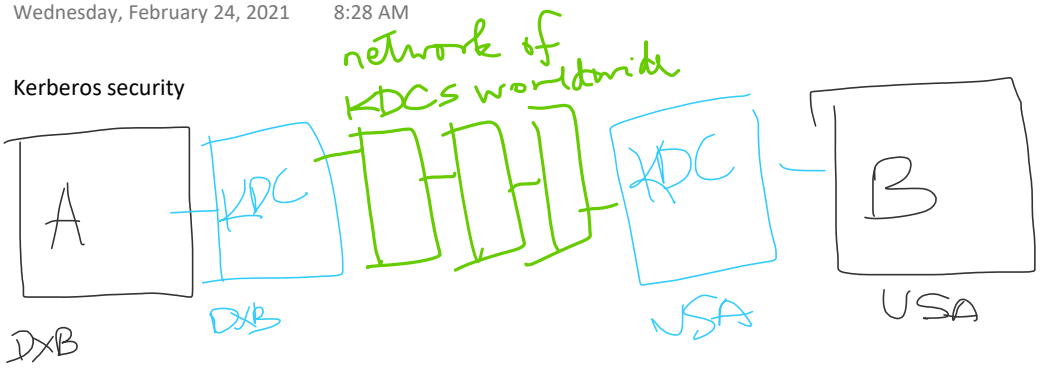
4. Kerberos + SSL

Wednesday, February 24, 2021 8:28 AM

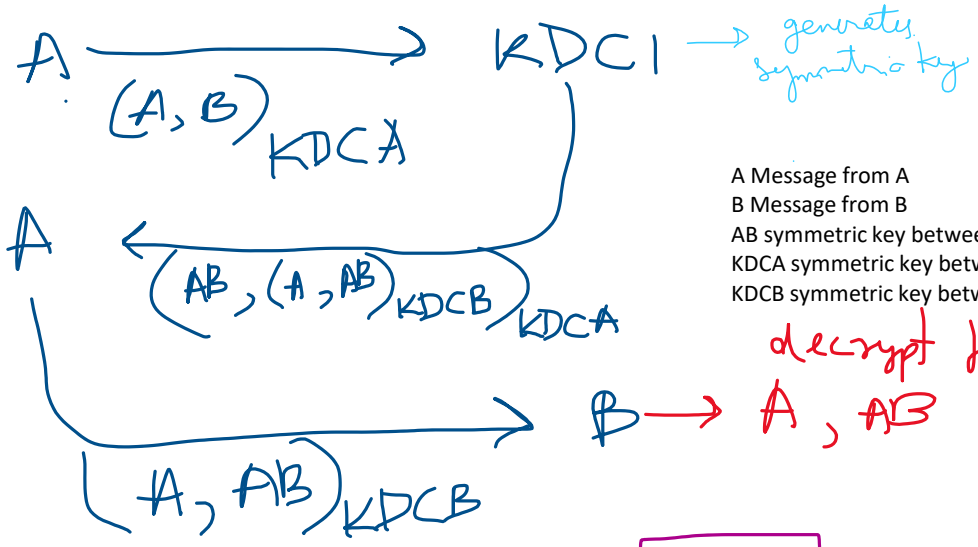
Kerberos security



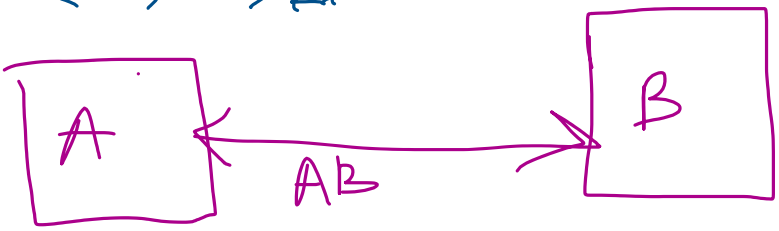
A and b want to communicate using symmetric key cryptography using KDC
A proves herself to KDC Dubai using credentials
KDC dub provides her with a symmetric key only between A and KDCDubai

