

ITS335 – Cryptography Notes

3 bit key
Decrypt C k = 000 P?
 k = 001 P?
 $2^3 = 8$ 010
 011
 100
 101
 110
 111

10 bits : $2^{10} = 1024$
30 bits : $\approx 10^9$
100 bits : 2^{100}

Figure 1: Simple Brute Attack Example; Lecture 02

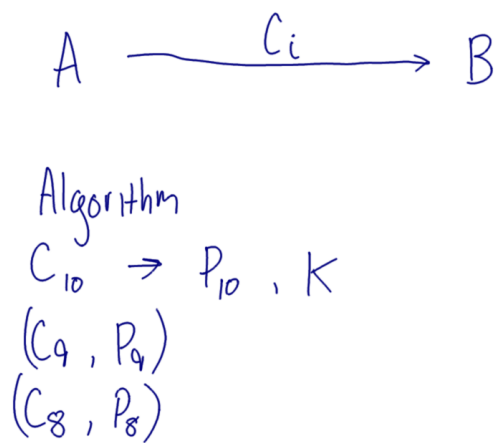
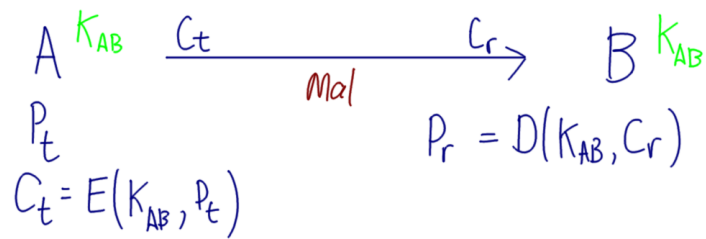


Figure 2: Example of Known Plaintext; Lecture 02



Case $C_r = C_t$: $P_r = P_t$
 Case $C_r \neq C_t$: $P_r \neq P_t$ \swarrow integrity
 P_r is incorrect

$P_1 = D(K_1, C_t)$ P_1 is incorrect
 $P_2 = D(K_2, C_t)$ P_2 is incorrect

$E(K_1, P_1) = C_1$
 $E(K_1, P_2) = C_2$ $P_1 \neq P_2$ $C_1 \neq C_2$
 $E(K_2, P_1) = C_3$ $K_1 \neq K_2$ $C_1 \neq C_3$

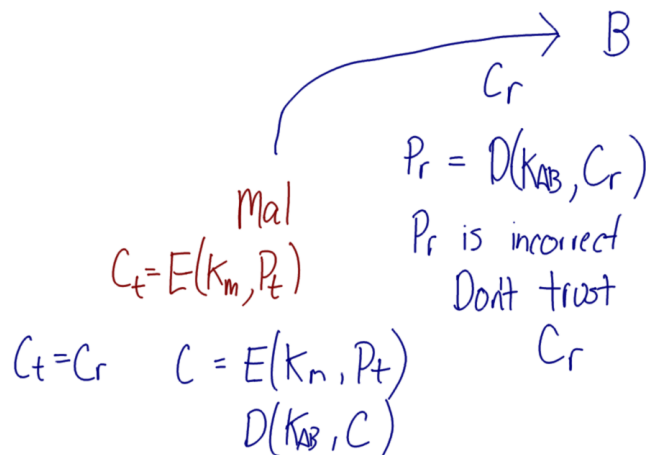


Figure 3: Confidentiality and Authentication with Symmetric Key Ciphers; Lecture 04

