CSS322 – Cryptographic Hash Functions Notes

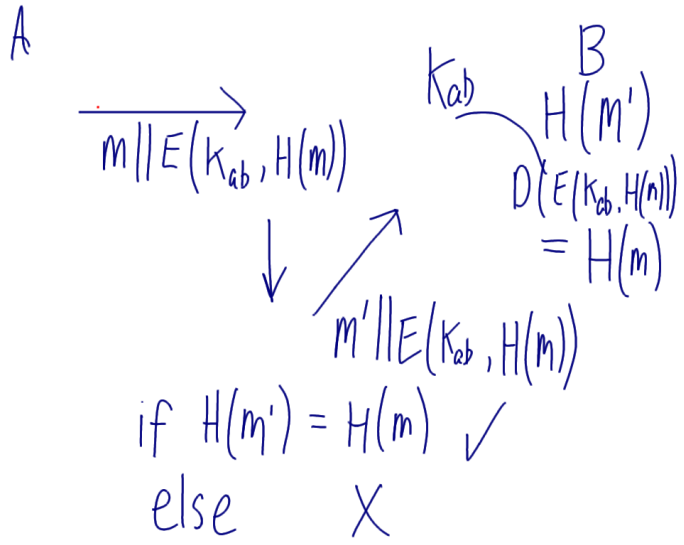

Figure 1: Attack on Hash for Authentication: Change M; Lecture 15

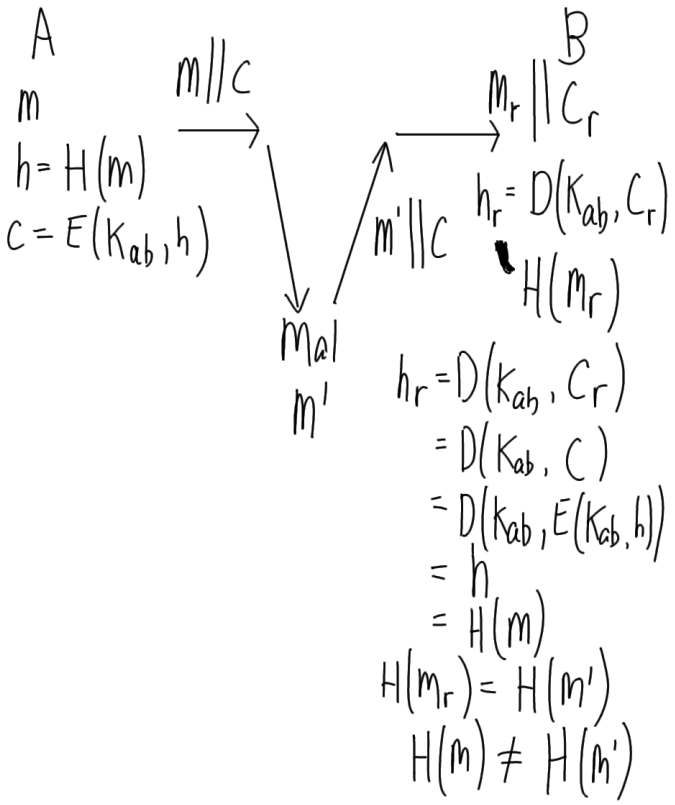

Figure 2: Attack on Hash Authentication with Symmetric Key: Change M; Lecture 16

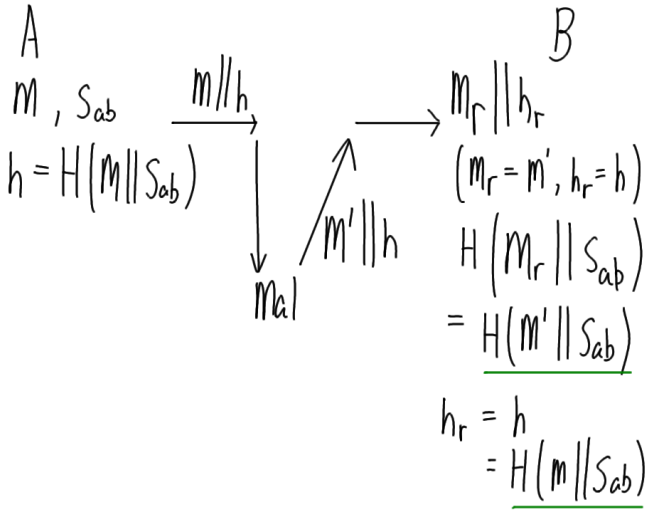

Figure 3: Attack on Hash Authentication with Secret: Change M; Lecture 16

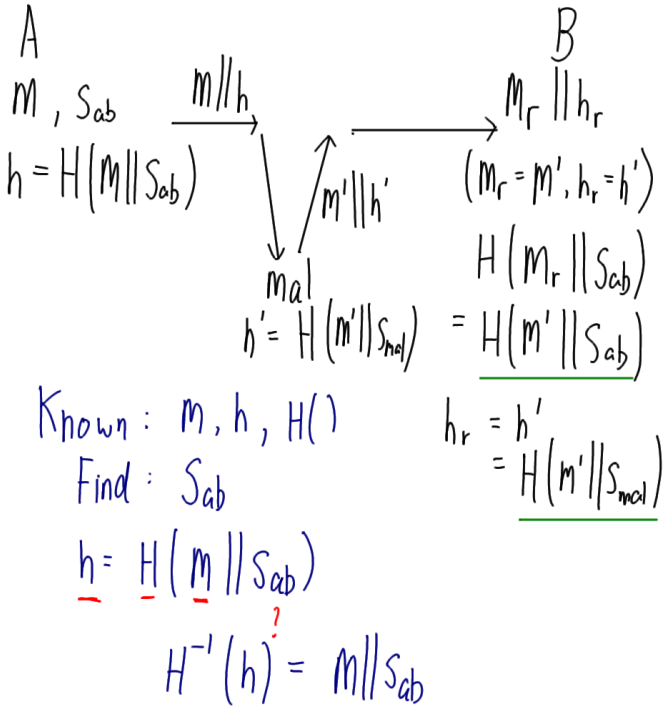

Figure 4: Attack on Hash Authentication with Secret: Change M and h; Lecture 16

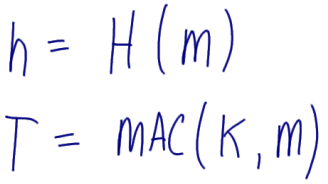

Figure 5: Hash Function vs MAC Function; Lecture 16

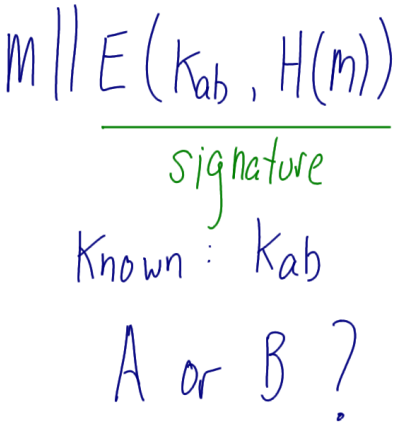

Figure 6: Symmetric Encryption cannot provide digital signature; Lecture 16