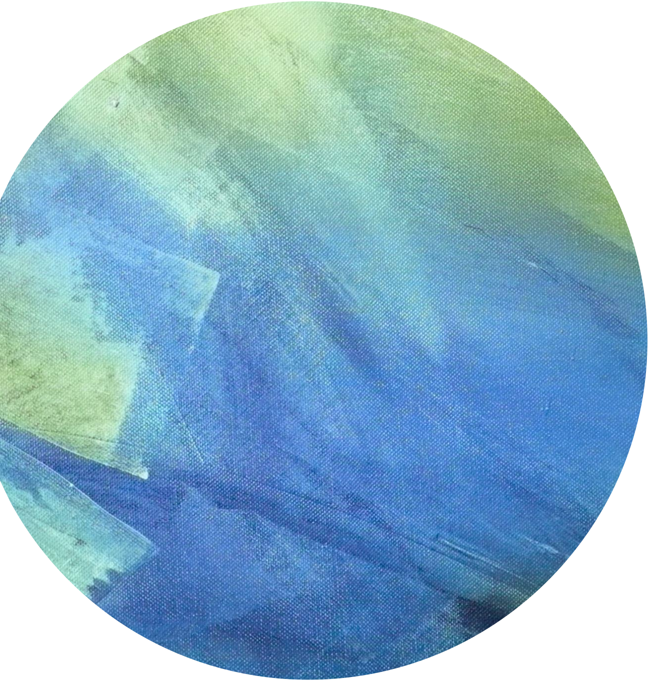
Lecture 9



Outline

Scribe : Ryan

~~Number Theory~~

~~Hard Problems~~

~~Key Exchange~~

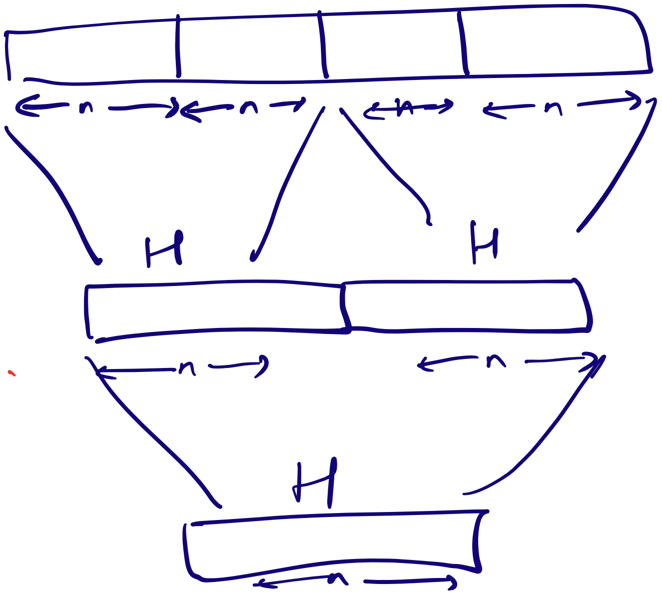
Collision Resistance

Domain extension

Given a hash function H: $\{0,1\}^{2n} \rightarrow \{0,1\}^n$, build a hash function $\cancel{H}$ G: $\{0,1\}^{4n} \rightarrow \{0,1\}^n$

I.

G :



Merkle tree

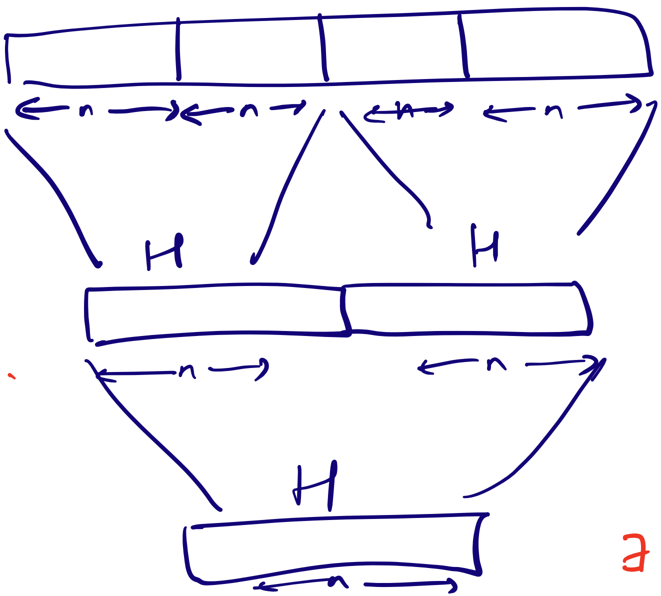
If H is C.R. then so is G.

