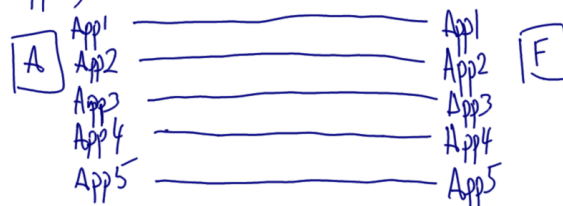


CSS441 – Key Management and Distribution Notes

Link-level : 20 keys

End-to-end : $\frac{10 \times 9}{2} = 45 \text{ keys}$ $\frac{n(n-1)}{2}$
(host)

End-to-end : $45 \times 5 = 225 \text{ keys}$
(5 apps)

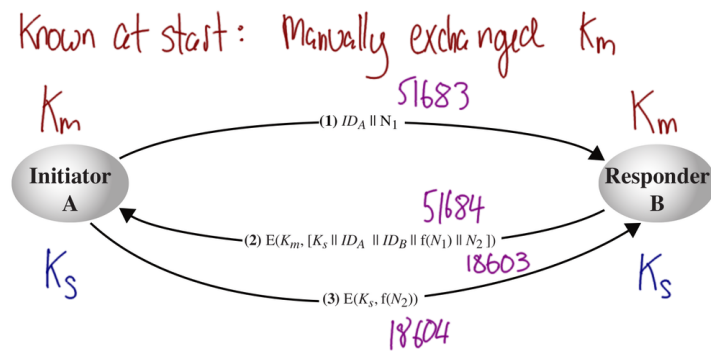


End-to-end : $\frac{50 \times 49}{2} = 1225 \text{ keys}$
(5 apps, any)

SIIT BKD : 1000 hosts

End-to-end : $\frac{1000 \times 999}{2} = \sim 500,000$

Figure 1: Number of Keys for Link and End-to-end Encryption; Lecture 19



Network : 1000 users

Master Keys: $\frac{1000 \times 999}{2} = 499,500$ (Manual)