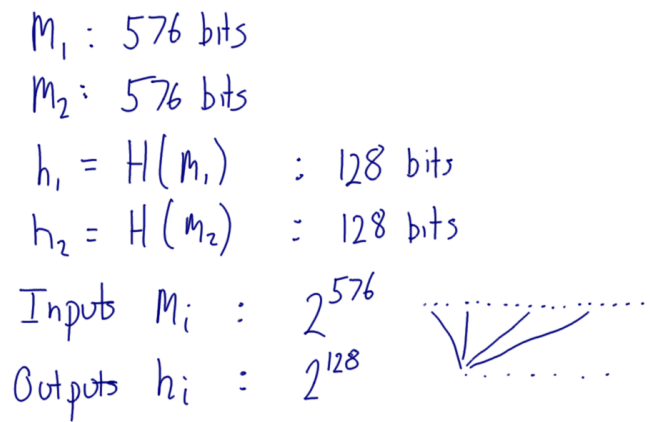


Figure 4: Hash Collisions; Lecture 04

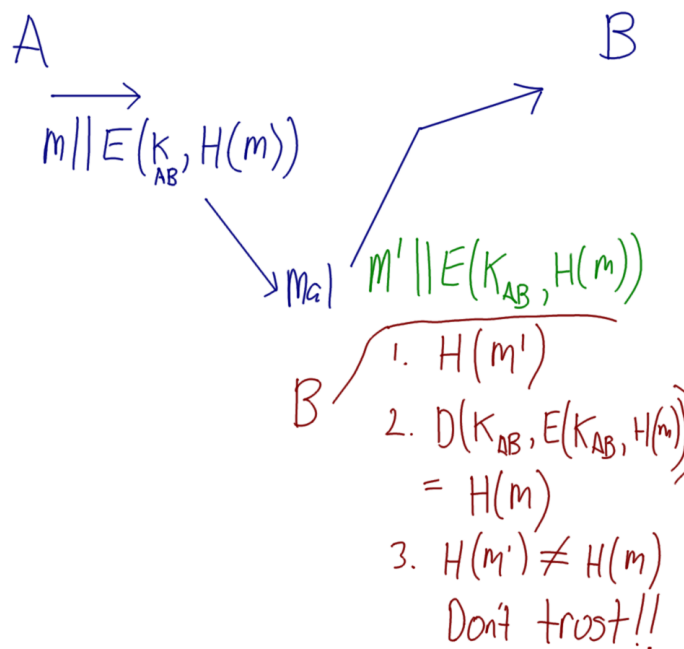


Figure 5: Authentication with Hash Functions - Attack 1; Lecture 05

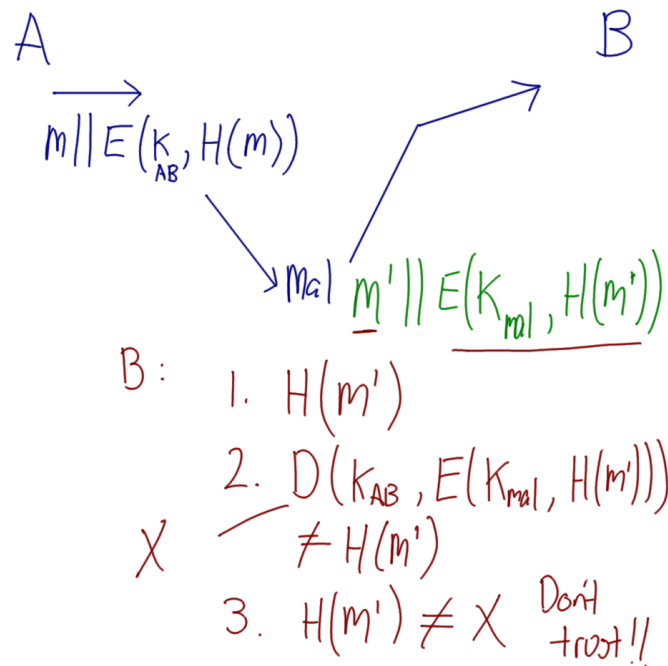


Figure 6: Authentication with Hash Functions - Attack 2; Lecture 05

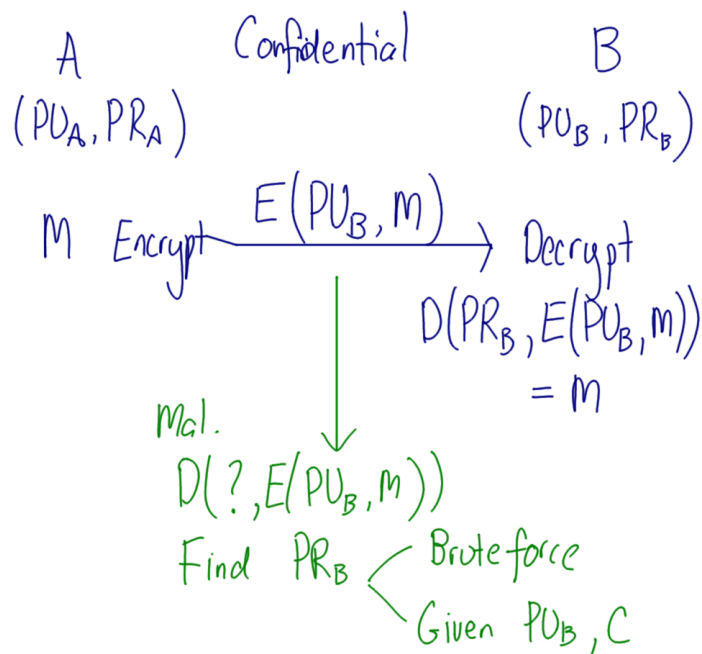


Figure 7: Public Key Cryptography for Confidentiality; Lecture 05

