

CAS - Central Authentication Server (does authentication)

- 1) Kerberos
- 2) RADIUS
- 3) TACACS+
- 4) LDAP / Active Directory (AD)
- 5) PKI (digital certificates)
 - * certificate authority that manages certificates
 - * asymmetric

Digital certificates uses Public Private Key

HASH (H) is integrity, MD5, SHA, NOT reversible

Symmetric, uses encryption SINGLE Key

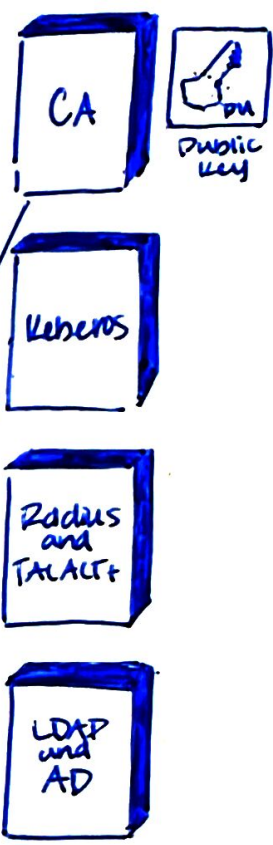
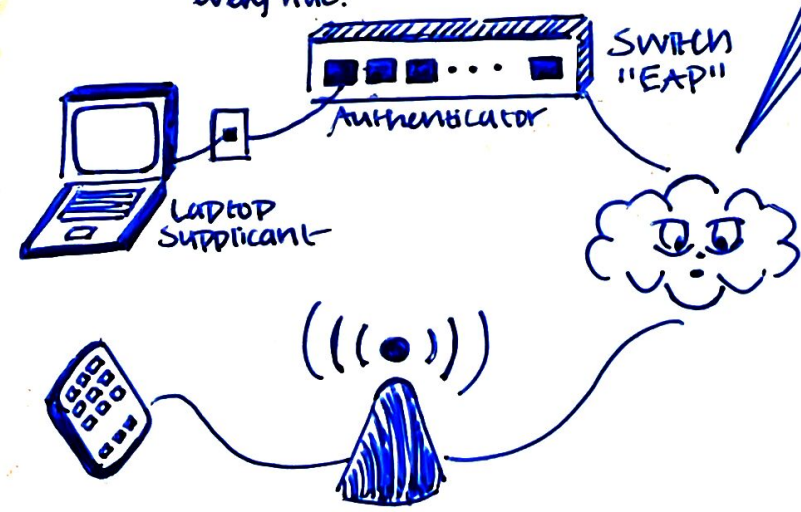
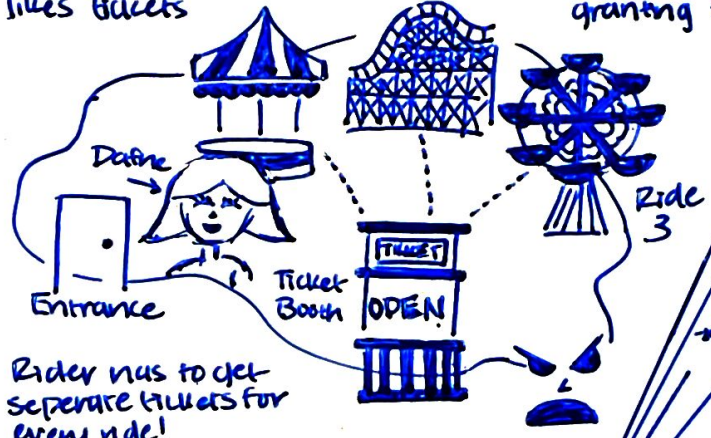
RC4, AES, DES, 3DES

Asymmetric, uses encryption Public AND Private Key

D-H, RSA, ECC

Kerberos (authentication)

- * client must be verified through trusted server
- * 3rd party
- * uses Private Key encryption
- * uses Symmetric Key encryption
- * Kerberos likes tickets
- * tickets
 - TGT (Ticket granting ticket)



* EAP = Extended Authentication Protocol

* NAC = Network Access Control "Quarantine"