Addendum: Message Authentication Code

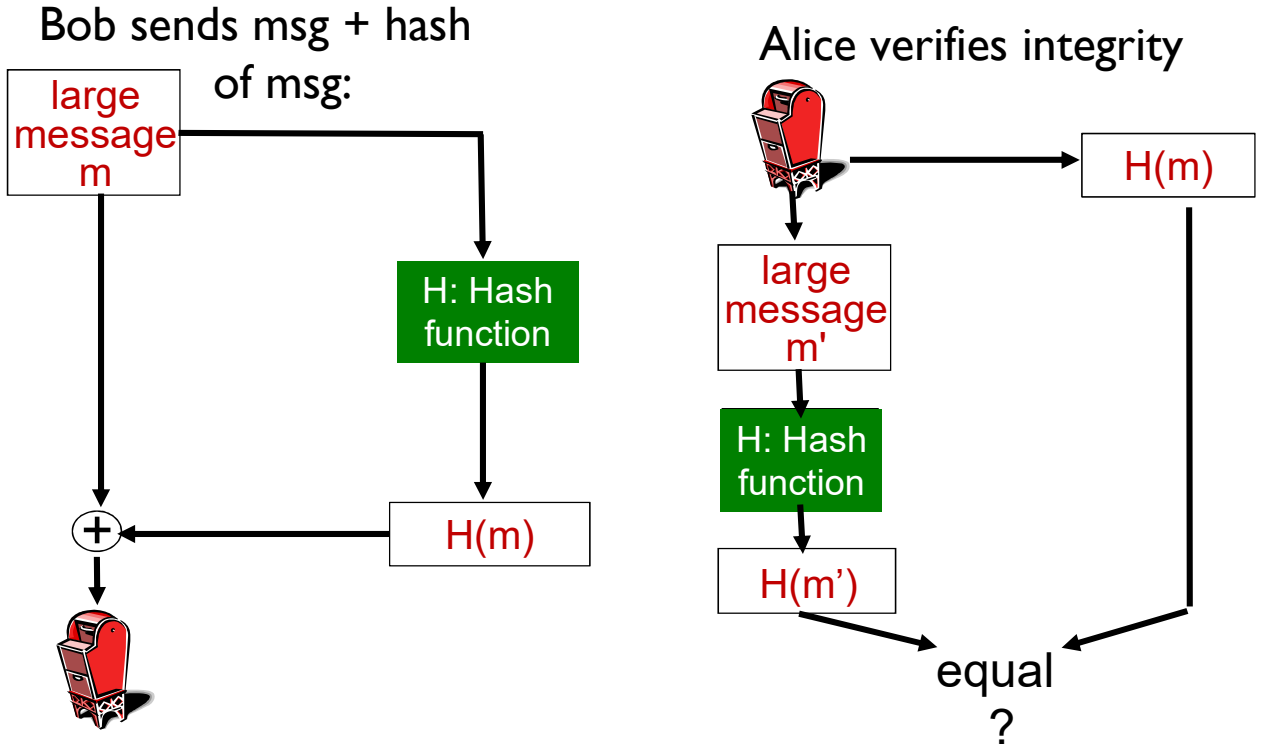
Context

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)



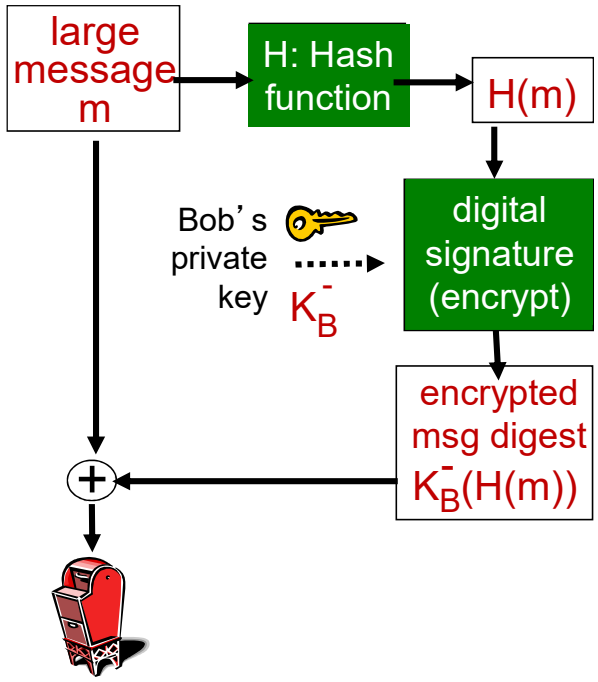
Think "Hash = Internet Checksum" or "CRC"

