CSS441 – Cryptographic Hash Functions Notes

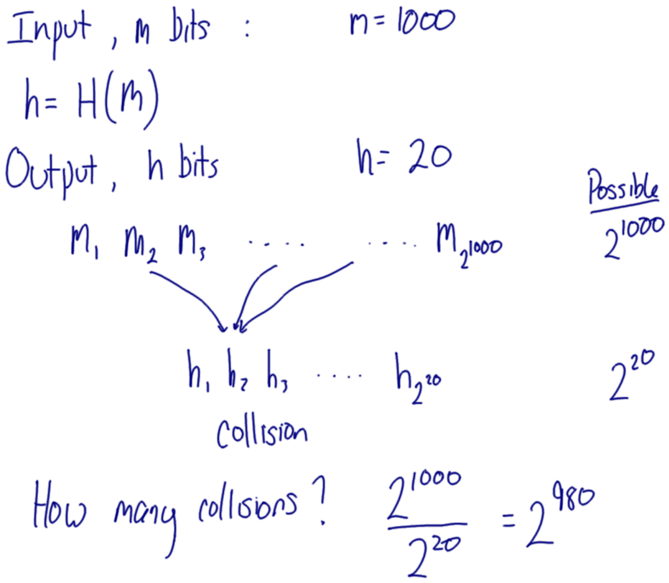


Figure 1: Number of Hash Collisions; Lecture 18

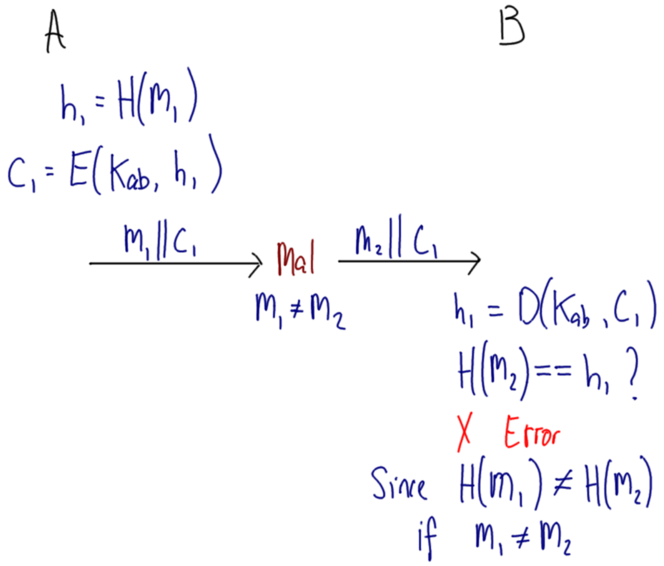


Figure 2: Symmetric Encryption of Hash; Lecture 18

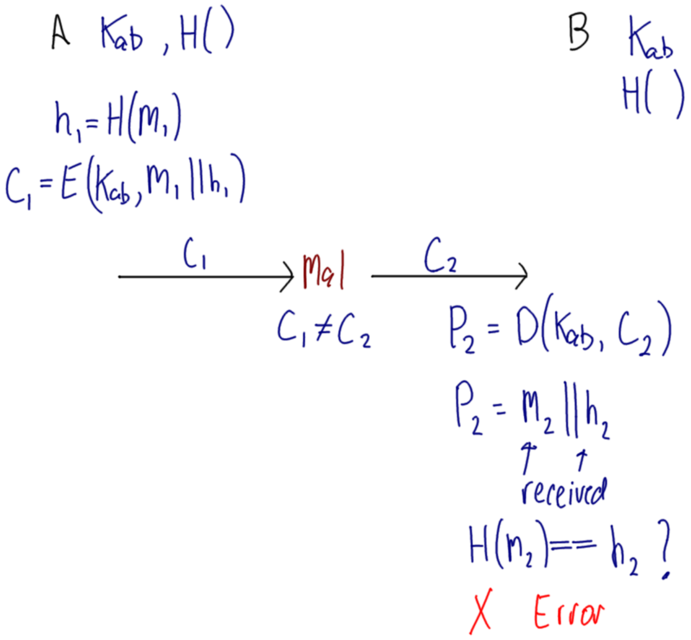


Figure 3: Symmetric Encryption of Message and Hash; Lecture 18

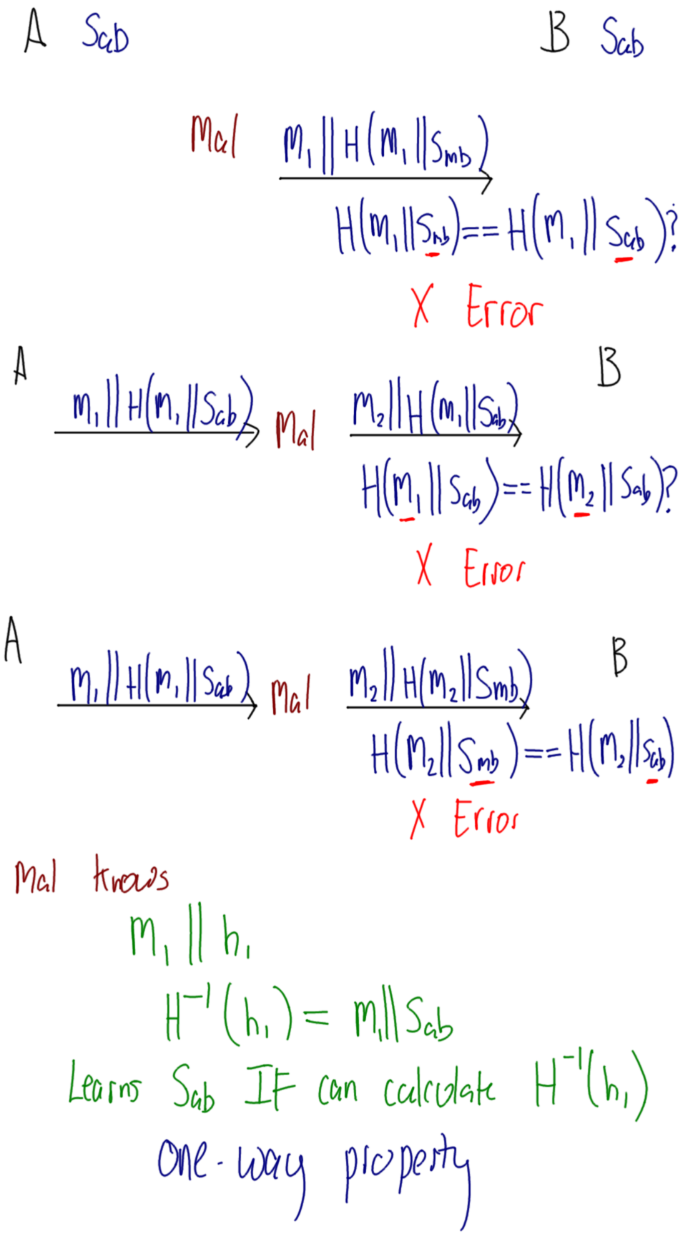

A S_{ab}
B S_{ab}
Mal
$M_1 \| H(M_1 \| S_{mb})$
$H(M_1 \| S_{mb}) == H(M_1 \| S_{ab})$?
X Error
A
$M_1 \| H(M_1 \| S_{ab})$
Mal
$M_2 \| H(M_1 \| S_{ab})$
B
$H(M_1 \| S_{ab}) == H(M_2 \| S_{ab})$?
X Error
A
$M_1 \| H(M_1 \| S_{ab})$
Mal
$M_2 \| H(M_2 \| S_{mb})$
