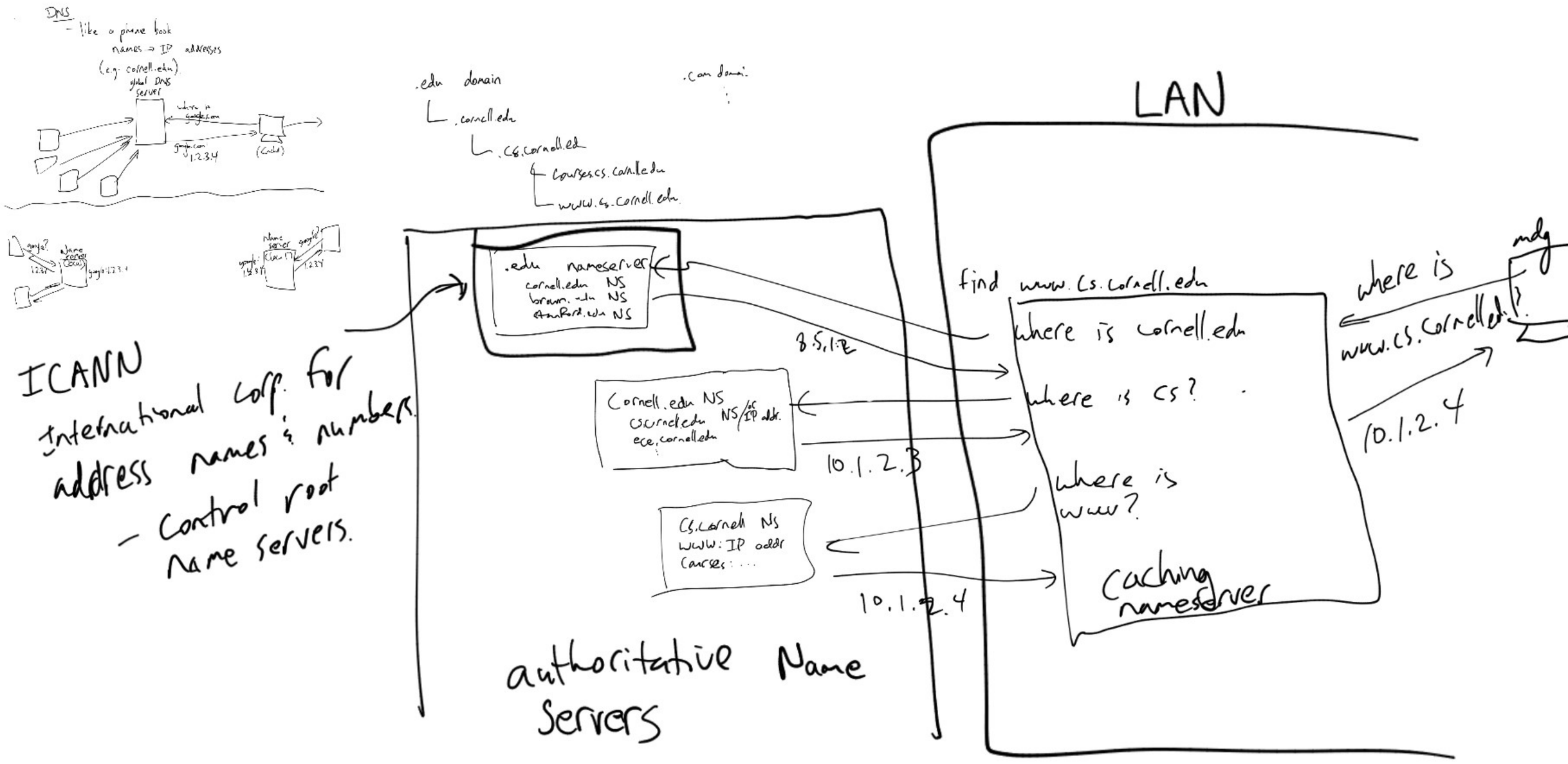
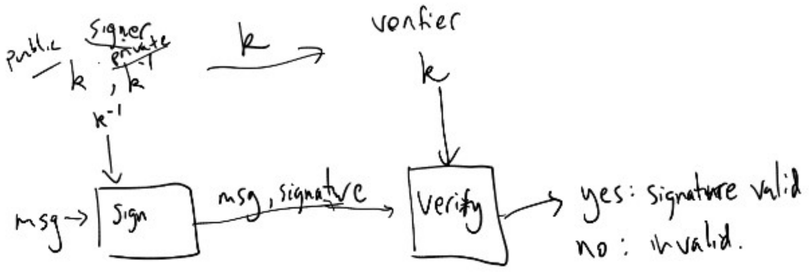
Lec 26: Naming & Encryption

- DNS (domain name service)
- TLS
  - key exchange
  - digital certificates.

