# Lecture 8: Authenticated Encryption

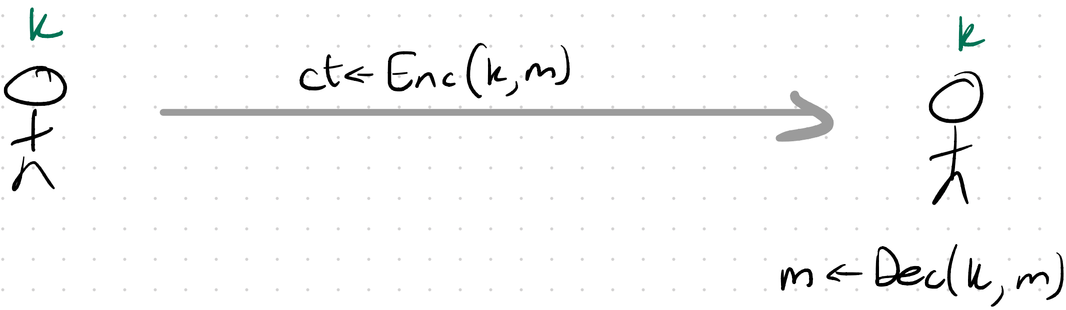

MIT - 6.1600
Fall 2023
Corrigan-Gibbs & Zeldovich

# Plan

→ Review: CPA Security
- Why CPA is insufficient
- Authenticated encryption
    * Encrypt then MAC
    * CCA security
- Recap of symmetric-key primitives

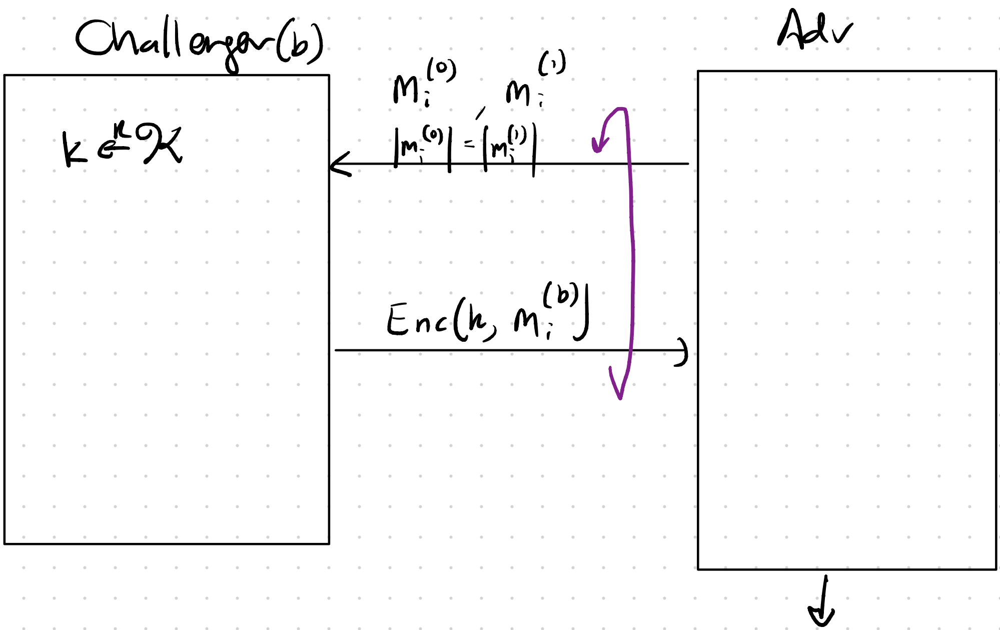
# Encryption with a shared secret

(Enc, Dec)



