Chapter 8 roadmap

8.1 What is network security?
8.2 Principles of cryptography
8.3 Authentication
8.4 Integrity
8.5 Key distribution and certification

42

Trusted Intermediaries

Symmetric key problem:

- How do two entities establish shared secret key over network?

Solution:

- trusted key distribution center (KDC) acting as intermediary between entities

Public key problem:

- When Alice obtains Bob's public key (from web site, e-mail, diskette), how does she know it is Bob's public key, not Trudy's?

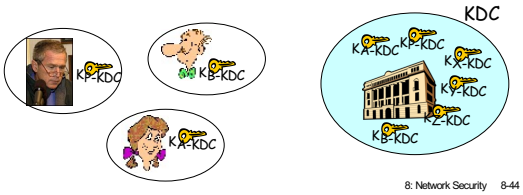
Solution:

- trusted certification authority (CA)

43

Key Distribution Center (KDC)

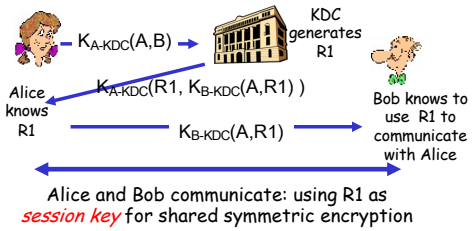
- Alice, Bob need shared symmetric key.
- KDC: server shares different secret key with *each* registered user (many users)
- Alice, Bob know own symmetric keys, $K_{A\text{-}KDC}$ $K_{B\text{-}KDC}$, for communicating with KDC.



44

Key Distribution Center (KDC)

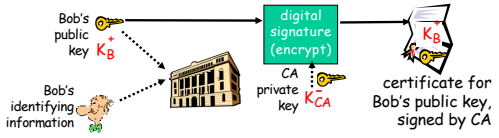
Q: How does KDC allow Bob, Alice to determine shared symmetric secret key to communicate with each other?



45

Certification Authorities

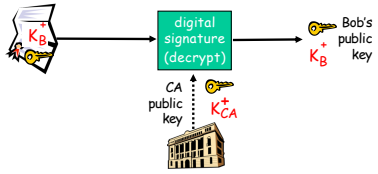
- Certification authority (CA): binds public key to particular entity, E.
- E (person, router) registers its public key with CA.
  - E provides "proof of identity" to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E's public key digitally signed by CA – CA says "this is E's public key"



46

Certification Authorities

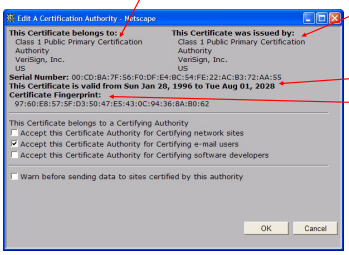
- When Alice wants Bob's public key:
  - gets Bob's certificate (Bob or elsewhere).
  - apply CA's public key to Bob's certificate, get Bob's public key



47

A certificate contains:

- Serial number (unique to issuer)
- info about certificate owner, including algorithm and key value itself (not shown)



- info about certificate issuer
- valid dates
- digital signature by issuer

48

Network Security (summary)

Basic techniques……

- cryptography (symmetric and public)
- authentication
- message integrity
- key distribution

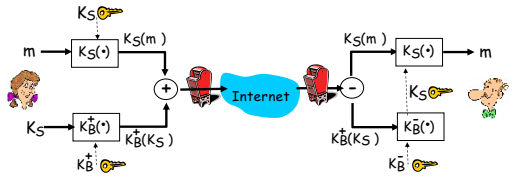
…. used in many different security scenarios

- secure email
- secure transport (SSL/TLS)
- HTTPS
- Etc.

49

Secure e-mail

- Alice wants to send confidential e-mail, m, to Bob.