Session Keys: 499,500 (automatic)
easy to change

Figure 2: Decentralised Symmetric Key Distribution; Lecture 19

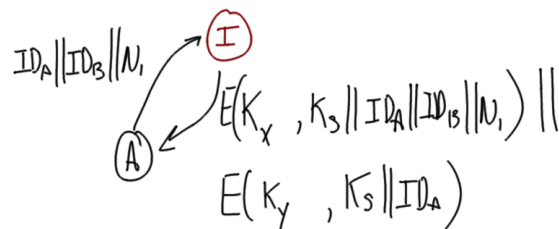


Figure 3: Attack on KDC 1; Lecture 19

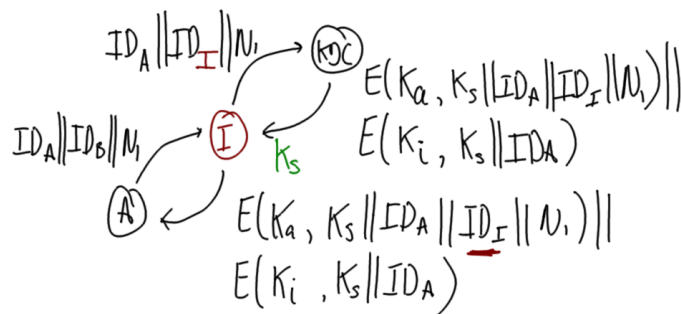


Figure 4: Attack on KDC 2; Lecture 19

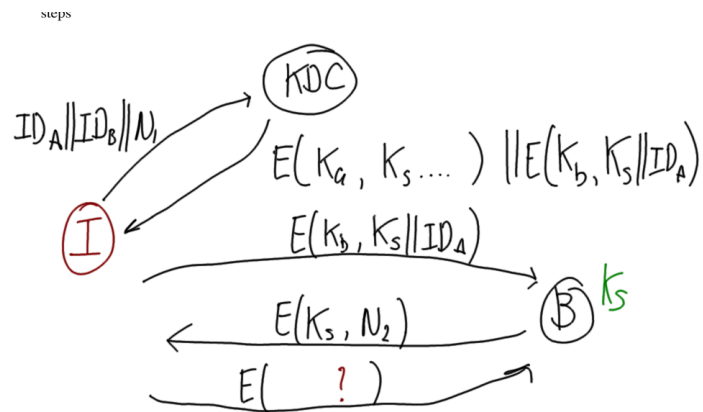


Figure 5: Attack on KDC 3; Lecture 19

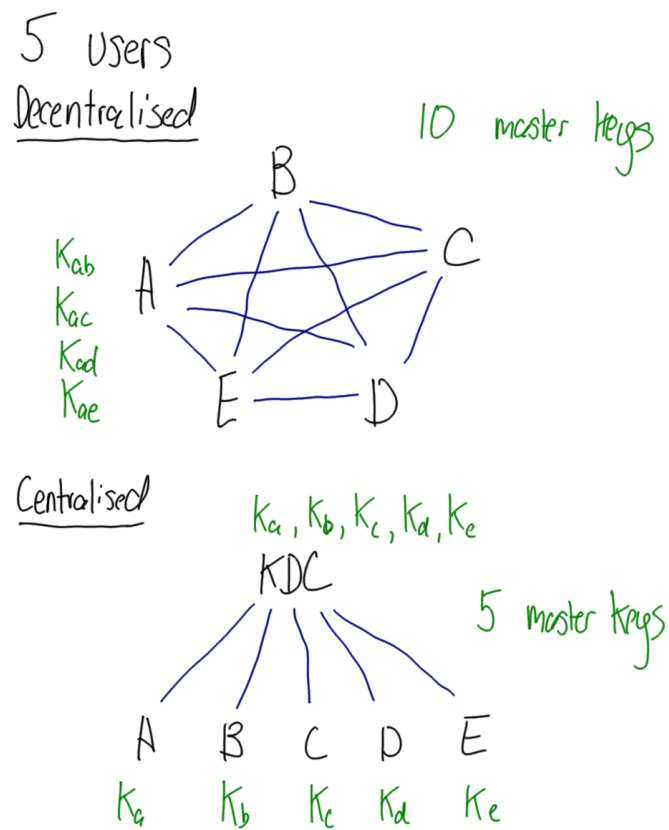


Figure 6: Centralised vs Decentralised Key Distribution; Lecture 20

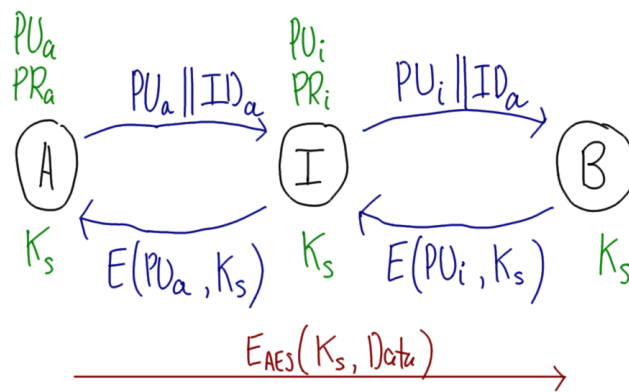


Figure 7: Man-in-the-middle Attack; Lecture 20

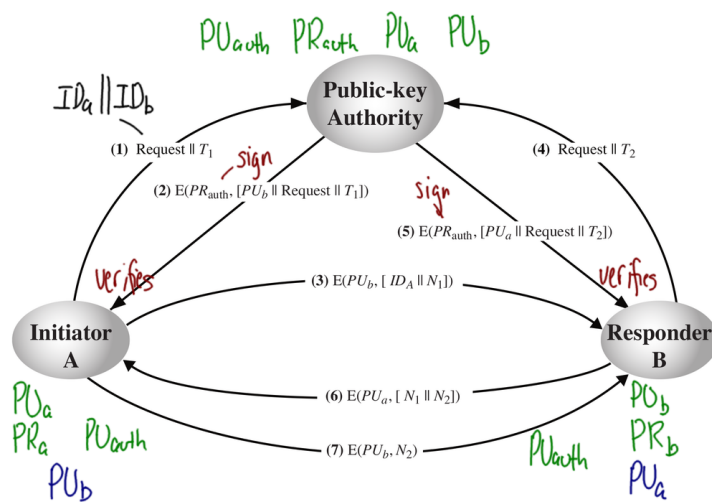


Figure 8: Public Key Authority; Lecture 20

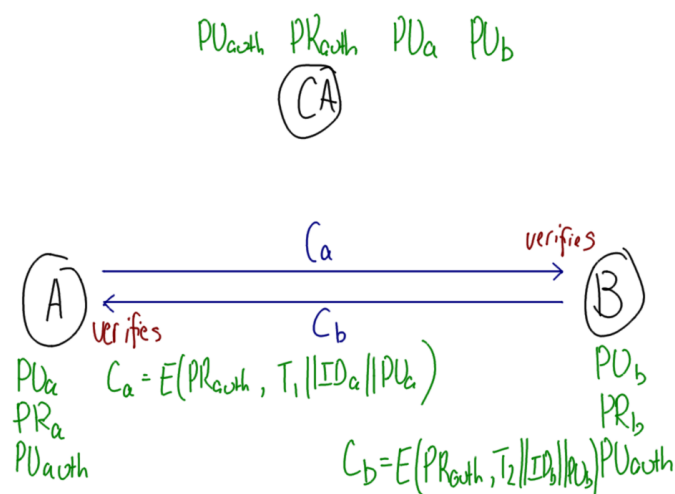


Figure 9: Certificate Authority; Lecture 20

$$C_{SIIT} = ID_{SIIT} || PU_{SIIT} || T, || \dots || E(PR_{COMODO-D}, H(\dots))$$

* .sint.tu.ac.th 2048 RSA

$$C_{COMODO-D} = ID_{COMODO-D} || PU_{COMODO-D} \dots E(PR_{COMODO-CA}, H(\dots))$$

$$C_{COMODO-CA} = \dots PU_{COMODO-CA} \dots E(PR_{COMODO-CA}, H(\dots))$$

Figure 10: Certificate Examples; Lecture 20

COMODO-D	<<SIIT>>	Trust
COMODO-CA	<<COMODO-D>>	Trust
COMODO-CA	<<COMODO-CA>>	Trust

self-signed

Figure 11: Certificate Hierarchy; Lecture 20