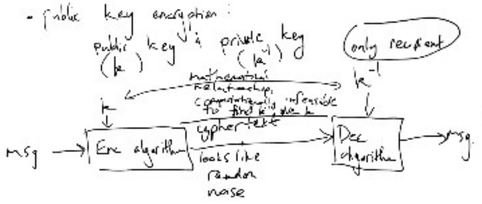

DNS
- like a phone book
names → IP addresses
(e.g. cornell.edu)
global DNS server
(Cache)
1234
.edu domain
.cornell.edu
cs.cornell.edu
courses.cs.cornell.edu
www.cs.cornell.edu
.com domain
LAN
.edu nameserver
cornell.edu NS
brown.edu NS
stanford.edu NS
3.5.1.2
find www.cs.cornell.edu
where is cornell.edu
where is cs?
where is www?
Cornell.edu NS
cs.cornell.edu NS/IP addr.
ece.cornell.edu
10.1.2.3
cs.cornell NS
www: IP addr
courses: ...
10.1.2.4
caching nameserver
where is www.cs.cornell.edu?
10.1.2.4
ICANN
International corp. for address names & numbers.
- Control root name servers.
authoritative Name Servers

Public key signatures



No security (at any layer)

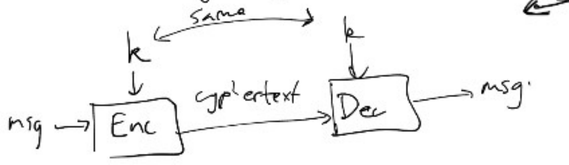
- public key encryption:



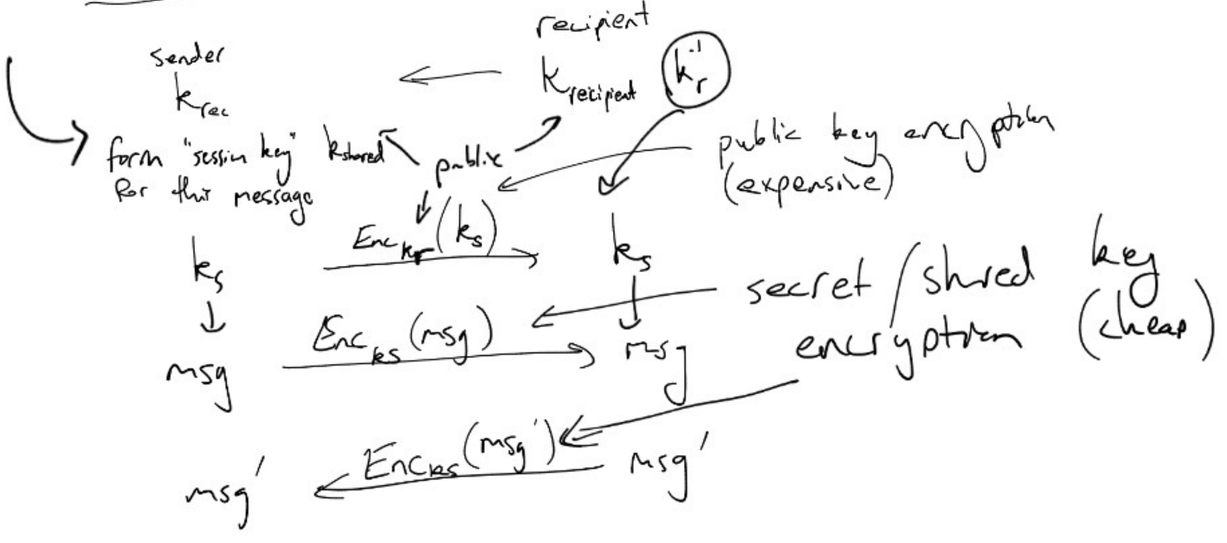
recipient forms private/public keys, tells everyone public key. never tells anyone priv. key

