Addendum: Message Authentication Code

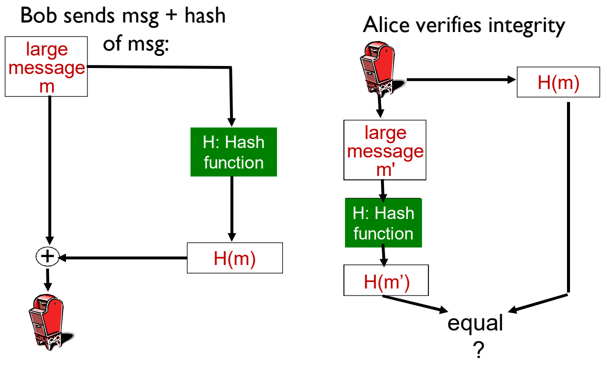
Context

Unfortunately, the slides don’t cover Section 8.3.2 of the text: *Message Authentication Code (MAC)*

We will refer to this material several times in subsequent sections.

Review: Message integrity (without authentication)

Section 6.2 (EDC)



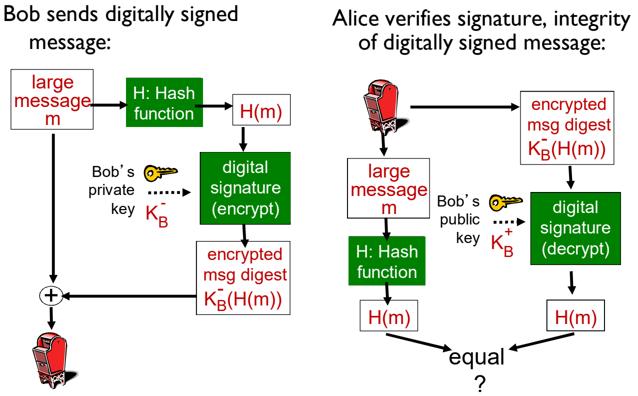
Bob sends msg + hash of msg:

Alice verifies integrity

Think “Hash = Internet Checksum” or “CRC”

Review: Digital signature = signed message digest

Slide 8-49



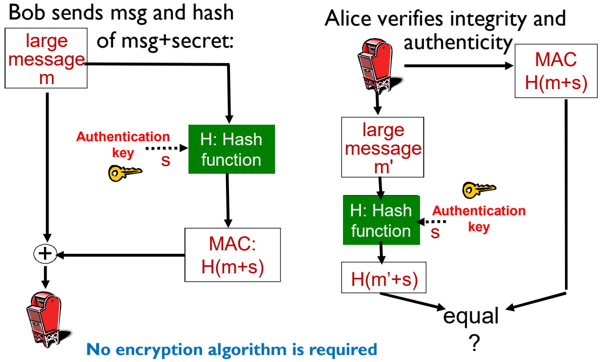
Bob sends digitally signed message:

Alice verifies signature, integrity of digitally signed message:

large message m
H: Hash function
H(m)
Bob's private key K_B^-
digital signature (encrypt)
encrypted msg digest $K_B^-(H(m))$
encrypted msg digest $K_B^-(H(m))$
large message m
Bob's public key K_B^+
digital signature (decrypt)
H: Hash function
H(m)
H(m)
equal ?

MAC = message digest with shared secret

Message Authentication Code



Bob sends msg and hash of msg+secret:

Alice verifies integrity and authenticity

No encryption algorithm is required

How to distribute *authentication key*?