CSS322 – Key Management Notes

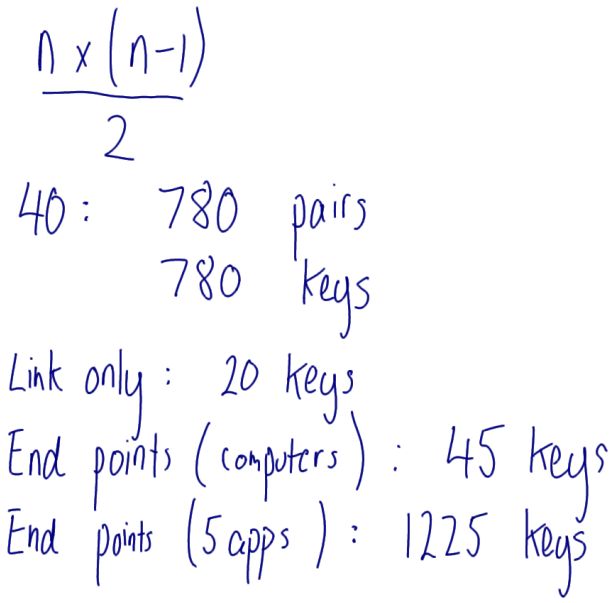

Figure 1: Number of Keys with Link and End-to-End Encryption; Lecture 20

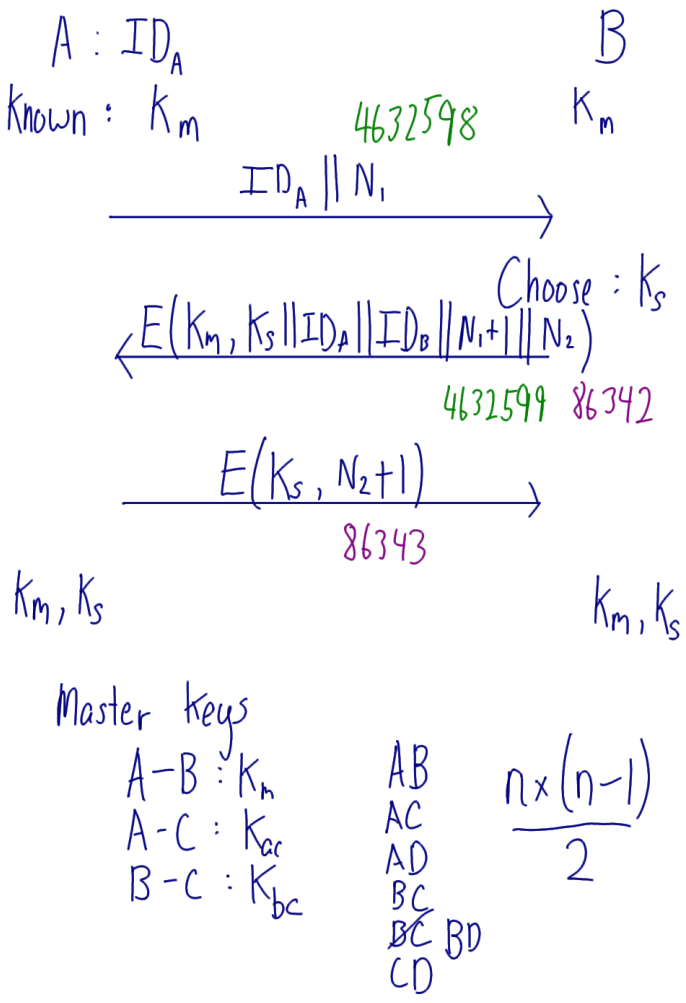

Figure 2: Decentralised Key Distribution; Lecture 20

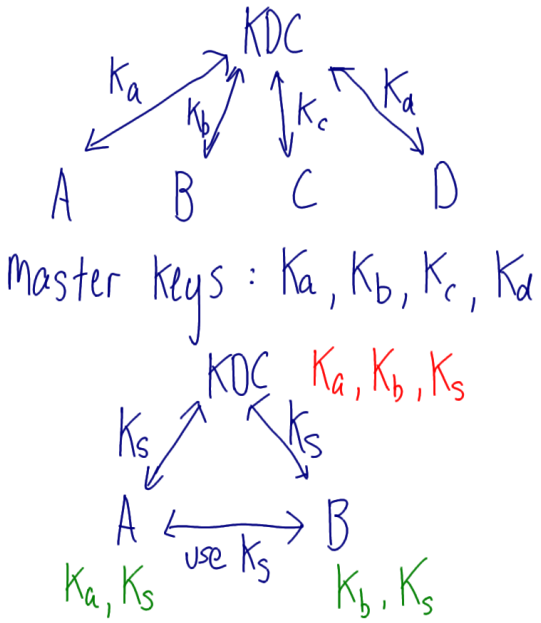

