ITS335 – Web Security Notes

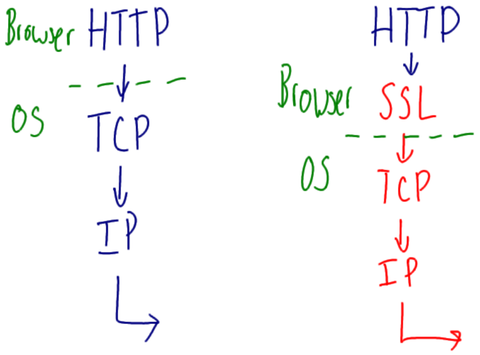


Figure 1: HTTP vs HTTPS; Lecture 20

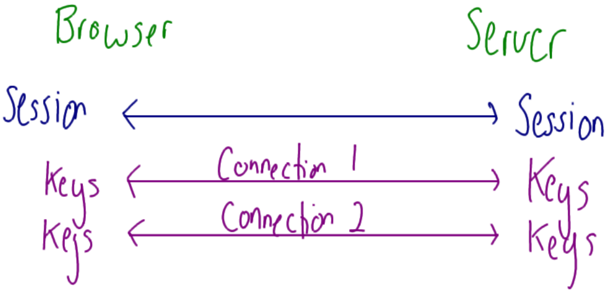


Figure 2: SSL Session and Connection; Lecture 20

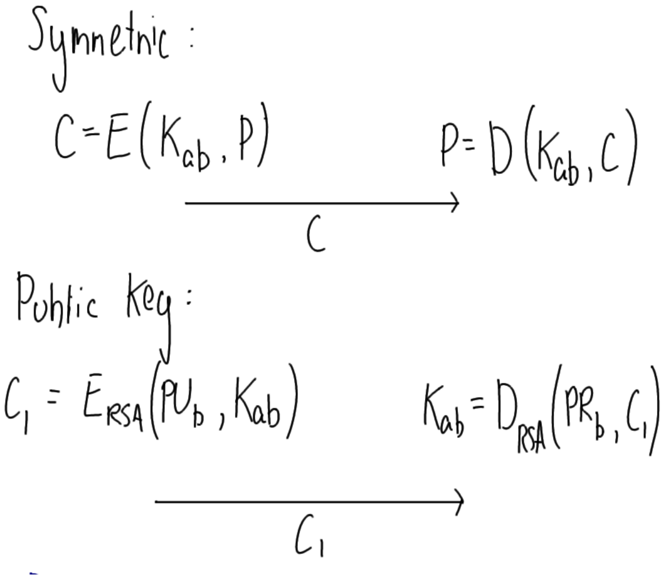


Figure 3: Exchange Symmetric Key using Public Key Crypto; Lecture 20

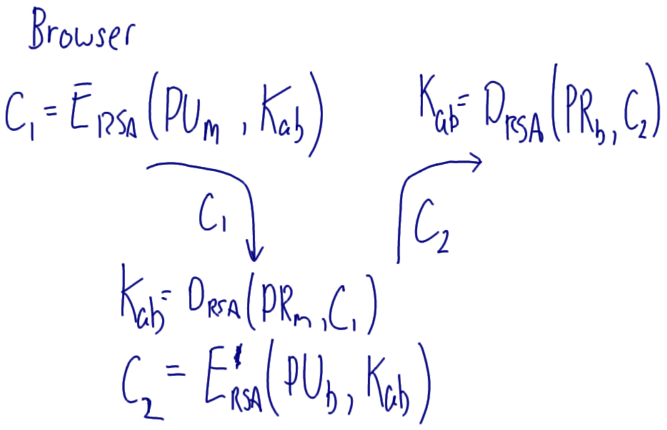


Figure 4: Man-in-the-Middle Attack on Public Key Exchange; Lecture 20

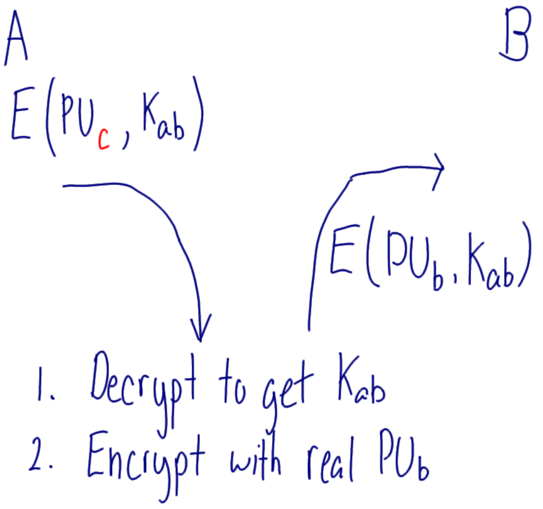


Figure 5: Man-in-the-Middle Attack on Public Key Exchange (2); Lecture 21

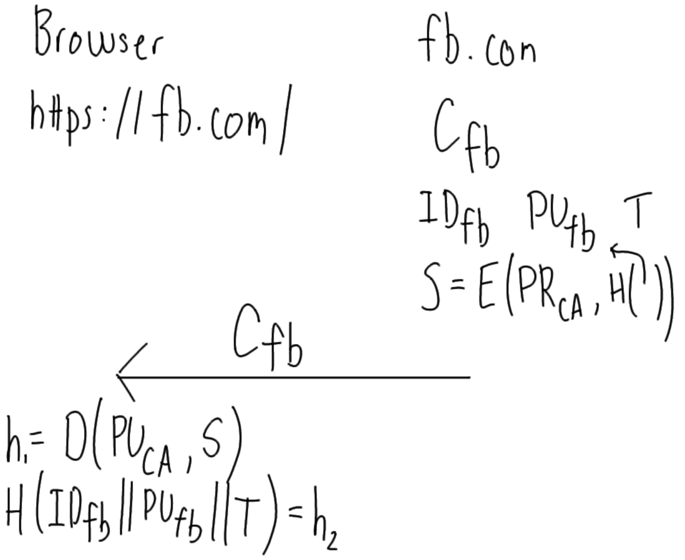
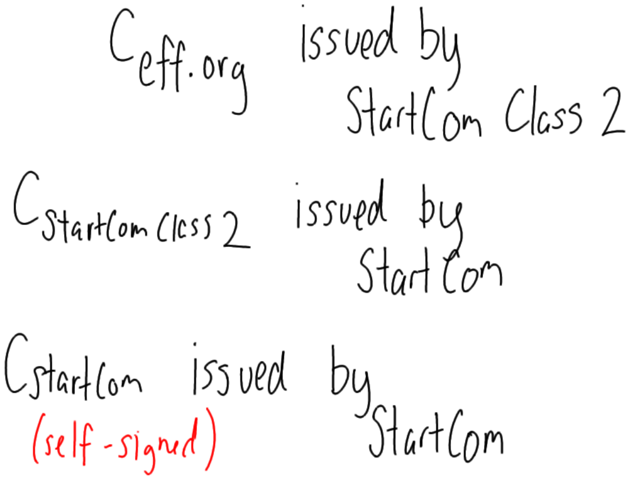


Figure 6: Server sending Certificate to Browser; Lecture 21



$C_{eff.org}$ issued by StartCom Class 2

$C_{StartCom\ Class\ 2}$ issued by StartCom

$C_{StartCom}$ issued by StartCom

(self-signed)

Figure 7: Certificate Hierarchy; Lecture 21