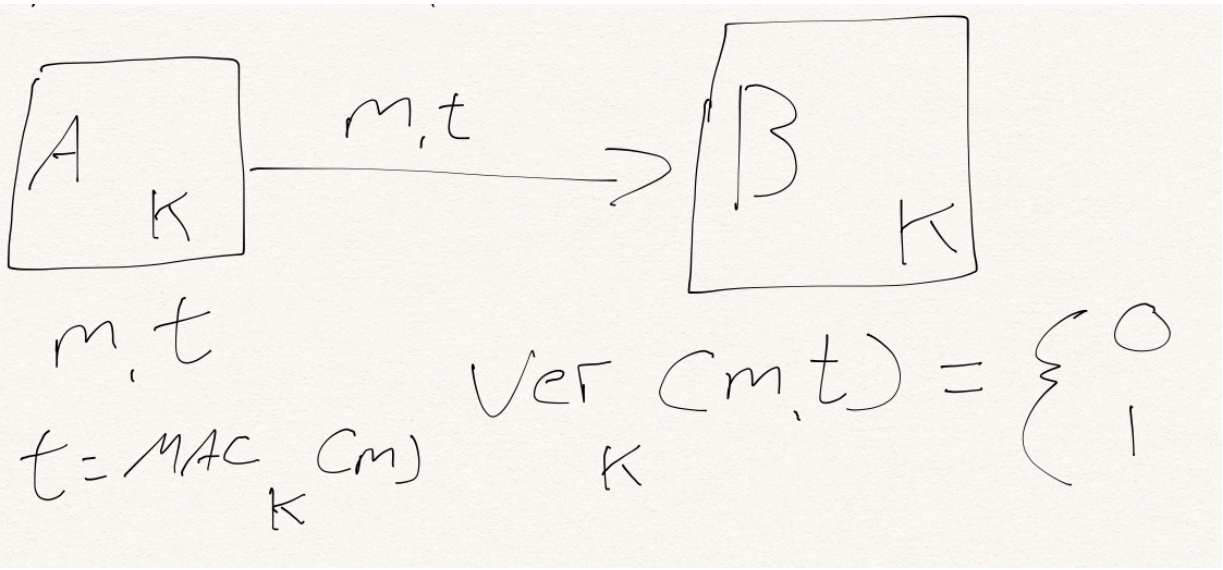
CS558 - Spring 2017
Lecture Notes for February 14th, 2017
Prepared by Brian Roach

Use MAC (Message Authentication codes) to protect against forged or tampered messages

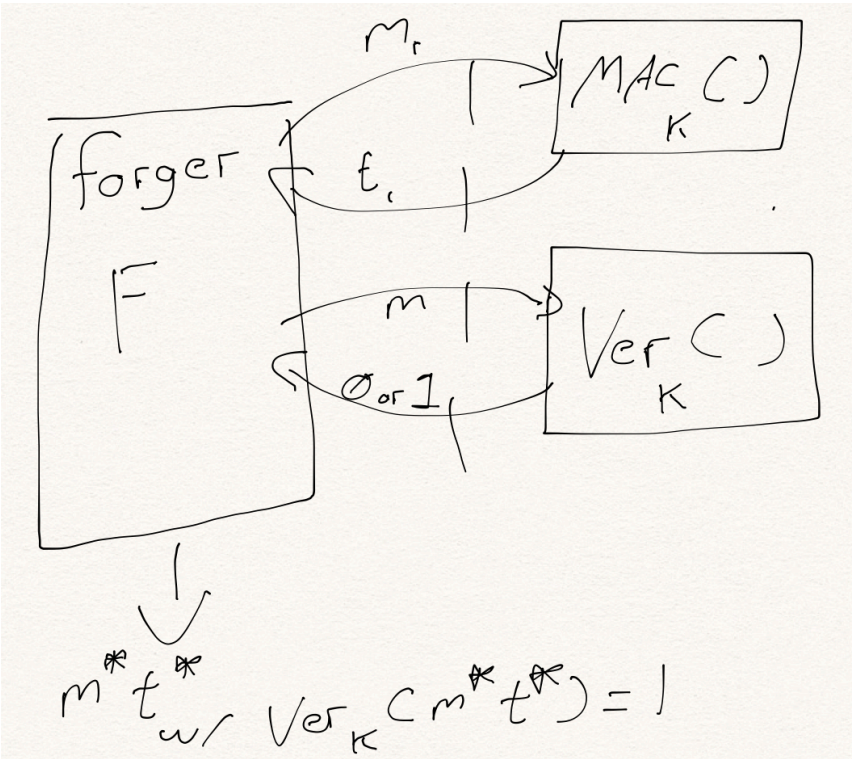
(MAC graphic)