B also does the same and gets a symmetric key between him and the local KDC

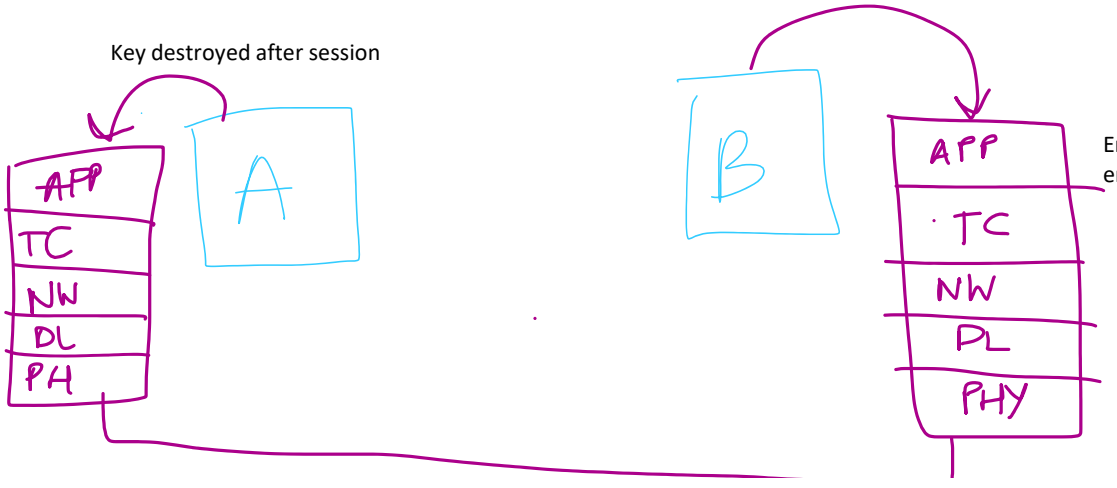
All KDCs have access to their client's keys (via a secure impenetrable network)



A Message from A
B Message from B
AB symmetric key between A and B
KDCA symmetric key between KDC and A
KDCB symmetric key between KDC and B



Key destroyed after session

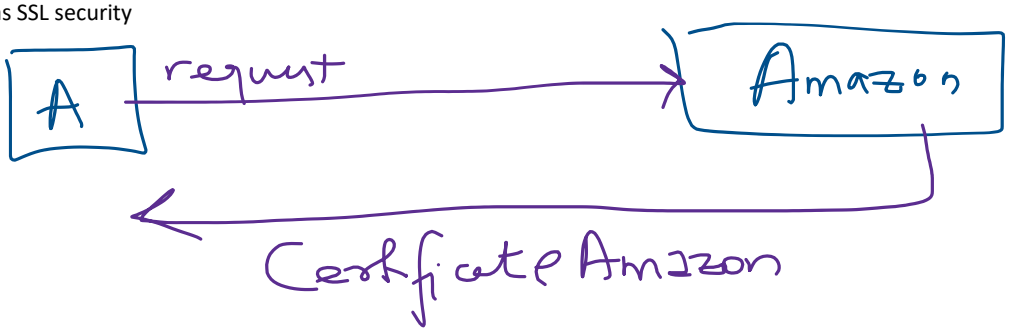


Email, browser, Java applications used for encryption

Applications that I develop should not have to handle confidentiality and integrity issues
Transport or IP layer can encrypt and decrypt data
Application layer becomes minimal
Security at many layers (application, transport, network, data link)

SSL Security
Secure socket layer
At transport layer

HTTPS has SSL security



1. A will verify integrity of the certificate and confirm it is from Amazon
2. A will extract public key from Amazon
3. A Generates random symmetric key
4. A Encrypts it with public key of Amazon
5. Amazon sends HTTPS response and HTML page encrypted with shared symmetric key

Similar to hybrid cryptography
Only server has to prove identity, not the client