Figure 3: Centralised Key Distribution with KDC; Lecture 20

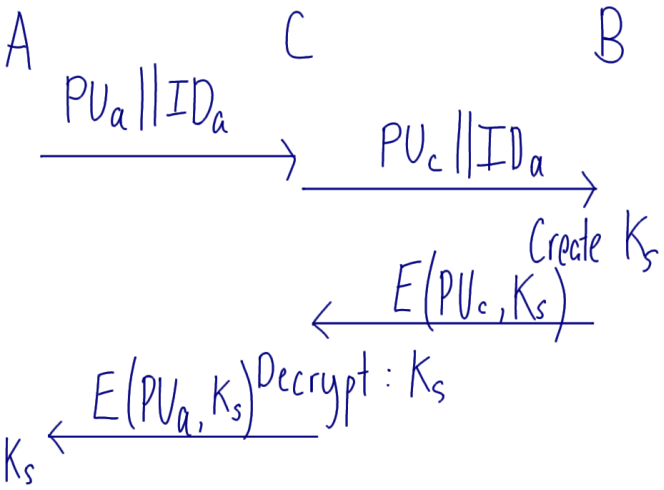

Figure 4: Man-in-the-Middle Attack on Public Key Exchange; Lecture 21

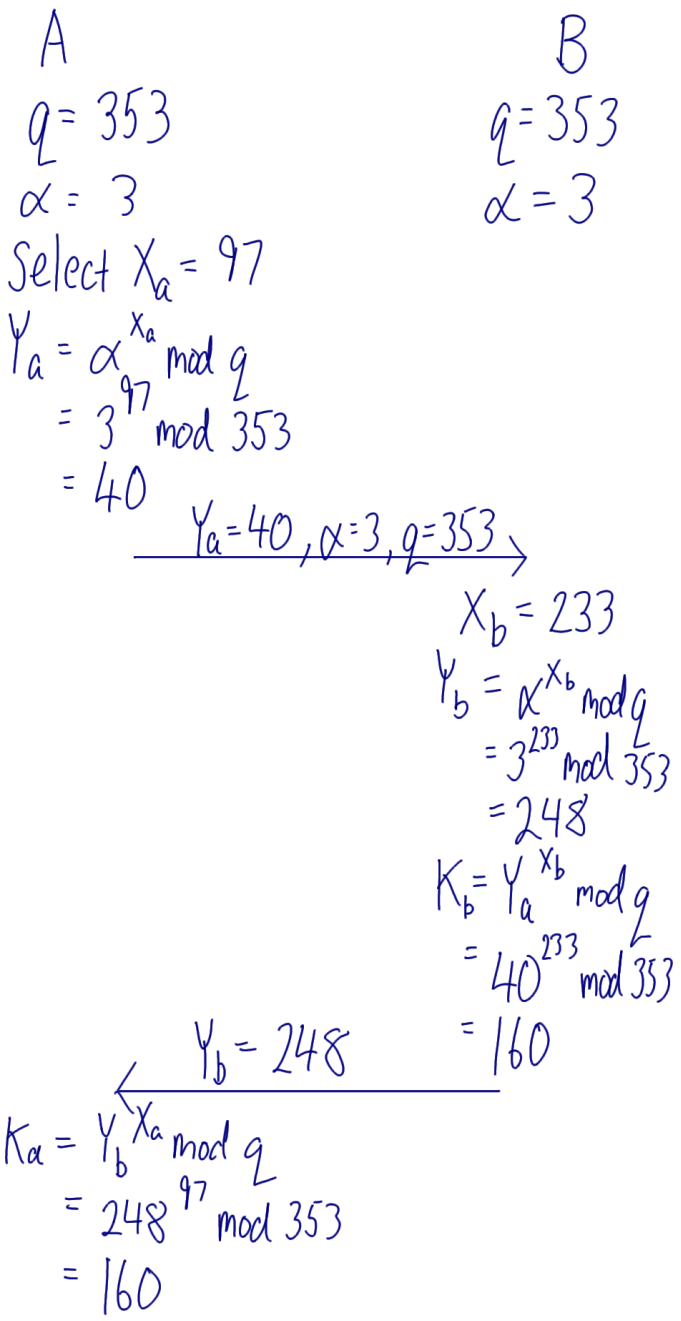

Figure 5: Diffie-Hellman Key Exchange Example; Lecture 21

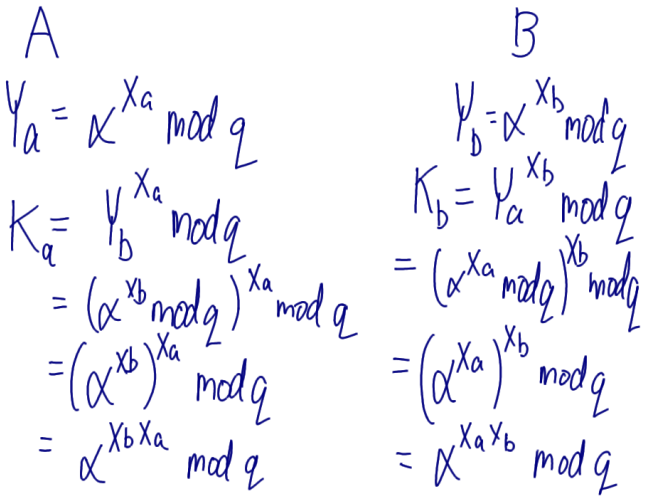

