

ITS335 – Cryptographic Hash Functions Notes

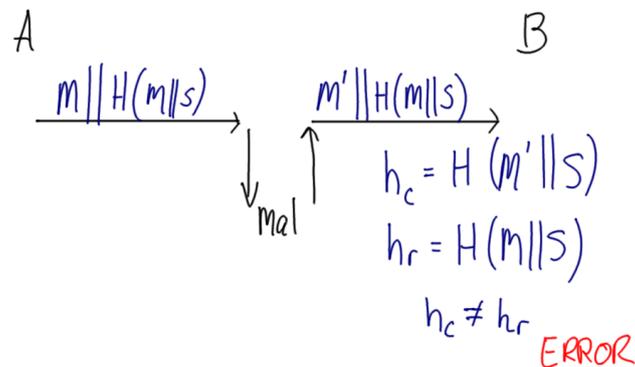


Figure 1: Attack 1 on Hash with Secret Authentication; Lecture 18

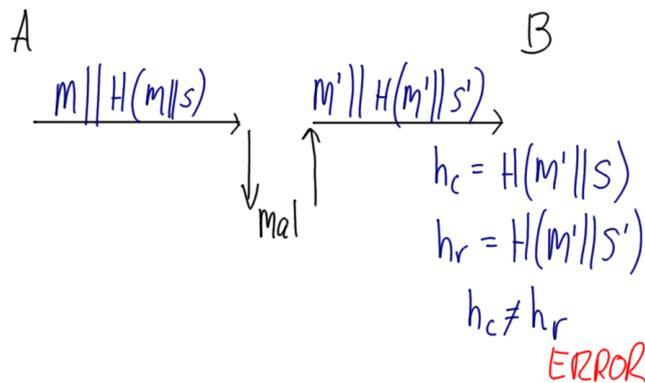


Figure 2: Attack 2 on Hash with Secret Authentication; Lecture 18

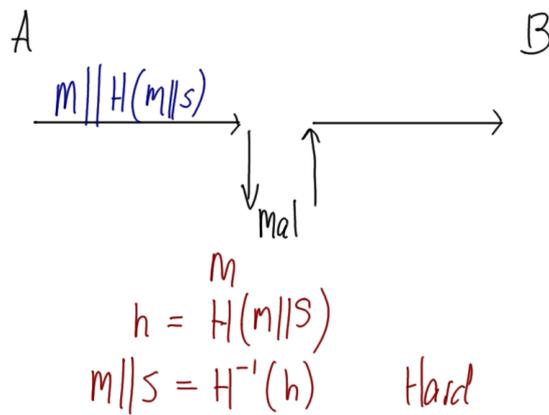


Figure 3: One Way Property Required for Hash with Secret Authentication; Lecture 18