# Recap: CPA Security

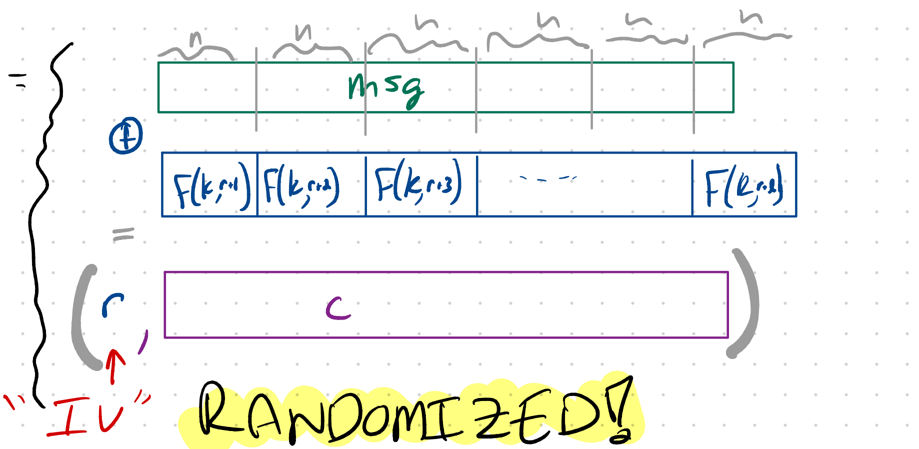
$Enc : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$




Enc scheme is CPA secure if no adv can distinguish world $b=0$ from world $b=1$. $b' \in \{0,1\}$

## CPA Secure encryption from PRF $F : \mathcal{K} \times [M] \to \{0,1\}^n$

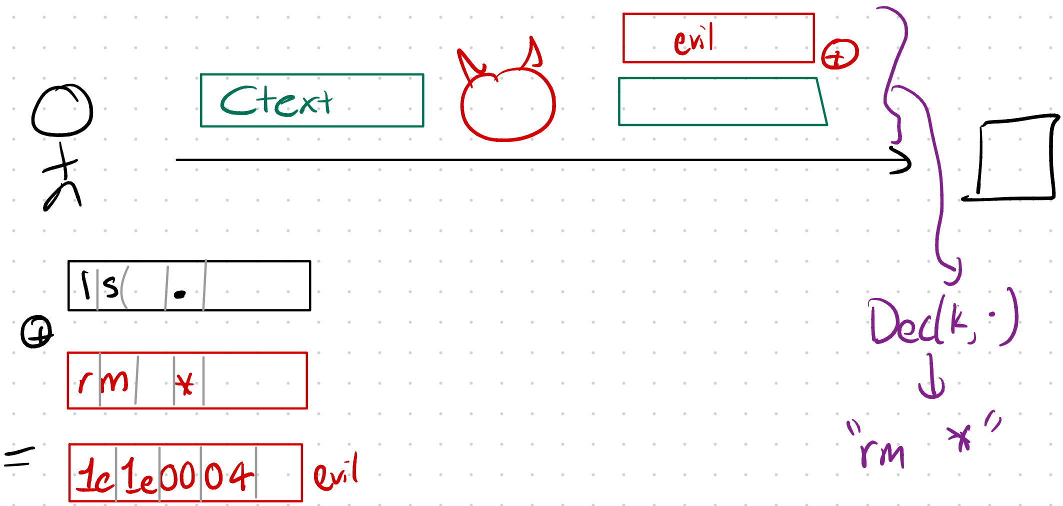
$Enc(k, m) :=$




Decryption essentially same as encryption.

# CPA Security is not enough.

Example: SSH server using CPA-secure enc




Key points

1) Adv can do lots of damage w/o learning encrypted msg

2) App-level failures (e.g. msg decrypts to garbage) can leak msg

How could A learn that failure occurred?

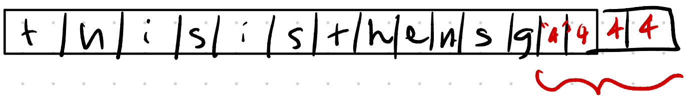
- * B could reply w/ msg of varying len
- * B could throw error
- * B could reply in diff time
- * B could perform other action

# Example: CBC Padding Oracle

* CBC is a "mode of operation" like AES-GCM
* Essentially deprecated
* Required msg to be padded to multiple of 128 bits/ 16 bytes