Addendum 8-2

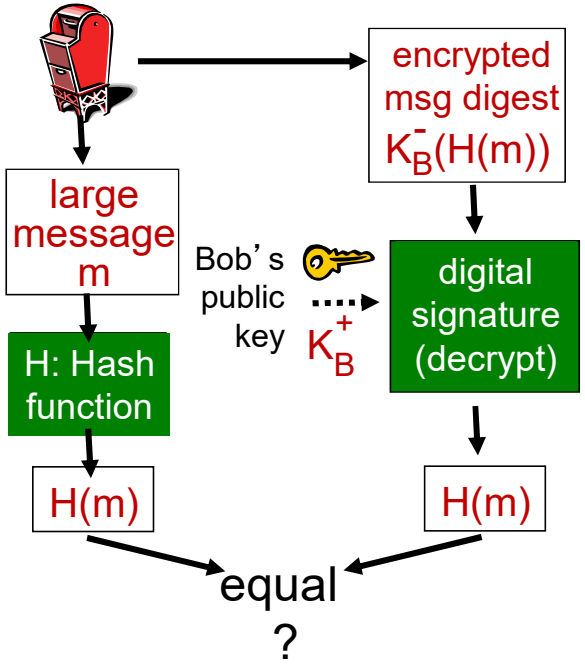
Review: Digital signature = signed message digest

Slide 8-49

Bob sends digitally signed message:



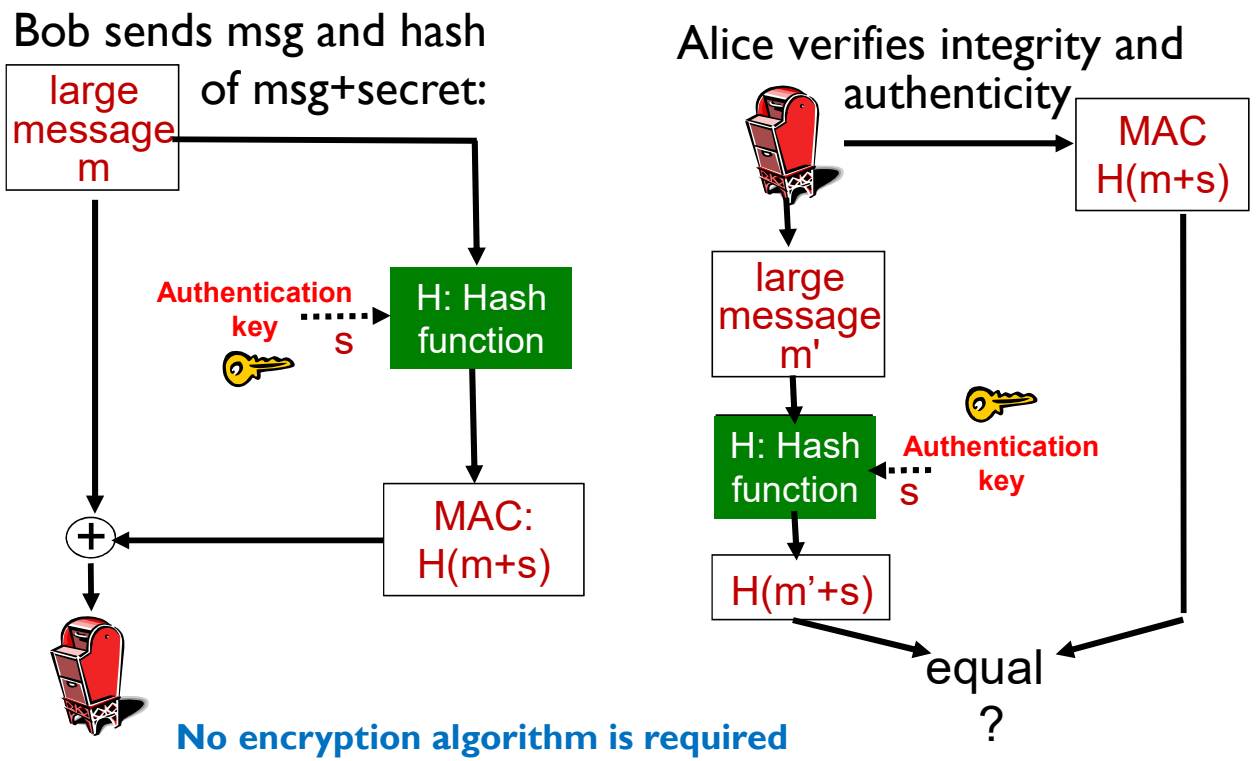
Alice verifies signature, integrity of digitally signed message:



Addendum 8-3

MAC = message digest with shared secret

Message Authentication Code



No encryption algorithm is required

How to distribute *authentication key*?

Addendum 8-4