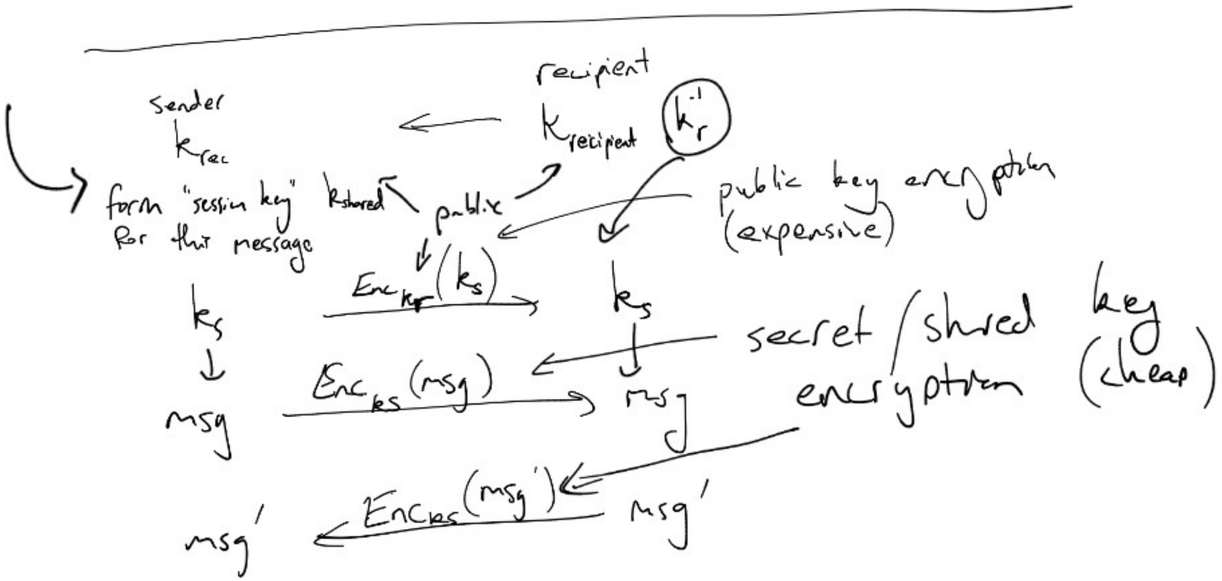
← Comp. expensive

- secret key encryption
  shared key encryption



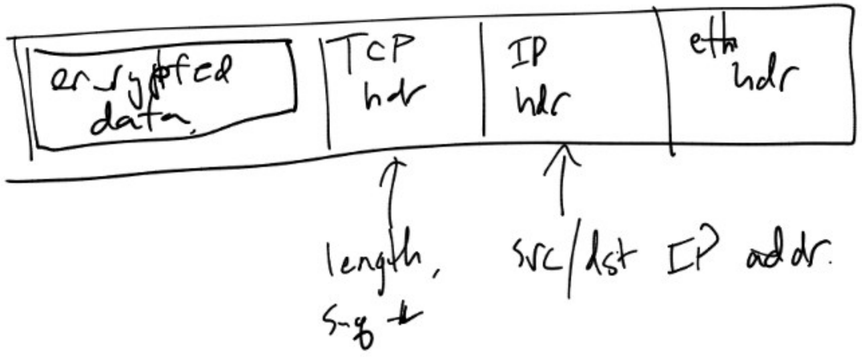
← Computationally cheap

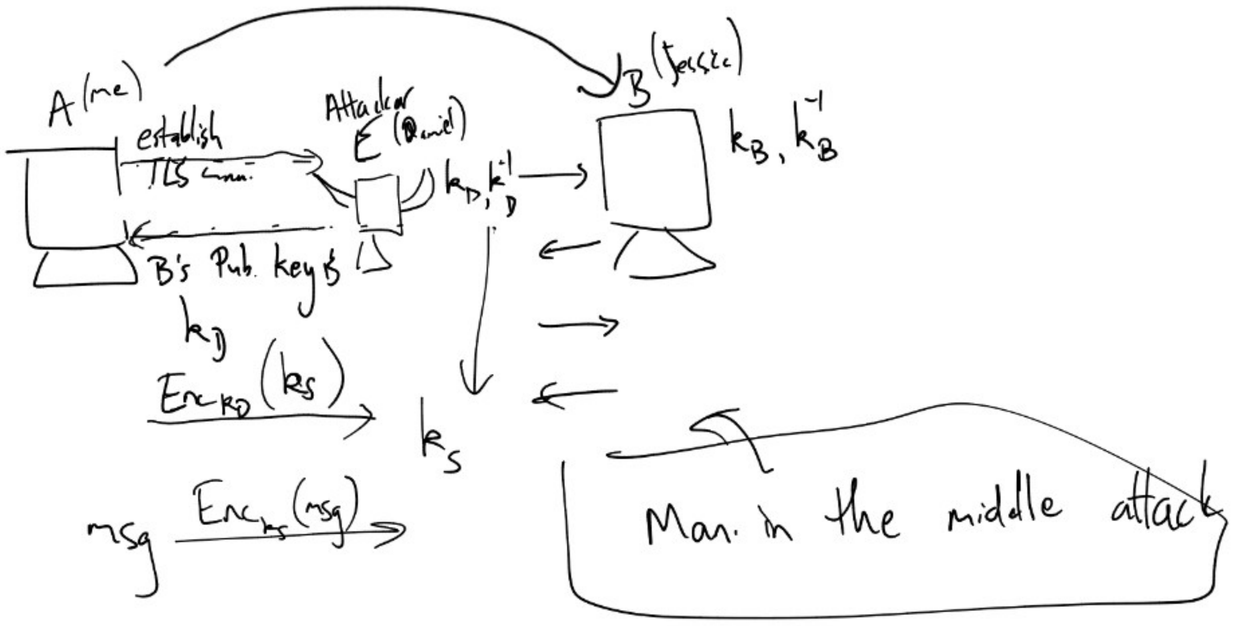




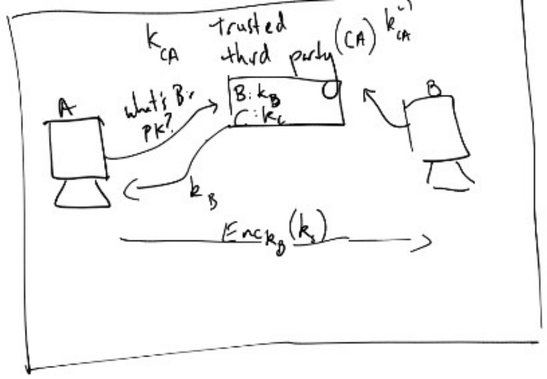
TLS: transport layer security

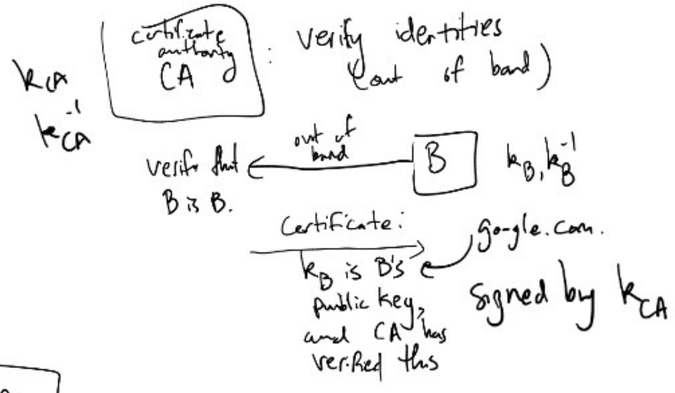
- establish a TCP connection
