Lecture: Encryption Intro

MIT - 6.5610

Spring 2023

Henry Corrigan-Gibbs

Plan

- Recap: PRF
- CPA Security [Weak encryption]
- CPA-secure encryption from PRF: Counter mode
- Pseudorandom permutation

Logistics

* Pset 1 out tomorrow.
  ↳ ONLY collab w/ pset grp
* We will assign pset groups tonight.

Recap: Pseudorandomness

OWF: Easy to compute, hard to invert

PRG: Stretch short random seed into long pseudorandom string

PRF: A keyed fn f s.t. $f(k,\cdot)$ "looks like" random fn when $k \xleftarrow{\$}$ keyspace.

[PRP]

A PRF is an eff. fn

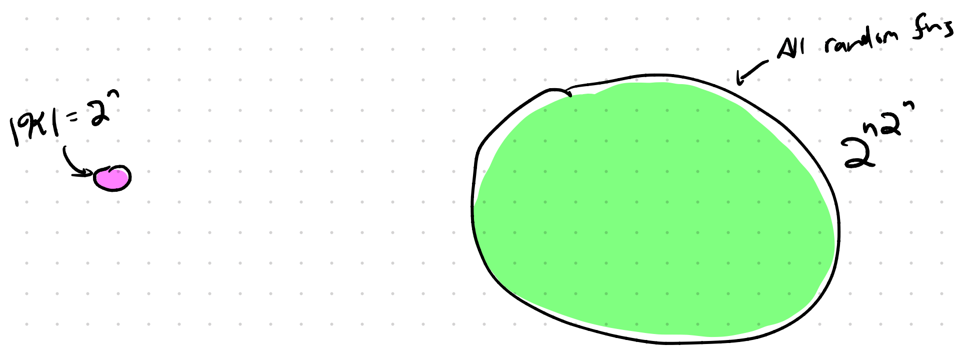
$$f : \mathcal{K}_n \times \{0,1\}^n \to \{0,1\}^n$$

Could be $\ell(n)$

s.t. $\forall$ eff adv $\mathcal{A}$, $\exists$ negl fn st.

$$\left| \underbrace{\Pr\left[\mathcal{A}^{f(k,\cdot)}(1^n)=1 : k \xleftarrow{\$} \mathcal{K}\right]}_{\text{Real world}} - \underbrace{\Pr\left[\mathcal{A}^{R}(\overset{???}{1^n}) = 1 : R \leftarrow \mathrm{Funs}_n\right]}_{\text{Ideal world}} \right| \le \mathrm{negl}(n).$$

$= \mathrm{PRFAdv}[\mathcal{A}, f]$.



[Q: Is PRF still pseudorandom if Adv gets 1 bit of key?]

Counter Mode

PRF $\Longrightarrow$ One-time (comp. sec.) enc w/ short key

* won't define

PRF $\quad f : \mathcal{K} : \{0,1\}^n \longrightarrow \{0,1\}^n$

$\mathrm{Enc}(k, m) :=$

$m =$ [ ]

$\oplus$

$f(k,0)$	$f(k,1)$	$f(k,2)$	$f(k,3)$	. . . . .

$=$

[ct]

Bonus: Parallelizable!

$\mathrm{Dec}(k, c) := c \oplus [\, f(k,0) \| \cdots \,]$

Idea:

If adv can distinguish

$\mathrm{Enc}(k, m_0)$ from $\mathrm{Enc}(k, m_1)$

can break PRF

Weaknesses of the one-time pad

* Long key ← PRF
* One ct per key ← Today
* Adv can tamper w/ ct ← Next time

Goal: Enc scheme secure if adv can see many msg encrypted with same key.

↳ NO Integrity protection (next time)

Applications:

* File encryption
* Some Internet protocols

⋮

Our security defn is going to consider strong adv:

* gets enc of many msg of its choice] why?
* just has to dist enc of m_0, m_1 (chosen)

"IND-CPA security"

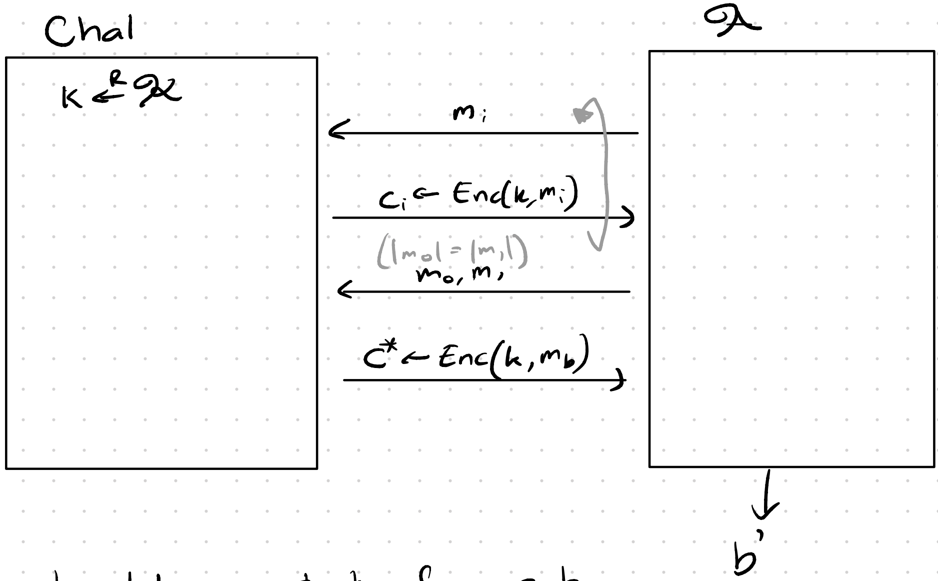
Historical example:

Give msg to embassy, ask to relay to home gov't

⇒ Enc of chosen msg!

CPA Security

For an enc scheme (Enc, Dec) over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, define game:



Let W_b = output of game b.

We say (Enc, Dec) is CPA-secure if $\forall$ eff advs $\mathcal{A}$: $\exists$ negl fn s.t.

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

If we want to be fully precise, parameterize everything by security parameter "n" or "λ"

Weak: * What if adv can't see decryption of chosen ct?
* Tamper w/ msg?

CPA-Secure Enc must be randomized!

Intuition:

* Think about SSH — encryption of 8-bit chars.

  p a s s w o r d

  ↳ Need to defeat freq attack

Concretely, show attack in CPA game.

* Even WEAK encryption requires randomness!

  ↳ Obvious? Or very non-obvious?

  (GM '84)

CPA-Secure Enc from PRF.

* Let (Enc, Dec) over $\mathcal{K}, \mathcal{M}, \mathcal{C}$ be a one-time (perfectly) secure enc scheme.

* Let $f : \mathcal{K}' \times \{0,1\}^n \to \mathcal{K}$ be a PRF

Then

$\mathrm{Enc}'(k', m) :=$

$$x \xleftarrow{R} \{0,1\}^n$$
$$k' \leftarrow f(k, x)$$
$$\text{output } (x, \mathrm{Enc}(k, m))$$

$\mathrm{Dec}'(k', (x, c)) :=$

$$k' \leftarrow f(k, x)$$
$$\text{output } \mathrm{Dec}(k', c)$$

Show instantiation w/ one-time pad.
↳ Still malleable!

Adv breaking Enc' breaks either Enc or PRF f.

(See Boneh-Shoup Thm 5.2)

Thm: For all CPA adv $\mathcal{A}$ making Q CPA queries, $\exists$ PRF adv $\mathcal{B}$ s.t.:

$$\mathrm{CPAadv}[\mathcal{A}, \mathrm{Enc}'] \leq \frac{Q^2}{2^n} + 2 \cdot \mathrm{PrfAdv}[\mathcal{B}, f]$$

PRP ("Block cipher")

* Used to be dominant, ... less so now

$P: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

$P^{-1}: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$

Correctness: $\forall k \in \mathcal{K} \ \forall x \in \{0,1\}^n$

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

Pseudorandomness

Same as PRF except that adv gets oracle access to $P(k,\cdot)$ $P^{-1}(k,\cdot)$. Cant dist from $\Pi(\cdot)$, $\Pi^{-1}(\cdot)$ for $k \xleftarrow{R} \mathcal{K}$, $\Pi \xleftarrow{R} \text{Perms}[\{0,1\}^n]$.

* People thought you needed to "encrypt" & "decrypt"
  ↳ PRF-based constructions simpler, faster (many core)

Still, important b/c NIST-standardized ciphers are PRPs:

- DES (1975) $|\mathcal{K}| = 2^{56}$ $n = 64$
- 3DES $|\mathcal{K}| = 2^{168}$ $n = 64$
- AES (1998) $|\mathcal{K}| \in \{2^{128}, 2^{192}, 2^{256}\}$ $n = 128$

N.B. DES key size is far too small.

in U.S. SECRET: AES-128/192/256
TOP SECRET: AES-192/256 } Algs are public!

Things to know about PRPs

- NEVER use directly to encrypt ("ECB mode") → Not even CPA secure
- CPUs have HW support for AES (GBs per second) (AES-NI)
- Can use as a PRF, as long as you don't use too much

"PRF Switching Lemma" (see Boneh-Shoup)

Let $P: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a PRF

Then for any PRP adv $\mathcal{A}_{PRP}$, $\exists$ PRF adv $\mathcal{A}_{PRF}$ s.t.

$$|\mathcal{A}_{PRP} - \mathcal{A}_{PRF}| \leq \frac{q^2}{2^{n+1}}.$$

Intuition:

- Collisions in outputs is only diff b/w PRF & PRP
- Until $q \simeq 2^{n/2}$ will not expect to see collisions by Birthday paradox.
- After that, can distinguish!

→ Very common to use AES in counter mode ("AES-GCM" later on)

What about 3DES???