ITS335 – Cryptographic Hash Functions Notes

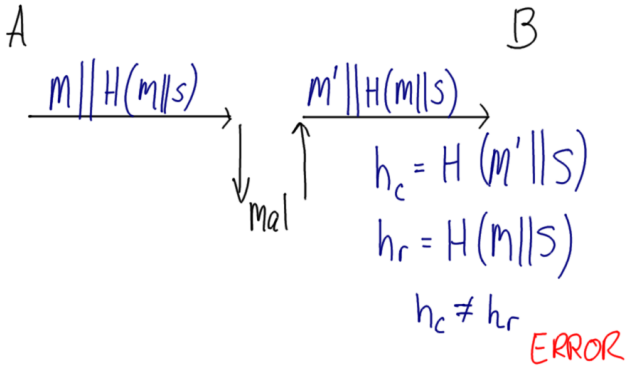

Figure 1: Attack 1 on Hash with Secret Authentication; Lecture 18

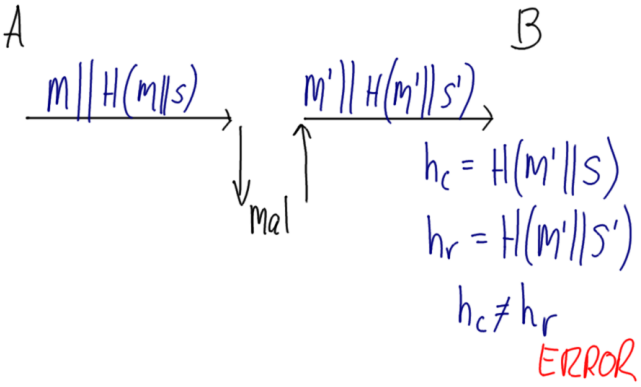

Figure 2: Attack 2 on Hash with Secret Authentication; Lecture 18

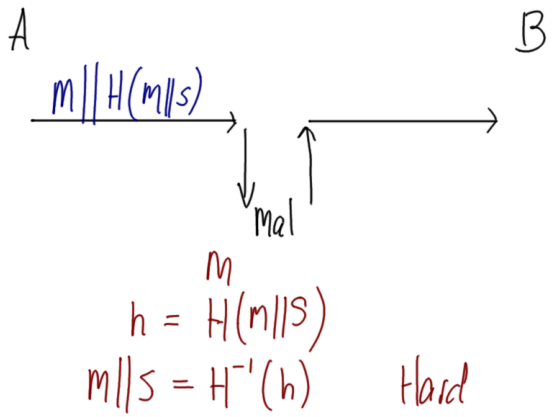

Figure 3: One Way Property Required for Hash with Secret Authentication; Lecture 18