- use connection to establish shared key k_s
- use k_s to encrypt further traffic.





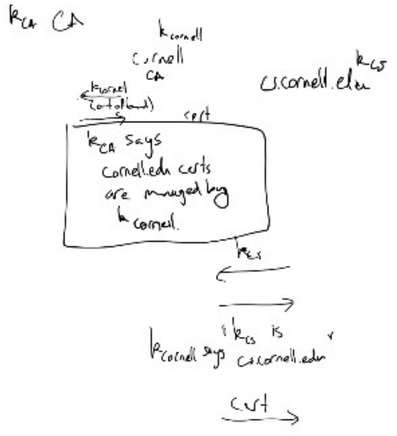
to prevent: some kind of "out of band" communication = very expensive.



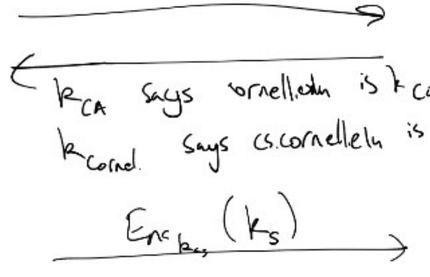


k_{CA} can grant authority to other CA's for subdomains

e.g. Cornell CA, responsible for cornell.edu keys.



A



VPN (virtual private network)