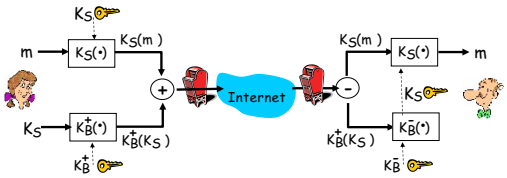
Alice:

- generates random *symmetric* private key, K_S.
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key.
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob.

50

Secure e-mail

- Alice wants to send confidential e-mail, m, to Bob.



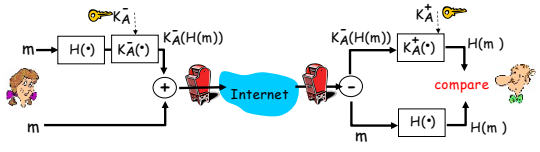
Bob:

- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m

51

Secure e-mail (continued)

• Alice wants to provide sender authentication message integrity.

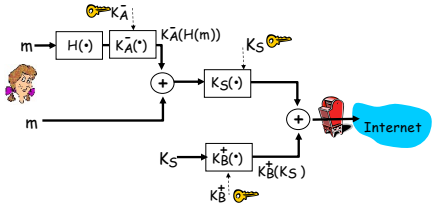


- Alice digitally signs message.
- sends both message (in the clear) and digital signature.

52

Secure e-mail (continued)

• Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key, Bob's public key, newly created symmetric key

53

Secure sockets layer (SSL)

- transport layer security to any TCP-based app using SSL services.
- used between Web browsers, servers for e-commerce (shttp).
- security services:
  - server authentication
  - data encryption
  - client authentication (optional)
- server authentication:
  - SSL-enabled browser includes public keys for trusted CAs.
  - Browser requests server certificate, issued by trusted CA.
  - Browser uses CA's public key to extract server's public key from certificate.
- check your browser's security menu to see its trusted CAs.

54

SSL (continued)

Encrypted SSL session:

- Browser generates *symmetric session key*, encrypts it with server's public key, sends encrypted key to server.
- Using private key, server decrypts session key.
- Browser, server know session key
  - All data sent into TCP socket (by client or server) encrypted with session key.
- SSL: basis of IETF Transport Layer Security (TLS).
- SSL can be used for non-Web applications, e.g., IMAP.
- Client authentication can be done with client certificates.

55

End of Security!!!
Questions

56

Last Class

1/ Final Exam info
2/ Course recap
3/ Follow-on courses
4/ Broad questions from students
5/ Feedback forms.

Final Exam Info

1/ Dec 17, 1:30 pm, In-person for on-campus students
   - → Location: 141, 151 Loomis Lab.
   - → UG → Go to 141
   - → Grad → Go to 151

2/ Dec 17, 8pm, Remote students
   - → Zoom link TBA on website
   - → Conflict also in this slot

3/ Syllabus
   - → Comprehensive
   - → More emphasis post midterm but TCP still important.