Figure 6: Diffie-Hellman Key Exchange Proof of Same Key; Lecture 21

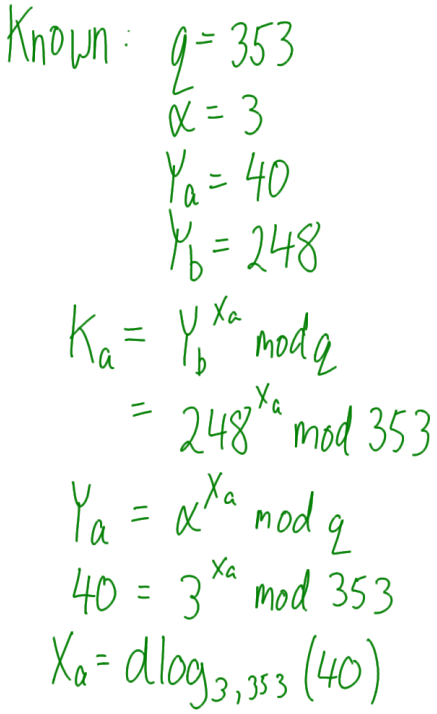

Figure 7: Diffie-Hellman Key Exchange Attack; Lecture 21

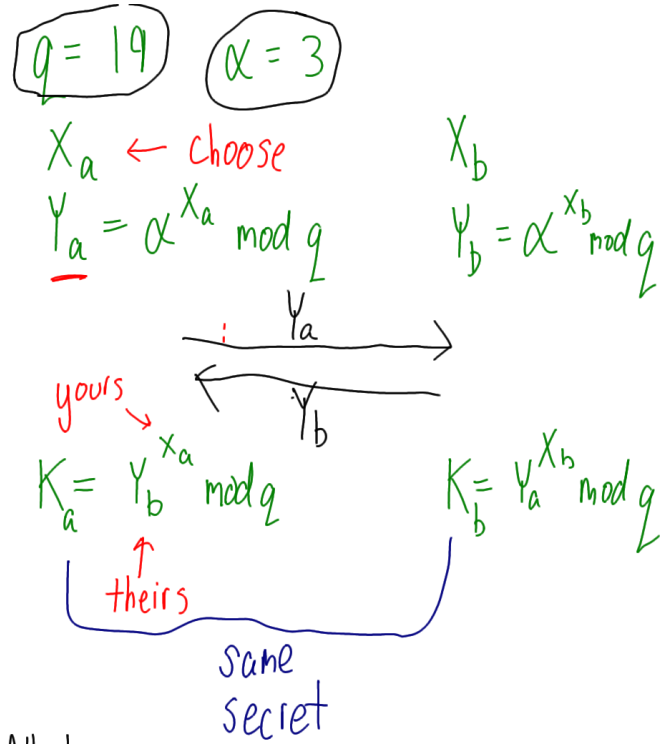

Figure 8: Diffie-Hellman Key Exchange Example 2; Lecture 22