Domain extension

Given a hash function H: $\{0,1\}^{2n} \rightarrow \{0,1\}^n$, build a hash function G: $\{0,1\}^{4n} \rightarrow \{0,1\}^n$

I.

G:



If H is C.R. then so is G.

Suppose G is not C.R.

$\exists\, A(G) \rightarrow x_1x_2x_3x_4 \neq x_1'x_2'x_3'x_4'$

s.t. $G(x_1x_2x_3x_4) = G(x_1'x_2'x_3'x_4')$

$\exists\, B^A(H) \rightarrow y_1y_2 \neq y_1'y_2'$ s.t.

$y_1 = H(x_1\ x_2)$ | $y_1' = H(x_1'\ x_2')$

$y_2 = H(x_3\ x_4)$ | $y_2' = H(x_3'\ x_4')$.

~~Claim: $(y_1\ y_2), (y_1'\ y_2')$ is a collision in H.~~

$H(y_1\ y_2) = H(y_1'\ y_2')$.

What if $\boxed{y_1 y_2 \overset{?}{=} y_1' y_2'}$.

Then $y_1 = y_1'$ and $y_2 = y_2'$.

$\Rightarrow H(x_1\ x_2) = H(x_1'\ x_2')$

$\boxed{\text{So } (x_1\ x_2), (x_1'\ x_2') \text{ is a collision}}$

or $(x_1\ x_2) = (x_1'\ x_2')$.

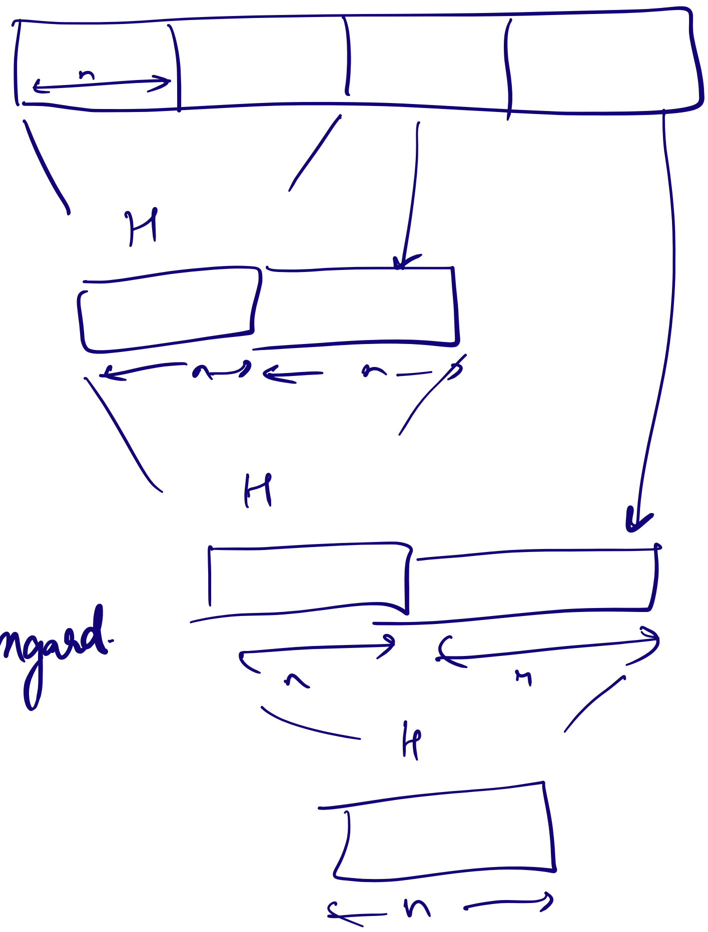
$\Rightarrow (x_3, x_4) \neq (x_3', x_4')$

$y_2 = H(x_3, x_4) = y_2' = H(x_3'\ x_4')$

$\boxed{\text{So } (x_3, x_4), (x_3', x_4') \text{ is a collision}}$

II.