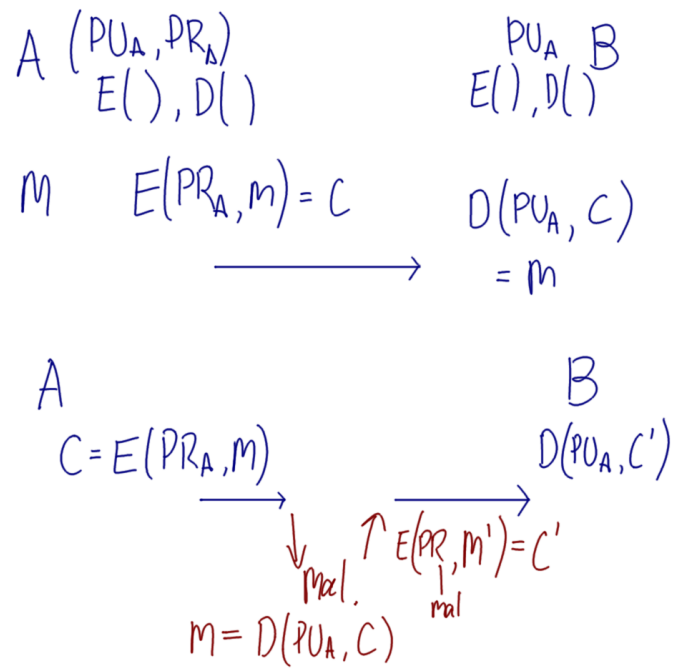


Figure 8: Public Key Cryptography for Authentication; Lecture 06

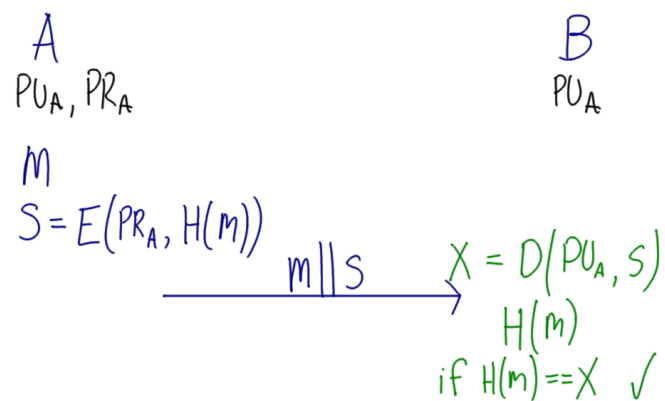


Figure 9: Digital Signature Example 1; Lecture 06

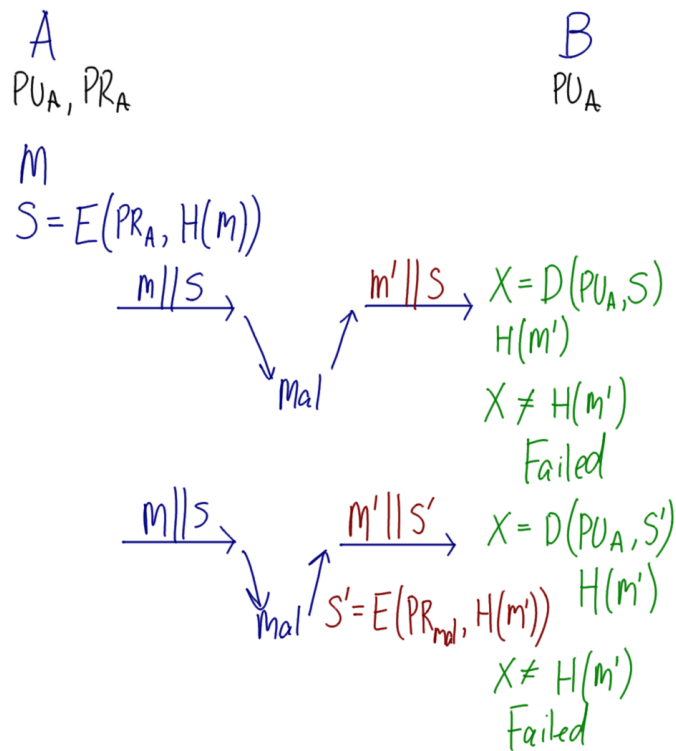


Figure 10: Digital Signature Example 2; Lecture 06

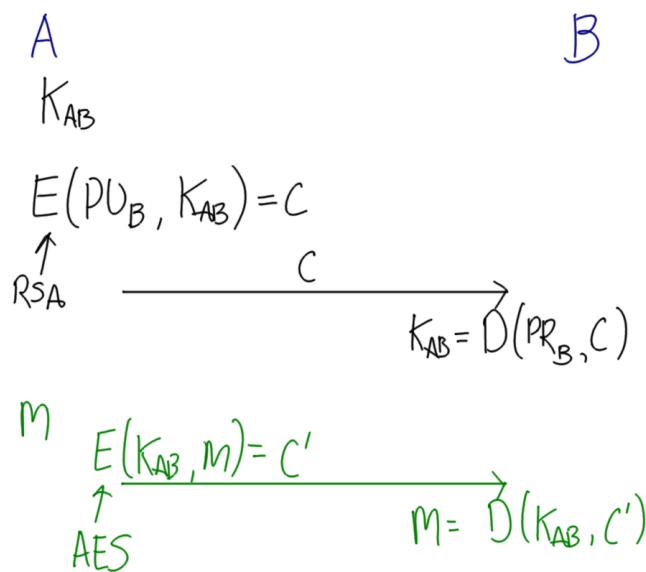


Figure 11: Shared Secret Key with Public Key Cryptography; Lecture 06