Tags validate for message with key

(*Side Note:* MD5 is an awful MAC, don't ever use it)

(forger game graphic)

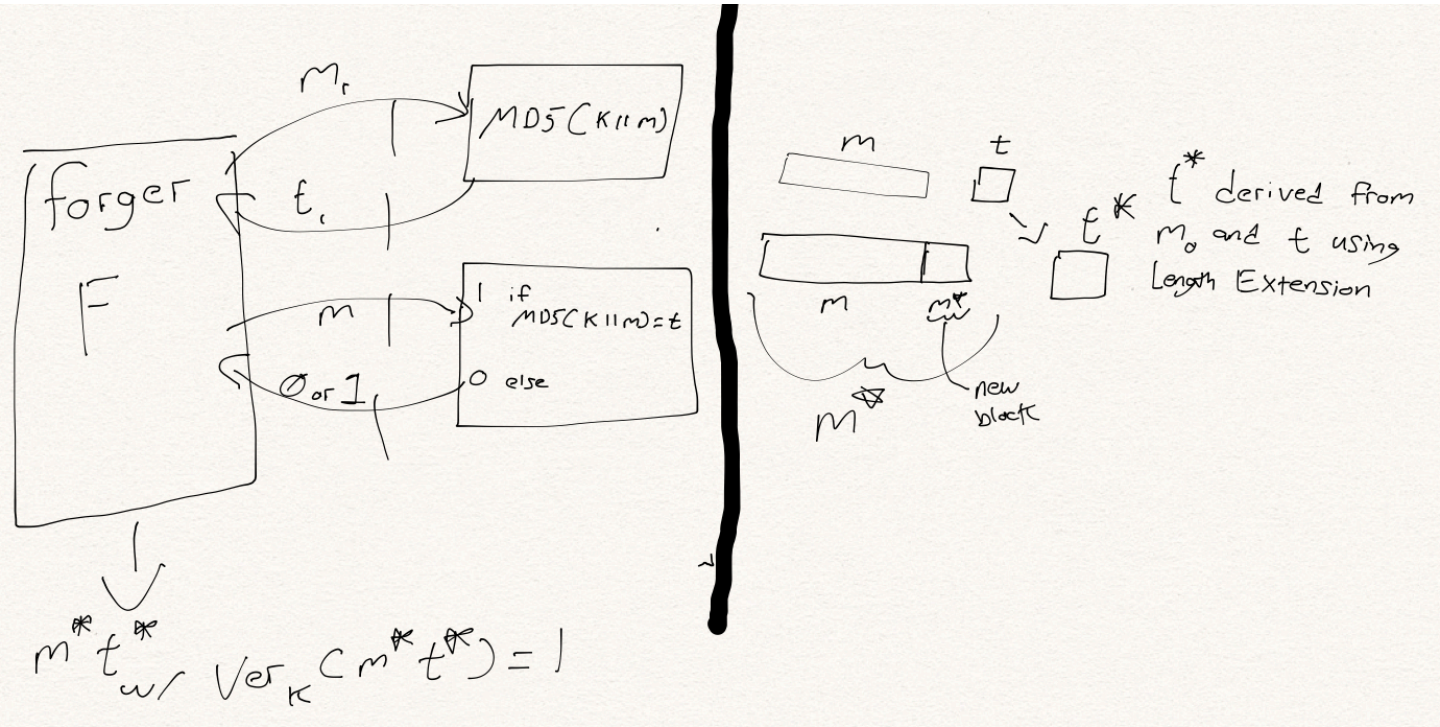


(Good MAC Scheme graphic)

$$PRF_K(m) = t$$

$$Ver_K(m, t) = \begin{cases} 1 & \text{if } PRF_K(m) = t \\ \text{else: } 0 \end{cases}$$