G :

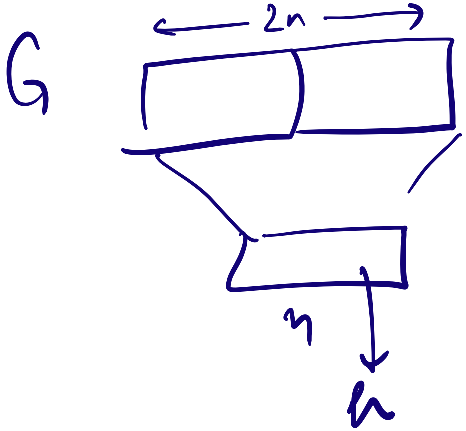


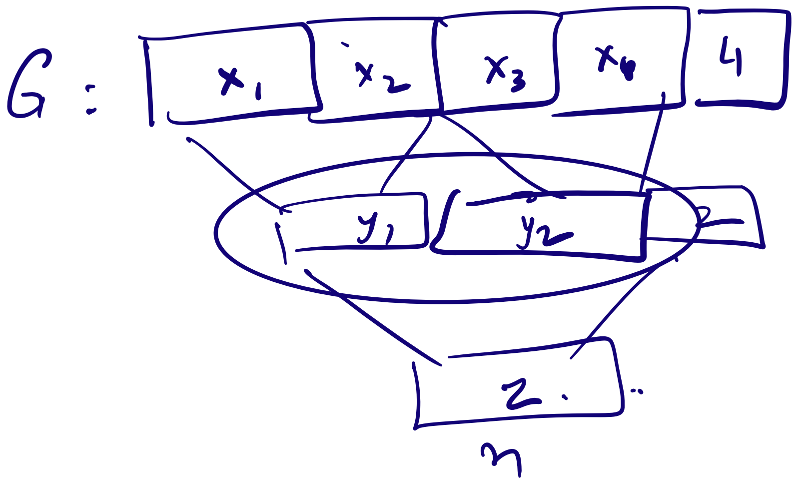
Merkle-Damgard.

Domain extension

Given a hash function H: $\{0,1\}^{2n} \rightarrow \{0,1\}^n$, build a hash function G: $\{0,1\}^{8n} \rightarrow \{0,1\}^n$

$G(x_1 x_2 x_3 x_4) = G(y_1, y_2)$ length of string





Domain extension

Given a hash function H: $\{0,1\}^{2n} \rightarrow \{0,1\}^n$, build a hash function ~~H~~ G: $\{0,1\}^{*} \rightarrow \{0,1\}^n$

n^c

Authenticated Symmetric Encryption

Recap: so far

Confidentiality: semantic security against a CPA attack

- Encryption secure against **eavesdropping only**

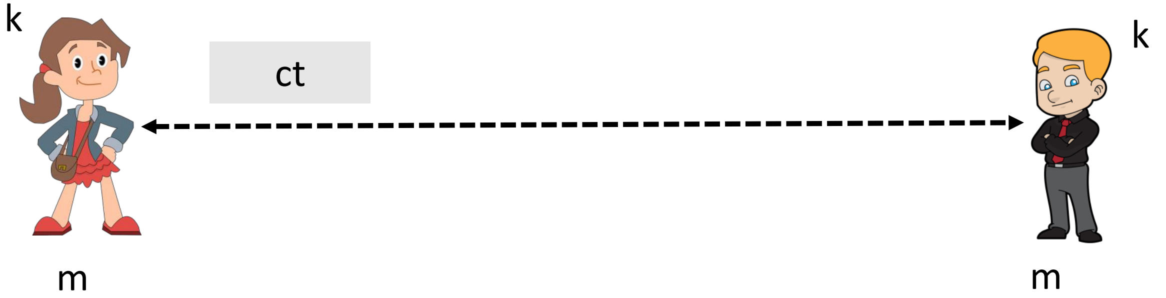
Integrity:

- Existential unforgeability under a chosen message attack EUF-CMA
- CBC-MAC, HMAC…