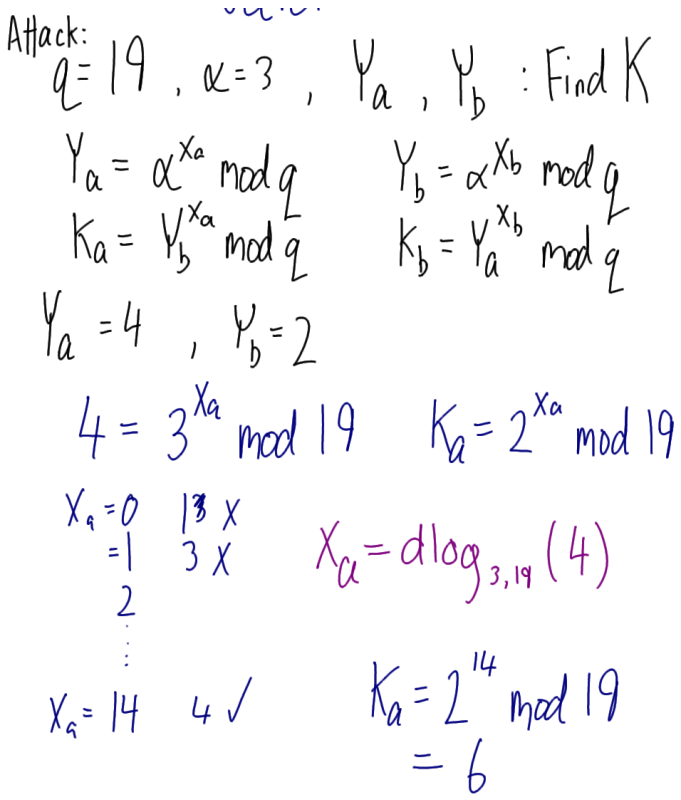

Figure 9: Diffie-Hellman Key Exchange Attack 2; Lecture 22

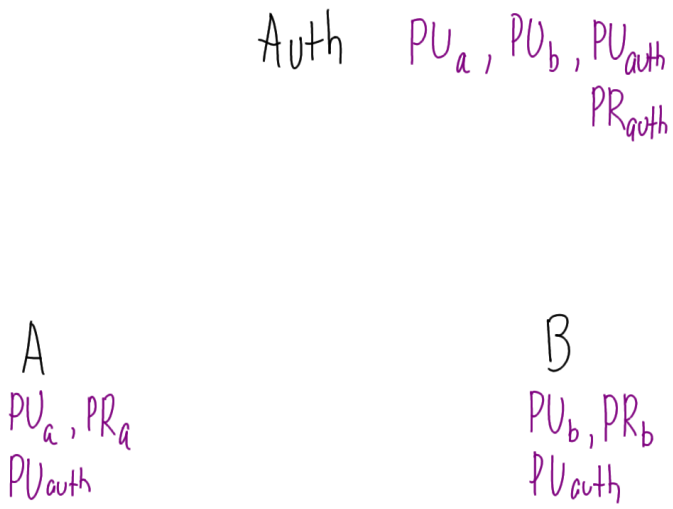

Figure 10: Public Key Authority: Known Keys; Lecture 22

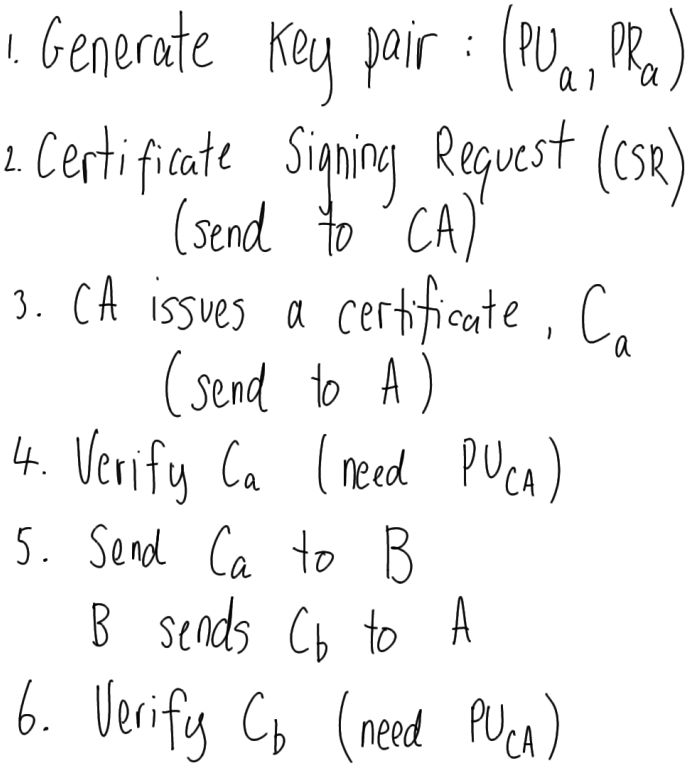

Figure 11: Certificate generation and signing steps; Lecture 24