(MD5 as MAC graphic)

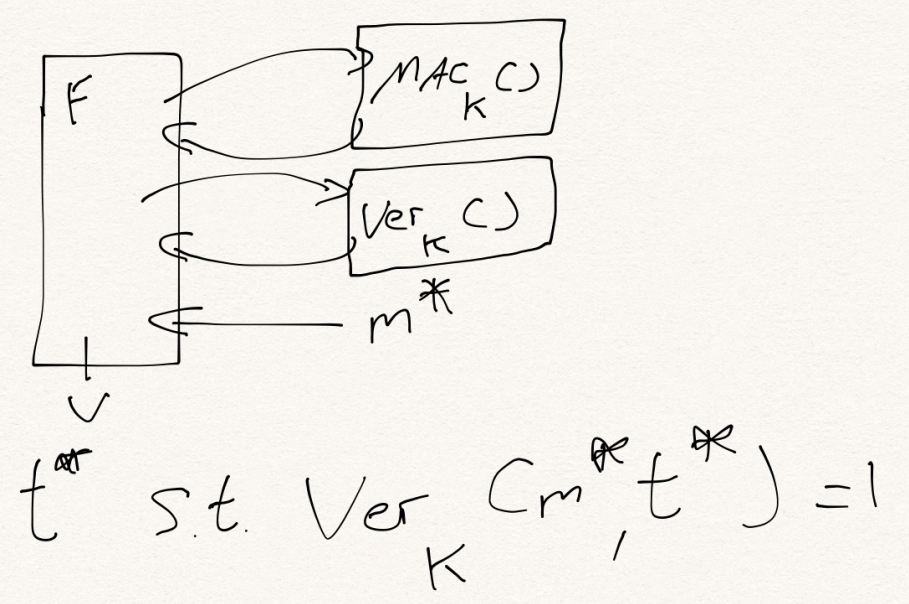


This is called Existential Forgery Against Chosen Message Attacks

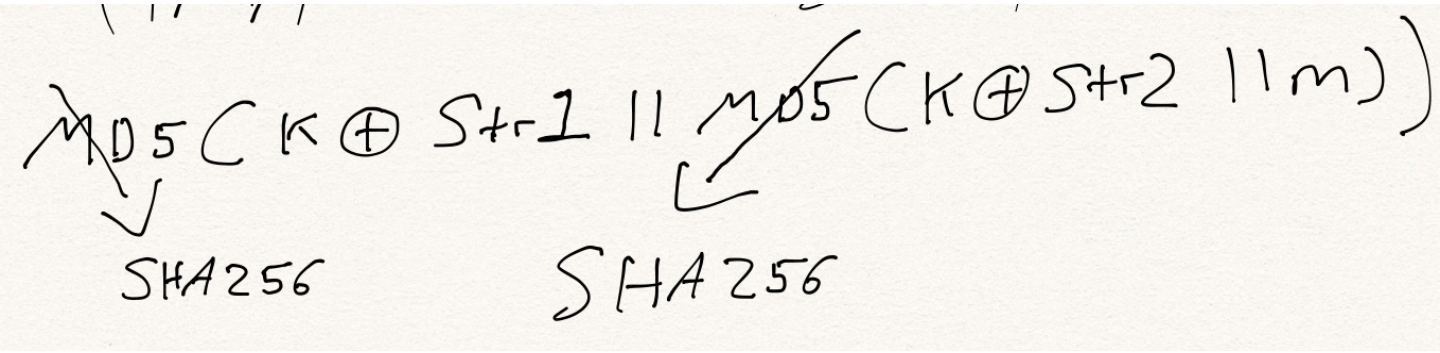
---

Known message scenario - not used in practice, just for reference

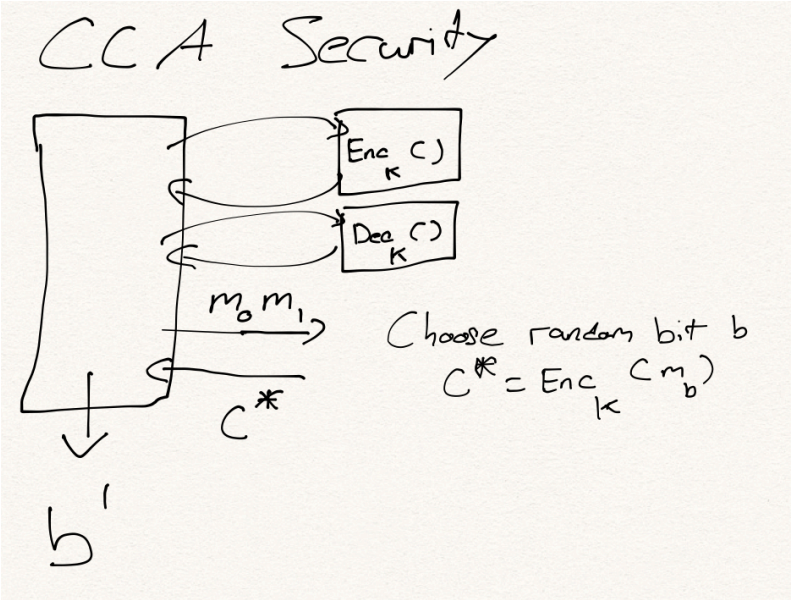
(known message graphic)



(HMAC MD5/ HMAC SHA graphic)

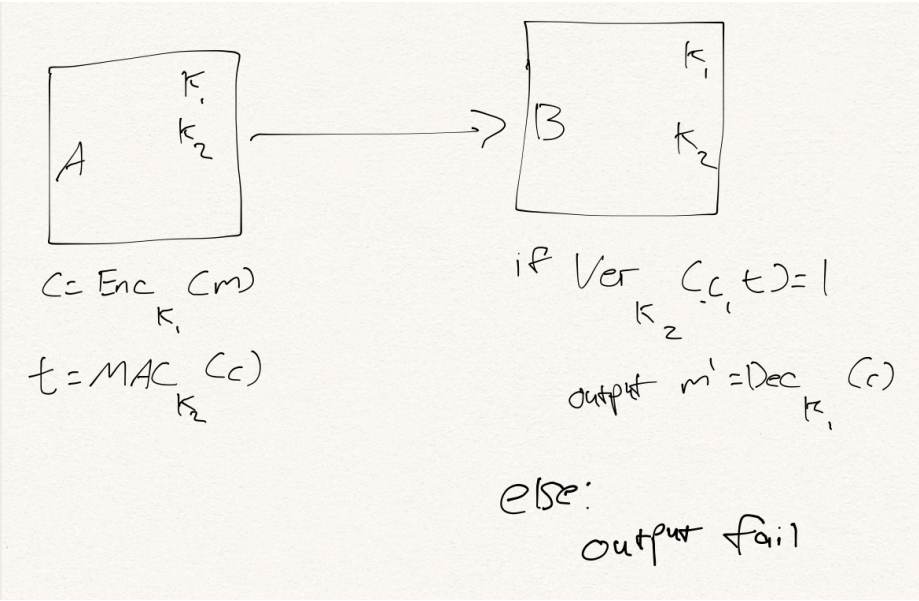


Necessity of MACing Messages
CCA-Security Compliance



(Note: CPA Secure **Is Not** CCA Secure)
To withstand the attack about (CCA), MACing the message is required

Let Enc, Dec be CPA secure
Let MAC, Ver be a secure msg auth (MAC)



In CCA, decryption oracle is useless, if not, implies adversary know t s.t. $ver_{k2}(c\ t) = 1$
& adversary cannot find t without k2

One such protocol is GCM (Galois Counter Mode), combines MAC and ENC to achieve CCA security