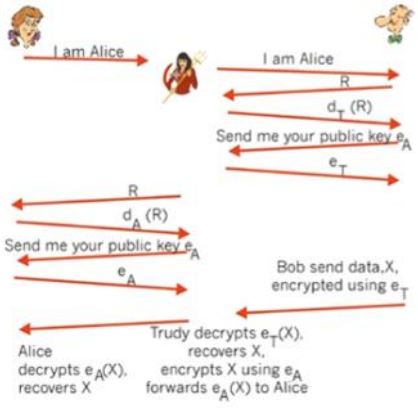
4. Web Service Security

Monday, February 22, 2021 2:53 PM

Man-in-the-middle attack



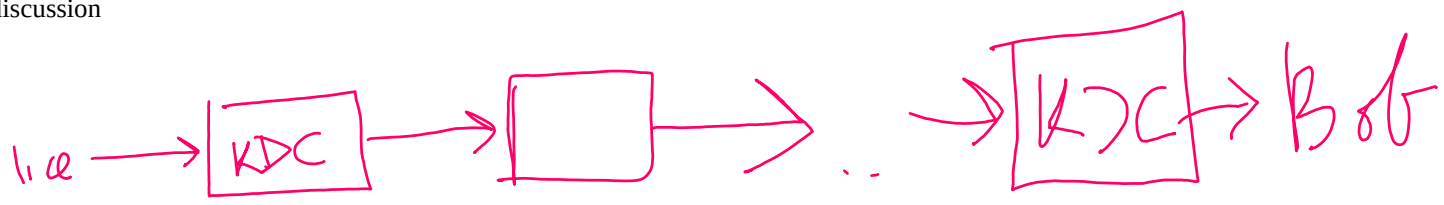
Falsely authenticated intruder
Before the advent of certificate authority, man-in-the-middle loophole in the asymmetric key cryptography authentication

Web service authentication (between client and web service) with

- SAML - security assertion markup language
- Password digest
- Certificates

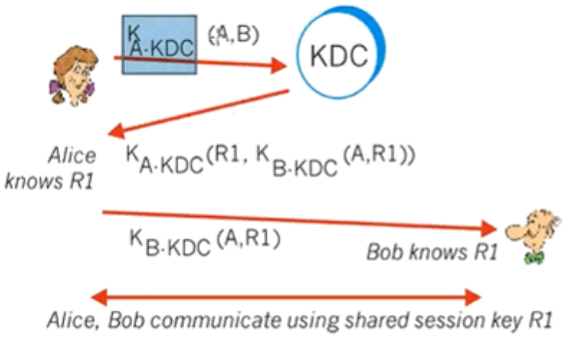
Kerberos authentication protocol:
Suppose Alice and Bob wish to communicate using symmetric key cryptography. Certificate authority is the central provider for asymmetric key cryptography.

KDC: key distribution center provides symmetric key in a certified manner.
KDC communication is beyond scope of discussion



- Setting up one-time session key using a Key Distribution Center

Alice and Bob communicate with their respective KDCs
KDCs exchange symmetric key of all clients with each other



1. KDC decrypts message from Alice to find out the receiver is Bob
2. Generates a symmetric key R1 encrypted using K(AKDC)