This module: encryption secure against **tampering**

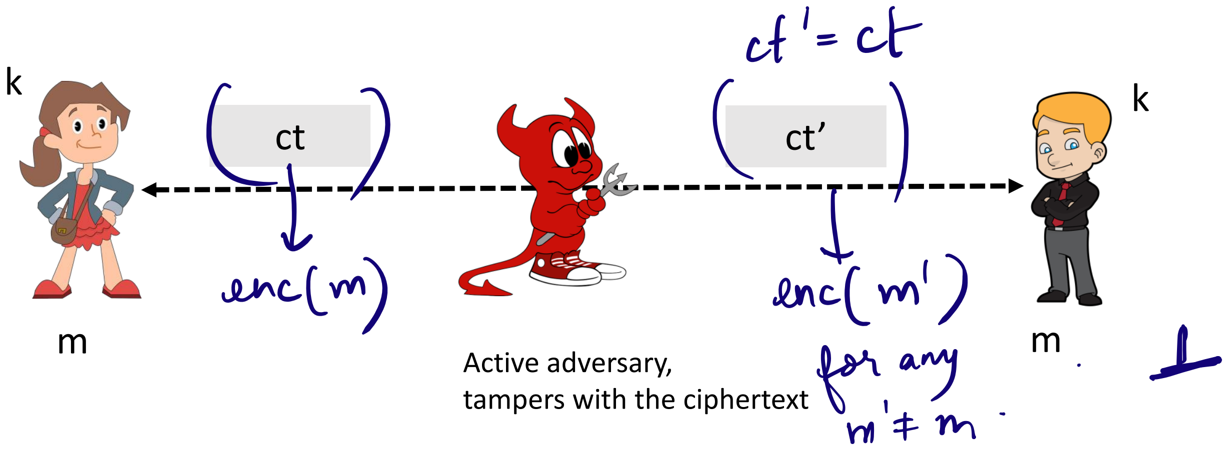
- Ensuring both confidentiality and integrity

Recap: Encryption



Authenticated

~~Recap:~~ Encryption



Authenticated Encryption

An **authenticated encryption** system (E,D) is a cipher where

As usual: $E: K \times M \times N \longrightarrow C$

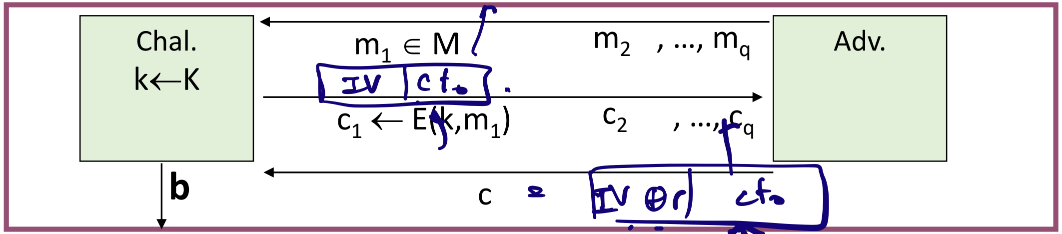
but $D: K \times C \times N \longrightarrow M \cup \{\perp\}$

Security: the system must provide

- sem. security under a CPA attack, and
- **ciphertext integrity:**
  attacker cannot create new ciphertexts that decrypt properly

Ciphertext Integrity

Let (E,D) be a cipher with message space M.



$\begin{cases} \mathbf{b}=1 & \text{if } D(k,c) \neq \perp \text{ and } c \notin \{c_1, \ldots, c_q\} \\ \mathbf{b}=0 & \text{otherwise} \end{cases}$

$m \oplus r$

$\Pr[c \notin \{c_1 \ldots c_q\} \text{ AND } D(k,c)=m \text{ for } m \neq \perp] = \text{negl.}$

Def: (E,D) has **ciphertext integrity** if for all "efficient" A:

$\mathrm{Adv_{CI}}[A,E] = \Pr[\text{Chal. outputs } 1]$ is "negligible."

Ciphertext Integrity

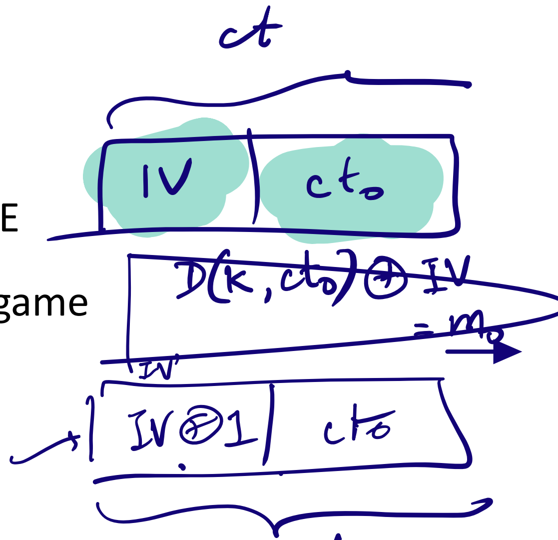
Def: cipher (E,D) provides **authenticated encryption (AE)** if it is