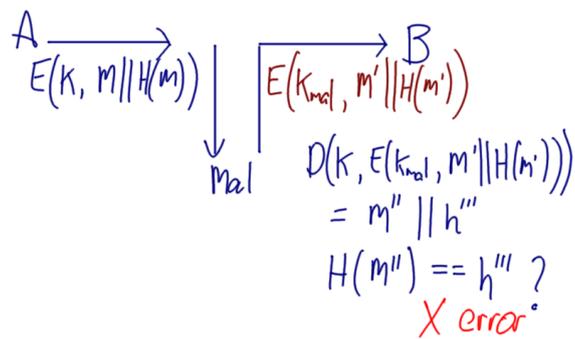


Figure 4: Hash with Encryption for Authentication 1; Lecture 19

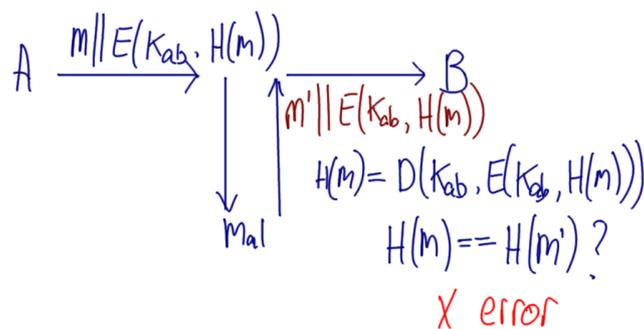


Figure 5: Hash with Encryption for Authentication 2; Lecture 19

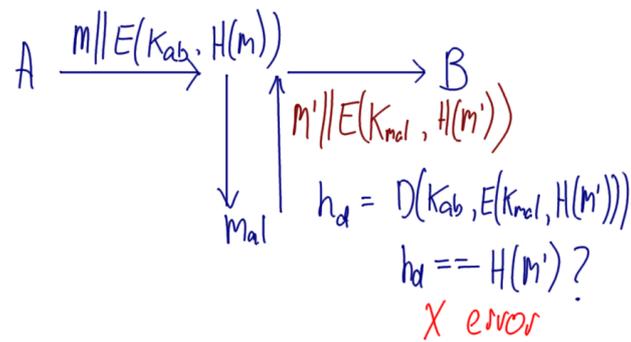


Figure 6: Hash with Encryption for Authentication 3; Lecture 19

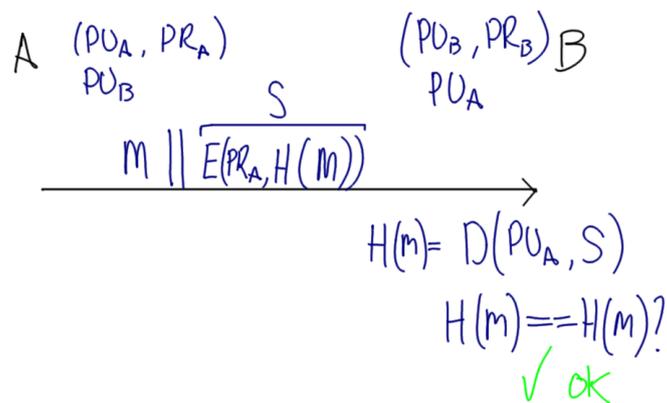


Figure 7: Digital Signature 1; Lecture 19

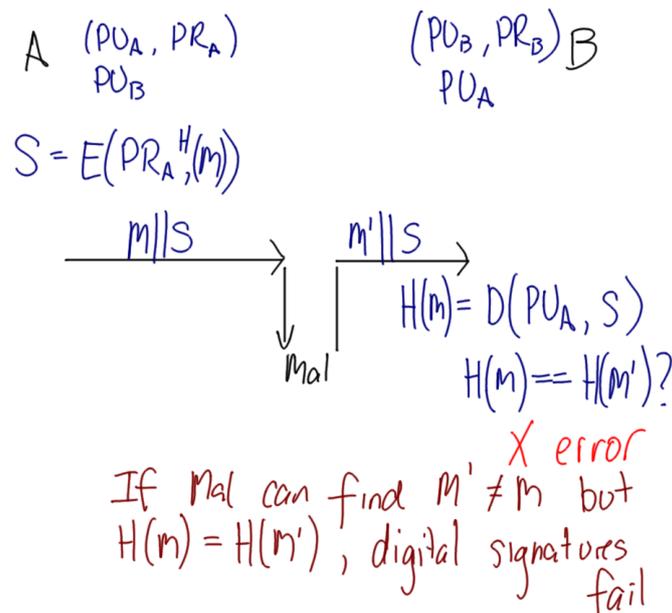


Figure 8: Digital Signature 2; Lecture 19

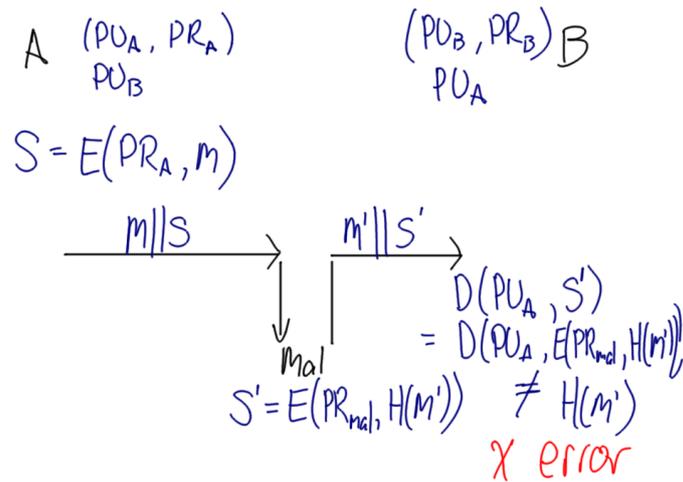


Figure 9: Digital Signature 3; Lecture 19

$m: 1000 \text{ bit}$
 $h: 20 \text{ bits}$
 Possible messages : 2^{1000}
 Possible hashes : 2^{20}
 Average collisions : $\frac{2^{1000}}{2^{20}}$

Figure 10: Average Number of Hash Collisions; Lecture 19

$$n = 2$$

$$P(\text{don't same Steve}) = \frac{364}{365}$$

$$P(\text{do same Steve}) = 1 - \frac{364}{365}$$

$$n = 3$$

$$P(\text{no one same Steve}) = \frac{364}{365} \times \frac{364}{365}$$

$$P(\text{someone same Steve}) = 1 - \left(\frac{364}{365}\right)^2$$

$$P(\text{any 2 people have same}) = P_{\text{any}}$$

$$P(\text{no 2 people have same}) = P_{\text{no}}$$

$$n = 2 \quad \begin{array}{l} \text{Steve} \\ \text{6 Apr} \end{array} \quad \begin{array}{l} \text{Other 1} \\ \frac{364}{365} \end{array} \quad P_{\text{no}} = \frac{364}{365}$$

$$n = 3 \quad \begin{array}{l} \text{Steve} \\ \text{6 Apr} \end{array} \quad \begin{array}{l} \text{Other 1} \\ \frac{364}{365} \end{array} \quad \begin{array}{l} \text{Other 2} \\ \frac{363}{365} \end{array} \quad P_{\text{no}} = \frac{364}{365} \times \frac{363}{365}$$

$$n = 4 \quad P_{\text{no}} = \frac{364}{365} \times \frac{363}{365} \times \frac{362}{365}$$

$$P_{\text{any}} = 1 - P_{\text{no}}$$

Figure 11: Example of Birthday Probability Calculations; Lecture 19