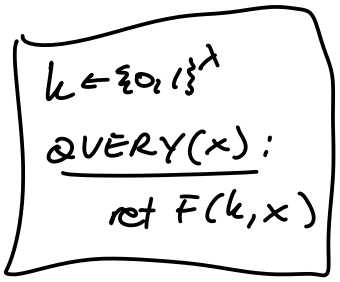
CCA: WTF?

PRFs are useless because I can only evaluate it on x chosen by Adversary, not the input I want

EVEN IF Adv chooses inputs to PRF, outputs look random

(of course they still look random when Adv doesn't control inputs)



Adv's perspective

CPA security is useless because I am only allowed to encrypt one of 2 possible plaintexts

Even if Adv has narrowed down ptxt to just 2 possibilities, ctxt doesn't help determine which ptxt was used

CCA security is useless because I'm not allowed to decrypt what I encrypted

seeing what's inside every OTHER ctxt in the world doesn't help you know what's inside this ctxt

(of course, if Adv learns only partial info about contents of other ctxts, it won't help)

Analogy: If I open any locked box in the world except for this special one, you won't know what's inside special box

Padding Oracles

Adv got partial info about contents of other ctxts (whether valid padding)

Attack:

$\underline{Enc(k,m):}$
$r \leftarrow \{0,1\}^\lambda$
ret $(r,\ F(k,r) \oplus m)$

} CPA secure
not CCA secure

Malleability

I give you ciphertext (r,s) that encrypts (unknown) m

$$Dec(r,s) = F(k,r) \oplus s = m$$

flip some bits in s (XOR s w/ any chosen x)

$$Dec(r, s\oplus x) = F(k,r) \oplus (s \oplus x)$$
$$= (F(k,r) \oplus s) \oplus x$$
$$= m \oplus x$$

As an attack:

request encryption of m_L or m_R
get back (r,s)
flip some bits in s to get new ctxt $(r, s\oplus x)$
Since $(r, s\oplus x) \neq (r,s)$, library will decrypt it happily
result of $Dec(r, s\oplus x)$ is either $m_L \oplus x$ or $m_R \oplus x$

$\Rightarrow$ solve for m, to know which library it is