(1) semantically secure under CPA, and

(2) has ciphertext integrity

Bad example: CBC with rand. IV does not provide AE

- D(k,·) never outputs ⊥, hence adv. easily wins CI game



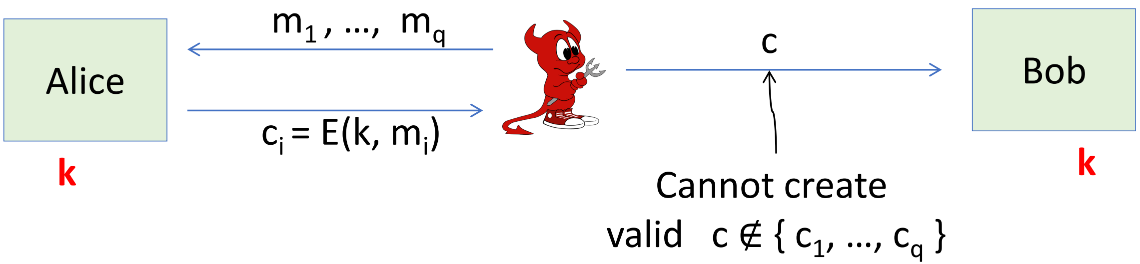
$(D(k, ct_0) \oplus IV \oplus 1)$

$= m_0 \oplus 1$

ct'

Implication 1: Authenticity

Attacker cannot fool Bob into thinking a message was sent from Alice



$\Rightarrow$ if $D(k,c) \neq \perp$ Bob knows message is from someone who knows k

(but message could be a replay)

Implication 2

chosen plaintext attack

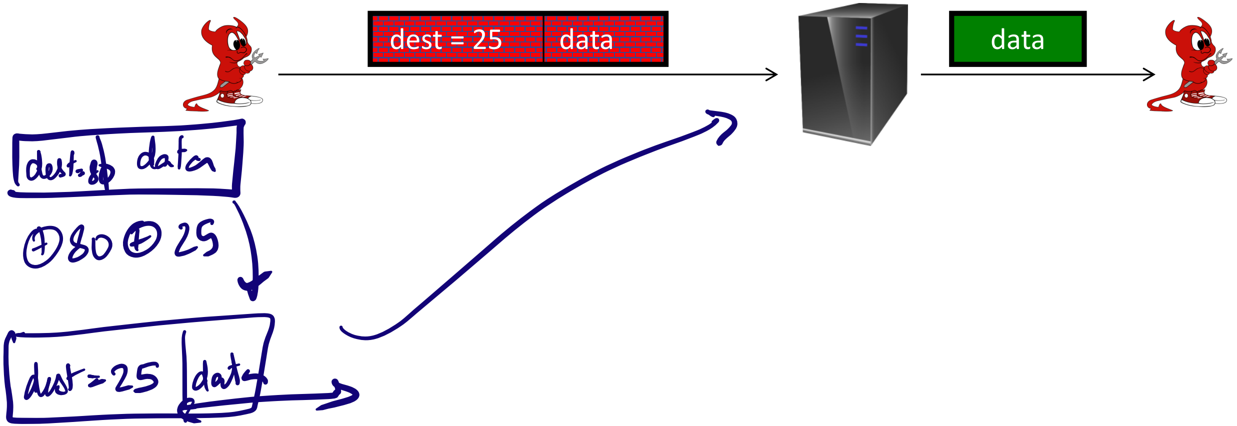
Authenticated encryption $\Rightarrow$

Security against **chosen ciphertext attacks**

Example Chosen Ciphertext Attacks

Adversary has ciphertext c that it wants to decrypt

- Often, adv. can fool server into decrypting **certain** ciphertexts (not c)



Chosen Ciphertext (CCA) Security

Adversary's power: both CPA and CCA

- Can obtain the encryption of arbitrary messages of his choice
- Can decrypt any ciphertext of his choice, other than challenge

(conservative modeling of real life)