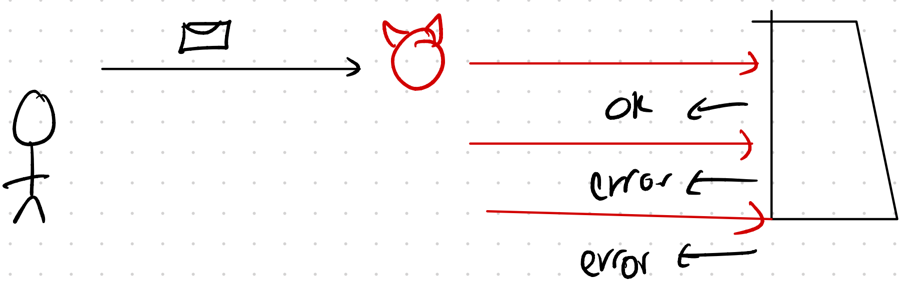
Simplified!

Last block

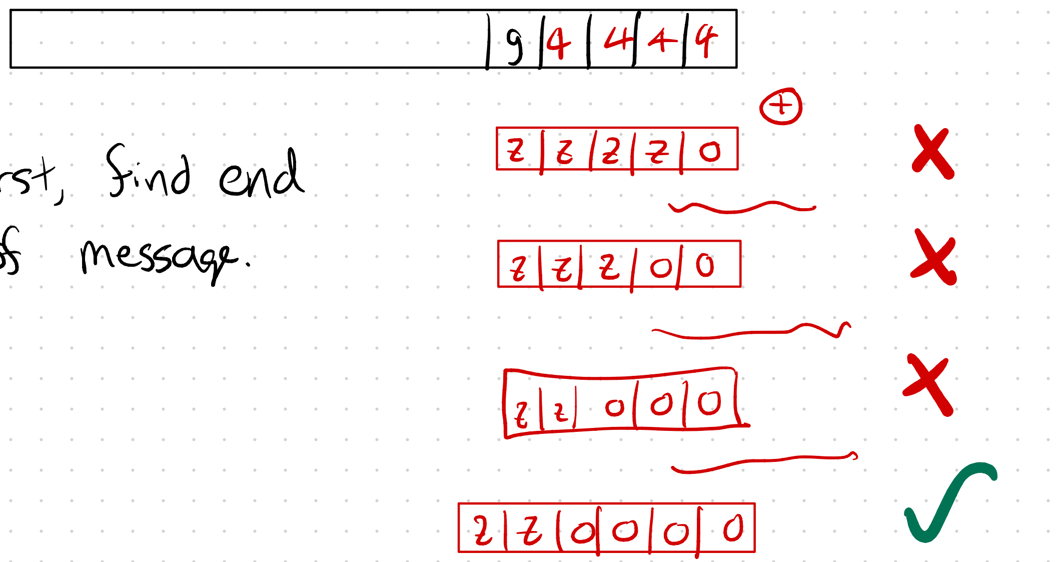



Put 4s in last bytes to indicate 4 padding bytes

In CBC mode, decryptor would
* decrypt ciphertext
* Check whether padding well formed
* If not, throw error

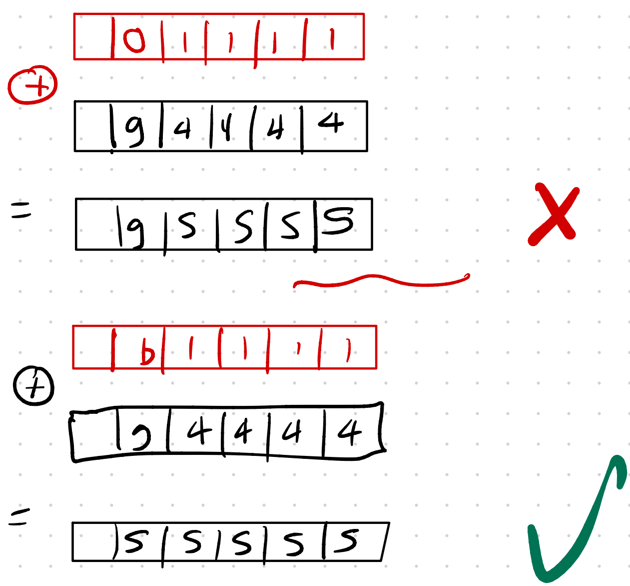



With a few queries per byte, can recover msg



First, find end of message.

