1. Following info from the previous lecture.   
   RSA is a cryptosystem allowing us to perform different actions based on asymmetric keys (Public, Private Keys).  
   Most popular length is 2048bits.
2. What is PKI?
3. PKI: Public Key Infrastructure.
4. PKI is set of different protocols, algorithms, entities, certificates allowing us to perform communication based on certificates (trusts).  
   Using these trusts (certificates), we can perform encryption of data and server authentication.
5. There are many different elements in PKI infrastructure.
6. Like **Certificate Authority**: To sign certificate or delegate the trust to entities such as Intermediate CA.
7. Intermediate CA’s main responsibility to sign certificates from other entities such as Web Site etc.
8. We can use certificates for
   1. SSL/TLS Encryption.
   2. To secure website.
   3. To build VPN to send data over VPN Tunnel securely.
9. What is certificate?
10. A set of data.  
    Owned by a company (Google, Facebook etc).  
    Used for HTTPS Protocol.  
    Most important info contained by certificate is the Public Key of the owner of the Certificate.  
    This means every entity in the PKI has its own public key and this public key is always included in the certificate of that entity.