Adversary's goal: Break sematic security

Chosen Ciphertext (CCA) Security: Definition

Chosen Ciphertext (CCA) Security: Definition

- **Example**: CBC with random IV is not CCA-secure

m_0, m_1 : $|m_0| = |m_1| = 1$

$c \leftarrow E(k, \mathbf{m_b}) = (IV, c[0])$

$c' = (IV \oplus 1, c[0])$

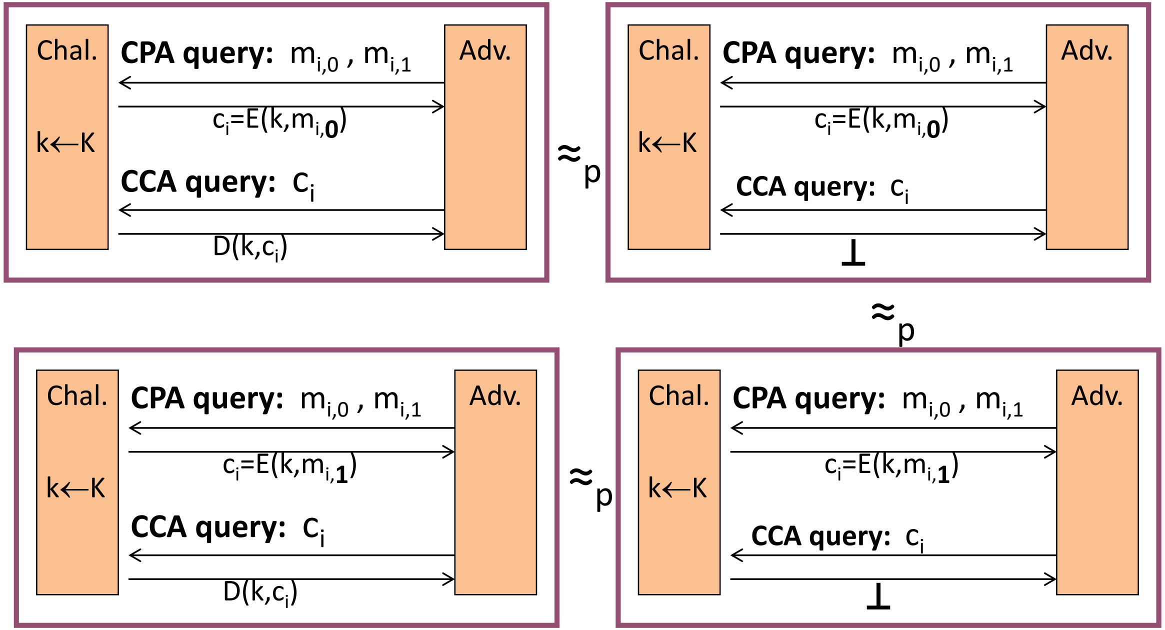
$D(k, \mathbf{c'}) = ?$

Authenticated Encryption => CCA Security

Thm: Let (E,D) be a cipher that provides Authenticated Encryption.
Then (E,D) is CCA secure!

Proof on next page..

Proof by pictures



So what?

Authenticated encryption:

- ensures confidentiality against an active adversary that can decrypt some ciphertexts

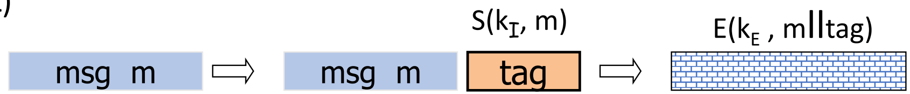
Limitations:

- does not prevent replay attacks
- does not account for side channels (timing)

Combining MAC and ENC (CCA)

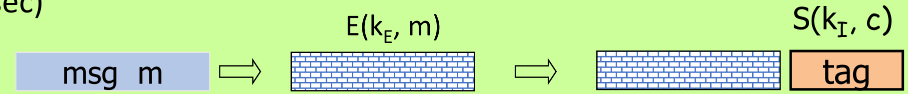
Encryption key k_E. MAC key = k_I

Option 1: (SSL)

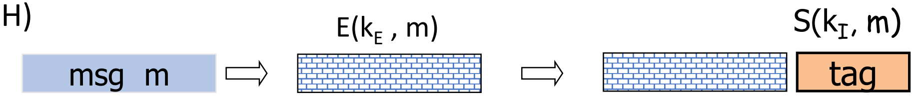


Option 2: (IPsec)

always correct



Option 3: (SSH)



Authenticated Encryption Theorems

Let (E,D) be CPA secure cipher and (S,V) secure MAC.

Then:

1. **Encrypt-then-MAC**: always provides A.E.

2. **MAC-then-Encrypt**: not necessarily A.E. or CCA secure

   However: when (E,D) is rand-CTR mode or rand-CBC
   M-then-E provides authenticated encryption