

ITS335 – Cryptography Notes

$P = \text{hellosteve}$
 $K = d(3)$
 $h \rightarrow k \quad e \rightarrow h \quad l \rightarrow o$
 $C = \text{khoorvwhyh}$

Figure 1: Caesar Cipher Example 1; Lecture 02

$C = \text{cokebsd}$
 $K = k$
 $P = \text{seaurity}$
 ↑
 c

Figure 2: Caesar Cipher Example 2; Lecture 02

$P = \text{hellostevesecurity}$
 $K = 3$
 $\begin{matrix} h & l & t & e & c & i \\ e & o & e & s & u & t \\ l & s & v & e & r & y \end{matrix}$
 $C = \text{hteci eo es ut lsvery}$

Figure 3: Rail Fence Cipher Example; Lecture 03

$P = \text{hellostevesecurity}$
 $K = \text{love|love|love|love|love}$
 $\begin{matrix} 7 \\ 11 \end{matrix}$
 $C = \text{ssap} \dots$

Figure 4: Vigenere Cipher 1; Lecture 03

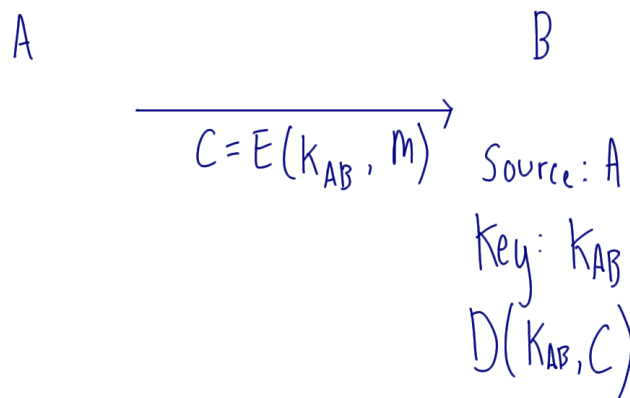


Figure 5: Authentication with Symmetric Encryption - Normal; Lecture 04