B
$H(M_2 \| S_{mb}) == H(M_2 \| S_{ab})$
X Error
Mal knows
$M_1 \| h_1$
$H^{-1}(h_1) = M_1 \| S_{ab}$
Learns S_{ab} IF can calculate $H^{-1}(h_1)$
One-way property

Figure 4: Hash of Message and Secret; Lecture 18

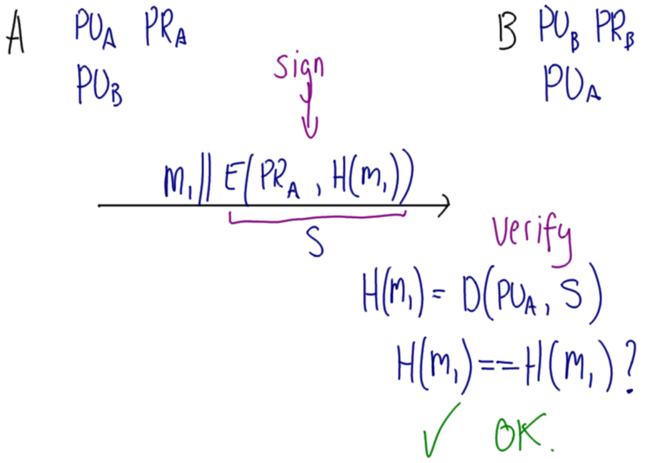


Figure 5: Digital Signature Verification; Lecture 18

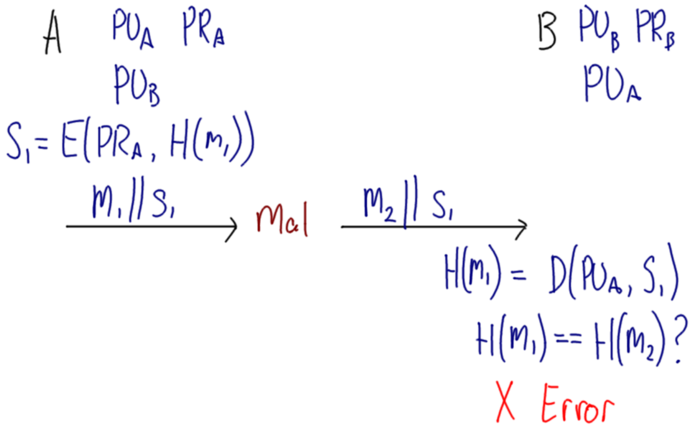
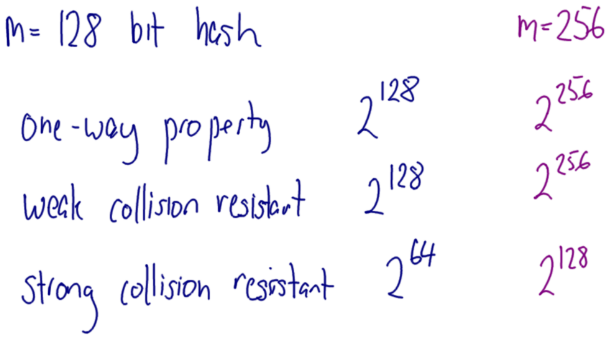


Figure 6: Attack on Digital Signature; Lecture 18



M= 128 bit hash		M=256
One-way property	2^{128}	2^{256}
weak collision resistant	2^{128}	2^{256}
strong collision resistant	2^{64}	2^{128}

Figure 7: Effort to Break Hash Properties; Lecture 18