Next, learn last byte.



**Problem:** Recipient acted on unauthenticated data.

# Authenticated encryption ("Gold standard" sec def)

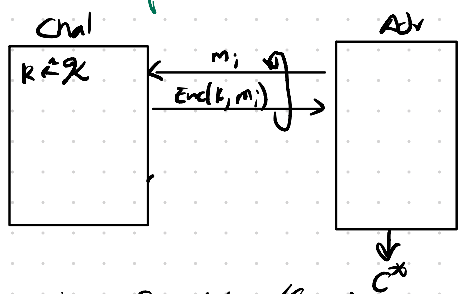
Syntax: (Enc, Dec) as before.
The type sig of decryption routine is now

$$\text{Dec}: \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M} \cup \underbrace{\{\perp\}}$$

= fail. no msg output

(Enc, Dec) is AE if:
1) Is CPA-secure and
2) Satisfies "ctext integrity"

{ Adv can't cook up new valid ciphertexts




Adv wins if
$c^* \notin \{c_1, \ldots, c_n\}$
and $\text{Dec}(k, c^*) \stackrel{?}{=}$ reject

Enc scheme has ctext integrity if $\forall$ eff advs A

$$\Pr[A \text{ wins ctext int. game}] < \text{"negl."}$$

AE Security $\Rightarrow$ CCA security. (strong)

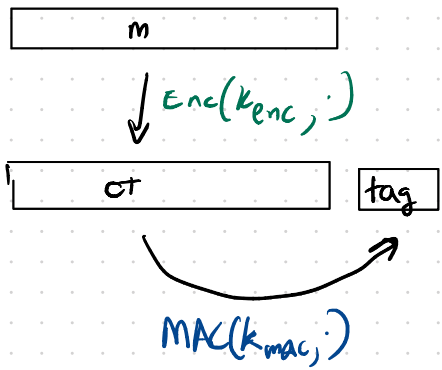
" $\Rightarrow$ Msg integrity

AE is "gold standard" for enc security.
↳ AEAD = AE + associated (auth but not enc) data

# Constructing AE schemes

"Encrypt then MAC" → As easy as it sounds

- Works with a "strong MAC" (Game 9.1 in Boneh-Shoup)
  - ↳ Given many $(m, t)$ pairs on chosen msgs hard to cook up a new valid $(m^*, t^*)$ pair.
- Independent keys for both parts (PRF)
- AES-GCM is standard
  CTR mode + GMAC
- ChaCha-Poly1305 is another




To decrypt:

1) Check MAC on ct first. If bad, FAIL.
2) Then decrypt.

(Don't even peek at msg before checking MAC.)

Sanity check: Why does enc-then-MAC provide ctext integrity?

* To get decryptor to decrypt, must produce new (ct, tag) pair
* Not possible by MAC security!

Encrypt-then-MAC is **the** safe way to combine enc & MAC

* AES-GCM ≃ AES-CTR then GMAC
* Also common = ChaCha20 + Poly1305 mac
* Well-designed crypto APIs handle this for you.

It's possible to construct AE directly from PRP (AES) — end of lecture

↳ OCB mode is one example

↳ Can be faster than generic encrypt & MAC (+ OCB is!)

↳ Why don't we use it? Sad story ☹

What do people often mess up?

- ✗ Same key for enc & MAC
- ✗ MAC doesn't cover whole ctext (e.g. IV)
- ✗ Provide data to application before checking MAC on entire ctext

# CCA Security

CPA-secure: Adv can see encryption of msgs of its choice
↳ What if adv can see decryptions?