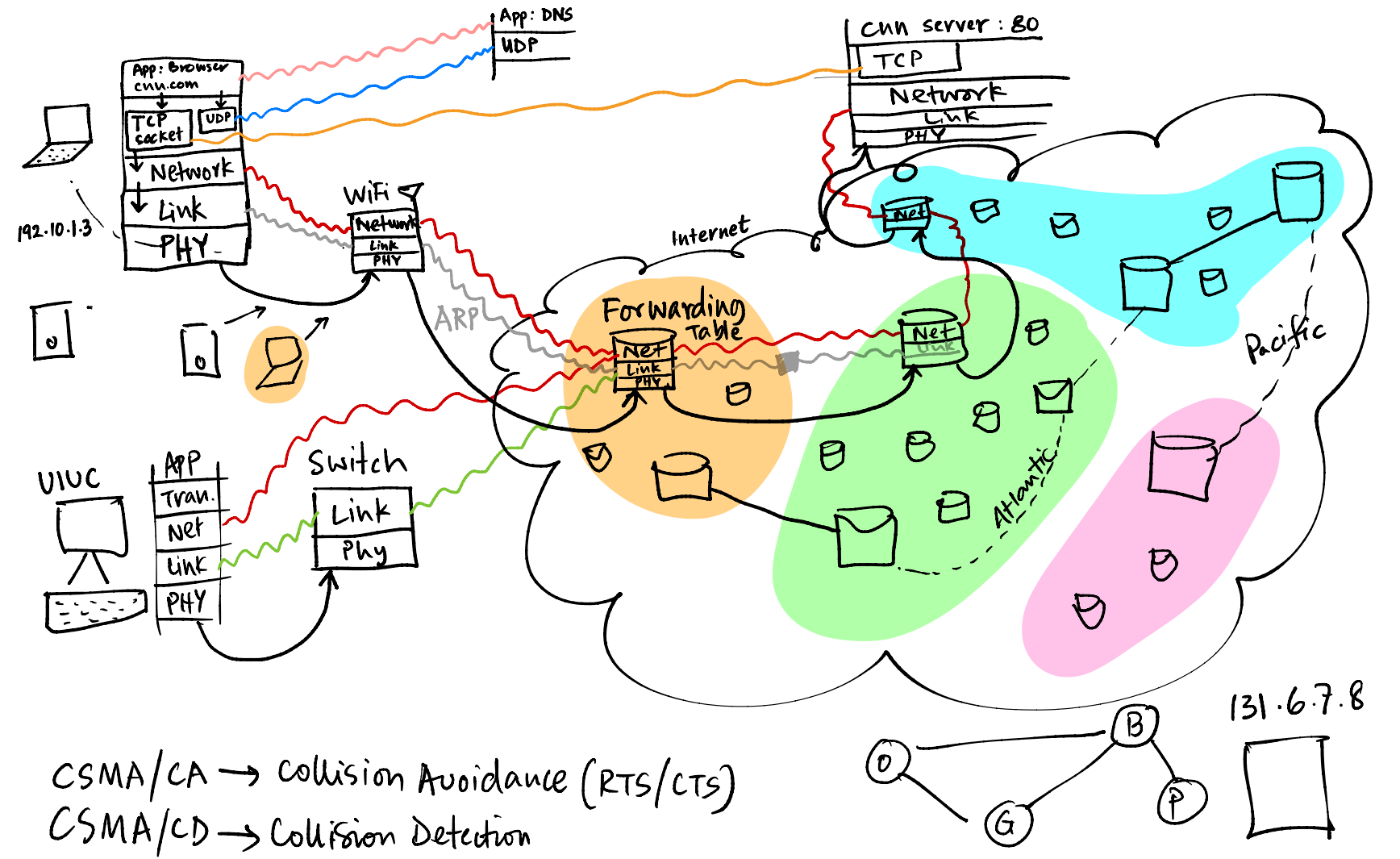
4/ 1 page cheat sheet → 2 sides

5/ Format → similar to HW #4, midterm

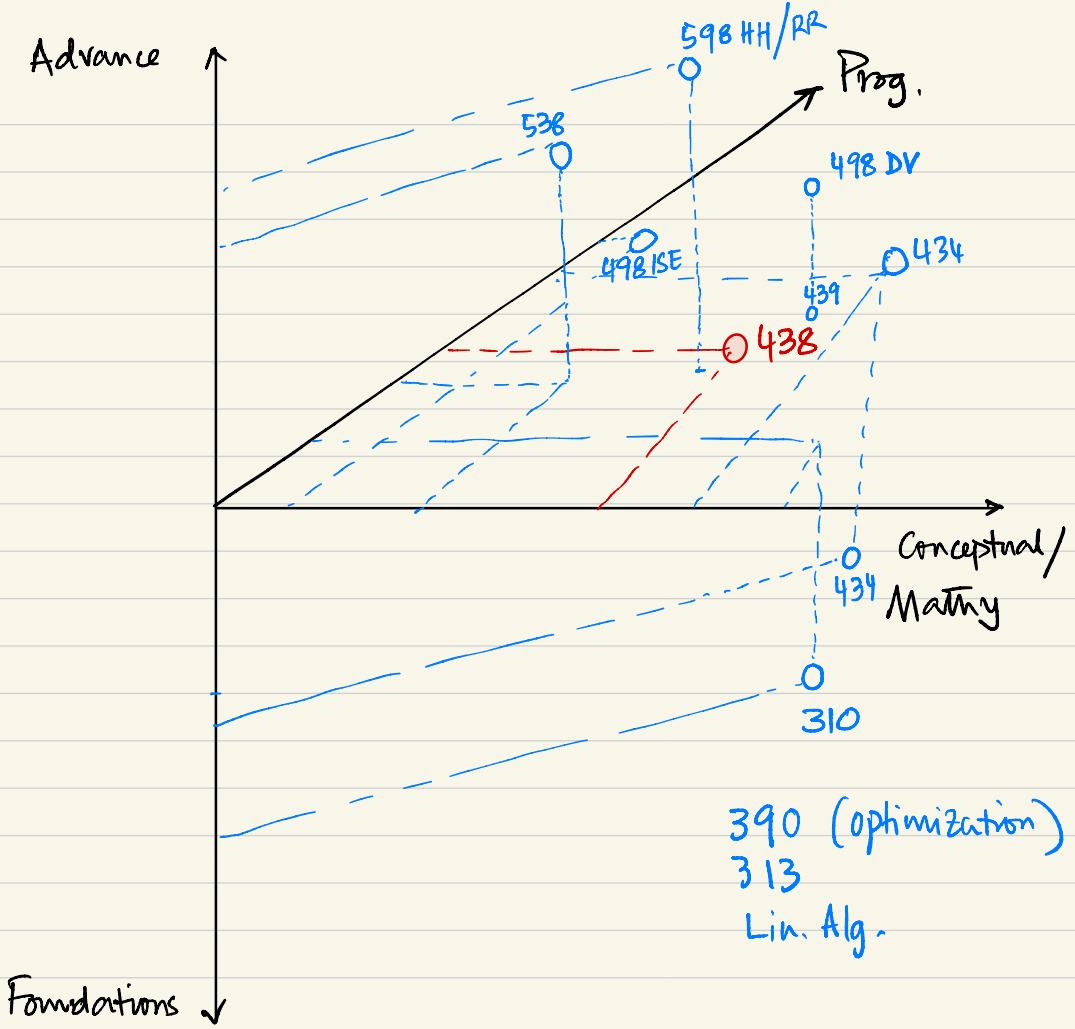
6/ Exam ~ 2hr long but you have 3 hrs.

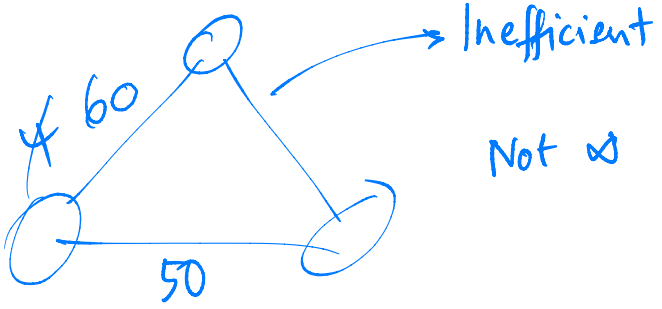
7/ Another email will go out with comprehensive information.

8/ No cellular network in syllabus.


App: DNS
UDP
cnn server : 80
TCP
Network
Link
PHY
App: Browser
cnn.com
TCP socket
UDP
Network
Link
PHY
192.10.1.3
WiFi
Network
Link
PHY
ARP
Internet
Forwarding Table
Net
Link
PHY
Net
Link
Pacific
Atlantic
UIUC
App
Tran.
Net
Link
PHY
Switch
Link
Phy
CSMA/CA → Collision Avoidance (RTS/CTS)
CSMA/CD → Collision Detection
B
O
G
P
131.6.7.8

Next Courses





Inefficient

Not ∝