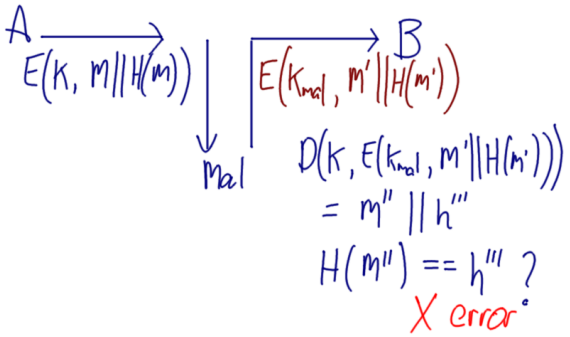

Figure 4: Hash with Encryption for Authentication 1; Lecture 19

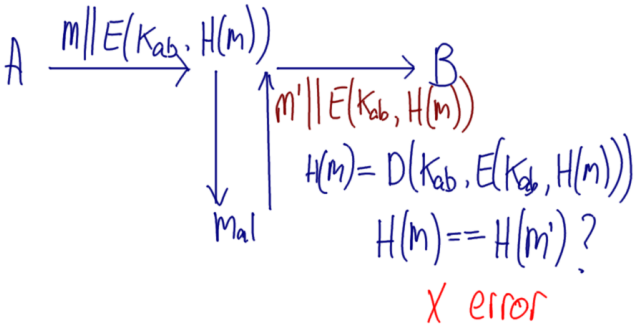

Figure 5: Hash with Encryption for Authentication 2; Lecture 19

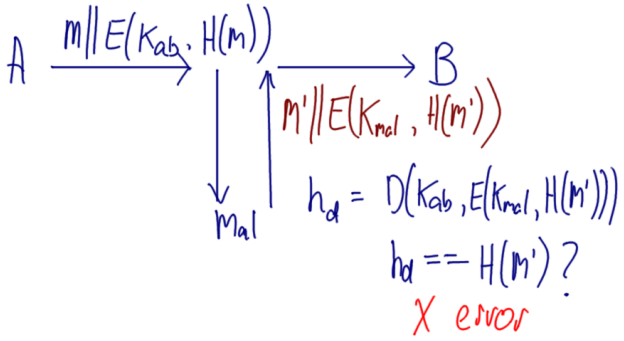

Figure 6: Hash with Encryption for Authentication 3; Lecture 19

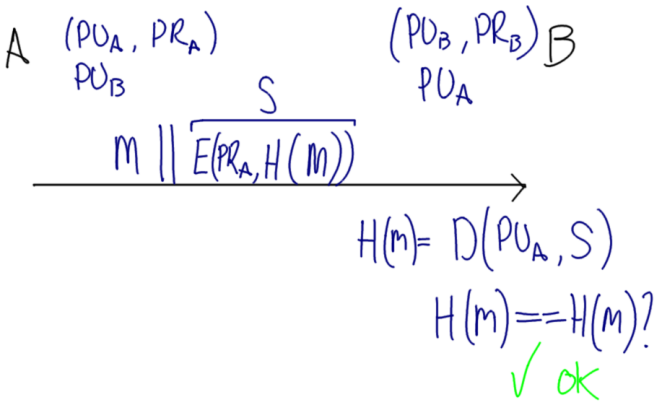

Figure 7: Digital Signature 1; Lecture 19