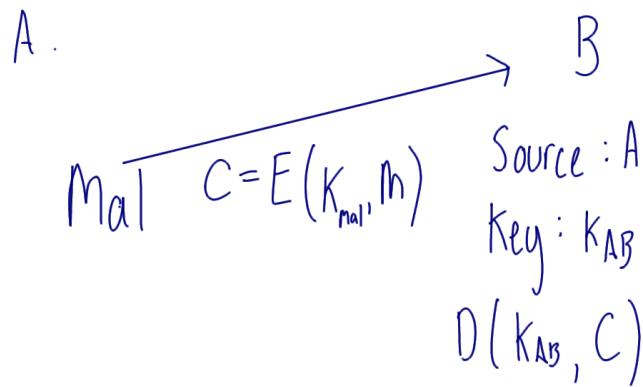


Figure 6: Authentication with Symmetric Encryption - Malicious; Lecture 04

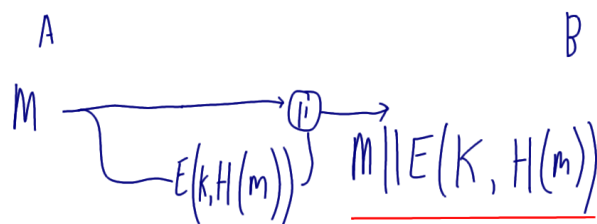


Figure 7: Authentication with Hash Function - Normal Case; Lecture 05

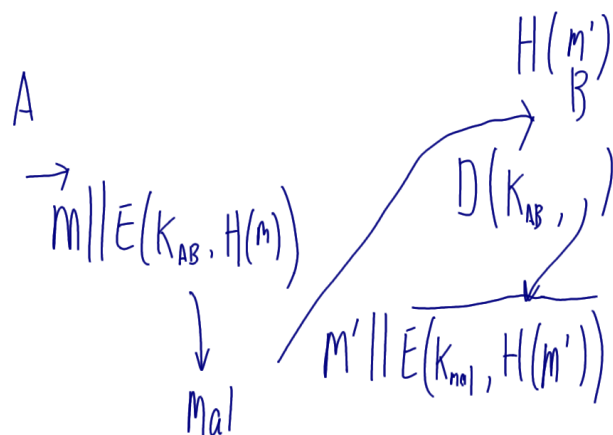


Figure 8: Authentication with Hash Function - Attack 1; Lecture 05

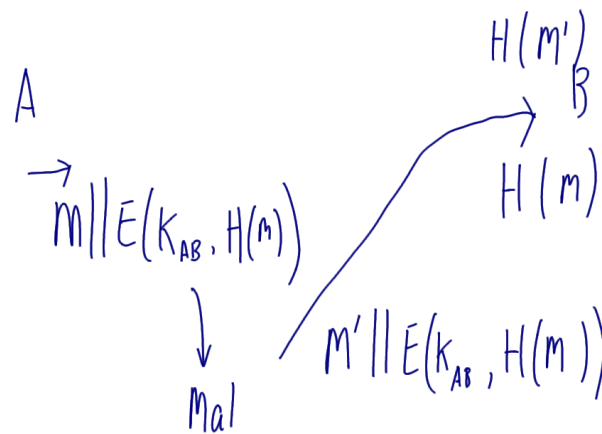


Figure 9: Authentication with Hash Function - Attack 2; Lecture 05

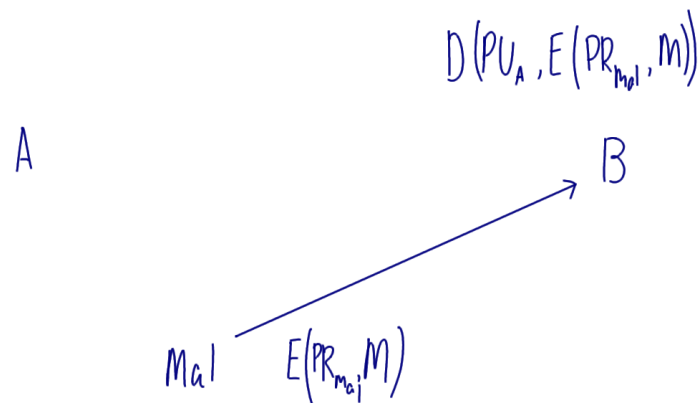


Figure 10: Authentication with Public Key Crypto; Lecture 05

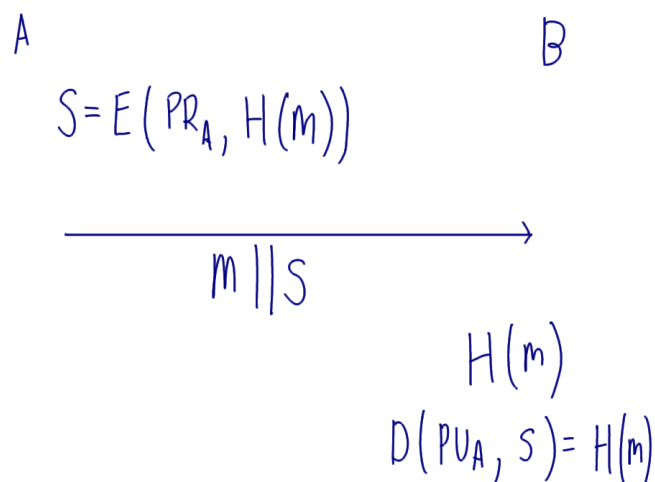


Figure 11: Digital Signature Normal Operation; Lecture 06

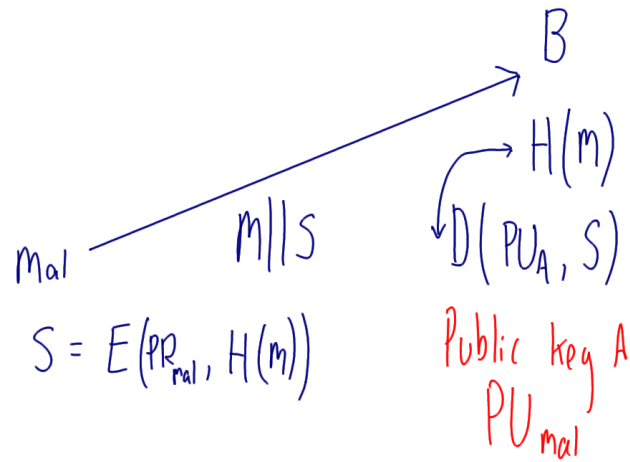


Figure 12: Digital Signature Masquerade Attack; Lecture 06

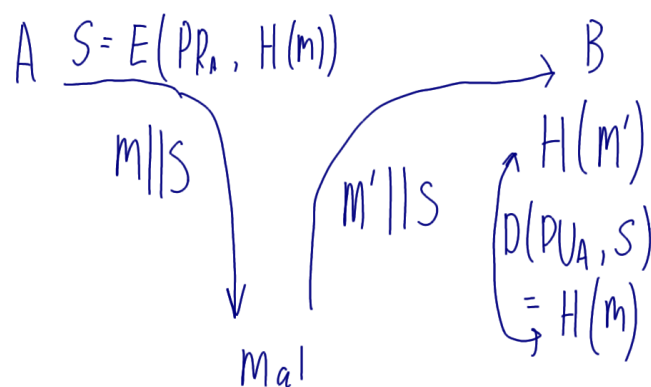


Figure 13: Digital Signature Modification Attack; Lecture 06