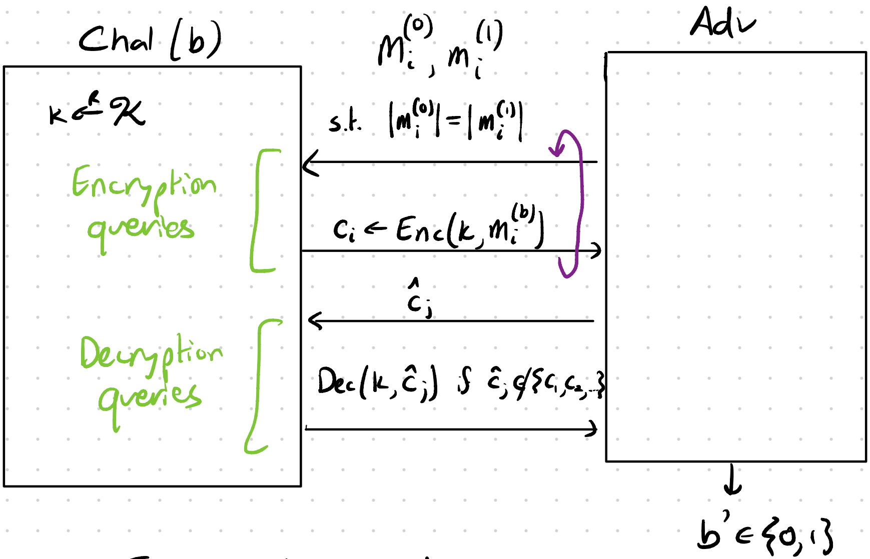
## Principle of CCA Sec Def:

- Adv shouldn't be able to dist enc of $m_0$ from $m_1$
- Even if it can ask for enc of many msgs of its choice

  AND

- Can ask for decryption of any ctext except answers to prior enc queries.

# CCA: Definition




Let $W_b$ = Event that adv outputs 1 in world $b \in \{0,1\}$

## CCA Security Defn

(Enc, Dec) is CCA secure if $\forall$ eff adv $A$ $\exists$ negl fn st.

$$\left| \Pr[W_0] - \Pr[W_1] \right| \leq \text{negl.}$$

Adv is very powerful here. AND adv's goal is very weak $\Rightarrow$ Strong security

↳ Strongest possible??? No...

## Sanity Check:

Why does CPA + Ctext integrity $\Longrightarrow$ CCA Security?

Idea: * Ctext integrity means that all decryption queries will output "fail"

* Then we're back to CPA game

* CPA says attacker can't win.

## CCA Observations

* CCA sec $\Rightarrow$ CPA sec $\Rightarrow$ CCA must be rand/stateful
* CCA cts cannot be "malleable" at all

$c^* \curvearrowright \hat{c}^*$ ask for dec of $\hat{c}^*$

# Bad Ideas

## MAC-then-encrypt

- ↳ Many many attacks (SSL)
- ↳ Basic idea: "padding oracle"

## Encrypt-and-MAC

- ↳ Used in SSH (old versions)

## Fundamental idea:

If enc scheme is CCA secure
secure adv cannot learn any
info on result of decrypting adv-chosen ct

MAC-then encrypt & encrypt-and-MAC don't
guarantee in general.

Before we leave symmetric-key crypto, I wanted to mention a few other concepts you might hear.

## So far

**OWF** $f: \{0,1\}^n \to \{0,1\}^n$

Given $y = f(x)$ s.t. $x \xleftarrow{R} \{0,1\}^n$
hard to find $x'$ s.t. $f(x') = y$.

**PRF:** $F: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

$F(k, \cdot)$ "looks like" a random fn from $\{0,1\}^n \to \{0,1\}^n$

**PRG:** $G: \{0,1\}^n \to \{0,1\}^{100n}$

Stretch a short random string into a long pseudo-random string.

$$\{G(s): s \leftarrow \{0,1\}^n\} \overset{c}{\approx} \{r: r \leftarrow \{0,1\}^{100n}\}$$

Can build from PRF $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

$$G(s) := \underbrace{\left(F(s,0) \,||\, F(s,1) \,||\, \cdots \,||\, F(s,99)\right)}_{\text{Pseudorandom by PRF Security}}$$

**PRP:** Pair $F, F^{-1}: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

s.t. (1) $F$ is PRF

(2) $\forall k \in \mathcal{K}\ \forall x \in \{0,1\}^n$

$$x = F^{-1}(F(k,x))$$

* AES is actually a PRP → why?
* N.B $F(k,\cdot)$ cannot have collisions!
* Use AES as PRF... okay until adv sees $2^{n/2}$ blocks → Birthday!

All equally powerful in theory terms...

THEORY

PRACTICE