Quiz 9/24

(1) Suppose a blockcipher E is a PRF. Does PRF security necessarily hold if the key to E is set such that the first half of the bits are zero's? NO

(2) CTR-$ generates a "pseudo one-time pad" YES

(3) If F is a PRF, then for random K, from $F_K(x)$ it is hard to guess the first bit of x. YES

and random x

(4) A mode of operation specifies how to use a blockcipher to encrypt large amounts of data. YES

(5) If F is a PRF, then necessarily given $F_K[K]$ for random K it is hard to recover K. NO

KDM

G* is a counter example

assume

$\rightarrow E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$

define

$E' : \{0,1\}^{2k} \times \{0,1\}^n \rightarrow \{0,1\}^n$

$\rightarrow E'_{K_1 \| K_2}(x) = E_{K_1}(x)$

$00 \ldots 00$

---

guesses better than 1/2

Let A be the first-bit-guesser.

Define PRF adversary

$B^{Fn(\cdot)}$

$x \xleftarrow{\$} \{0,1\}^n$

$y \leftarrow Fn(x)$

$b \leftarrow A(y)$

If $b = x[1]$ ret 1

Else ret 0

Let $G : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a PRF. Define $G' : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$

$\rightarrow G'_K(x) = \begin{cases} G_K(x) & \text{if } x \neq K \\ K & \text{O.W.} \end{cases}$

Suppose A is a PRF adversary against G'. Then define B against G:

Adversary $B^{Fn(\cdot)}$

Run A

When A makes query x do:

If x is the key halt & ret 1

Else ret Fn(x)

Until A outputs b

Ret b