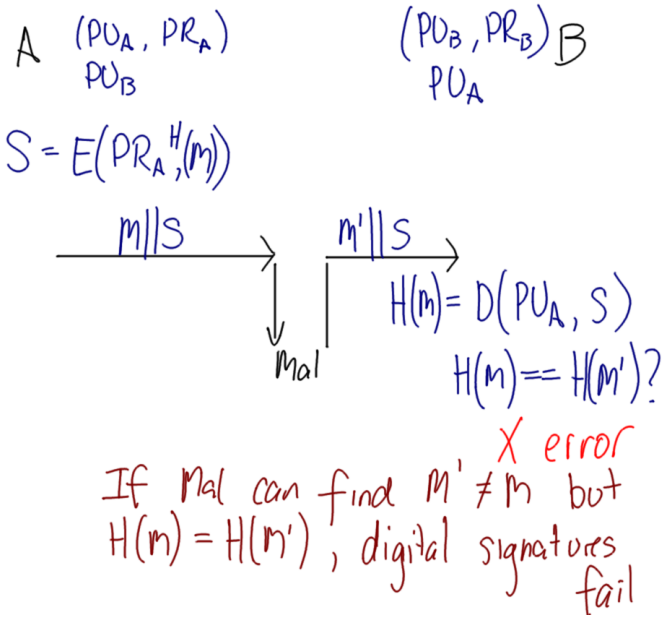

Figure 8: Digital Signature 2; Lecture 19

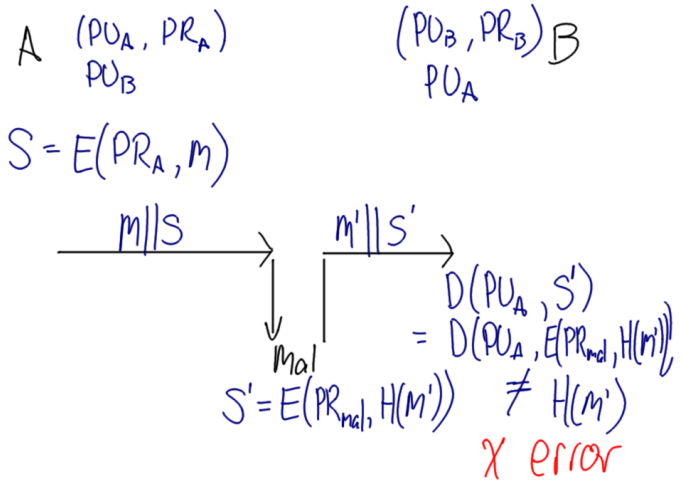

Figure 9: Digital Signature 3; Lecture 19

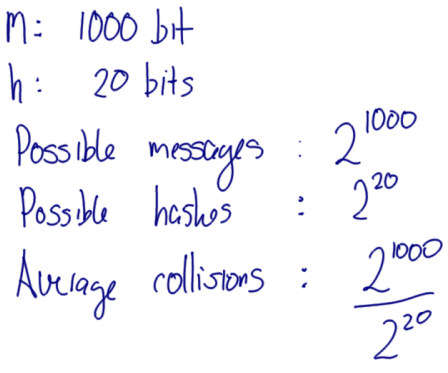

Figure 10: Average Number of Hash Collisions; Lecture 19

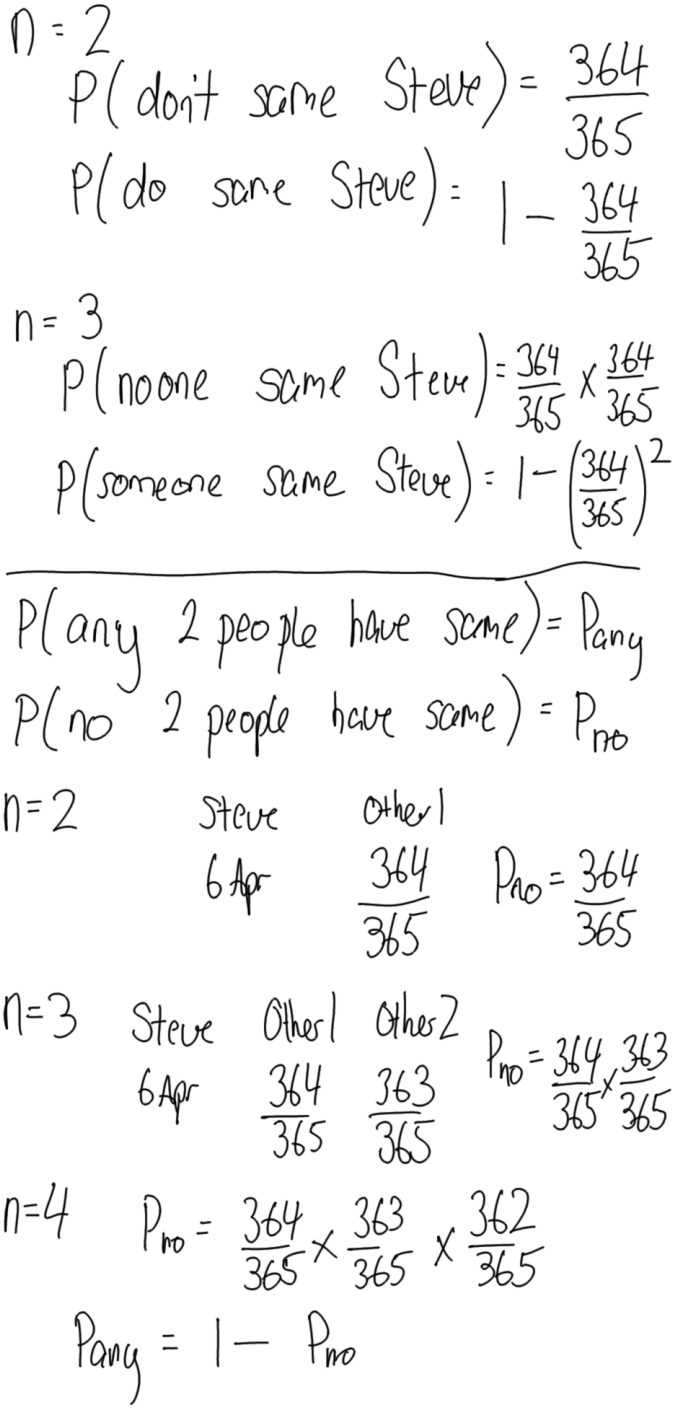

Figure 11: Example of Birthday Probability Calculations; Lecture 19