Homework #4

1. (a) Clearly not PRG

(b) By definition is [illegible] type of Output length

(c) input size = output size

(d) input size < output size

$F_x(0,..0)$ ← effectively choose random string

2. $F_k(x) = G_0(k) \oplus x$, $G_0(s)$ is PRG

$G_0(s)$ truncates $G(s)$ to first n bits

$D^G(1^n)$

1. Compute $O^D(0^n) = y_0$ $O^D(1^n) = y_1$

2. Return 1 if $y_0 \oplus y_1 = 1^n$

OW return 0

Determine $\Pr(D(r)=1)$, $\Pr(D(G_K(s))=1)$

Determine $\Pr[D^{F_n}(1^n)=1]$, $\Pr[D^{f_n}(1^n)=1$

$\Pr[D^{F_n}(1^n)=1]$

- $F_n(0^n) = G'(K) \oplus 0^n = y_0$

- $F_n(1^n) = G'(K) \oplus 1^n = y_1$

- $y_0 \oplus y_1 = 1^n$

$\Rightarrow \Pr[D^{F_n}(1^n)=1] = 1$

$\Pr[D^{f_n}(1^n)=1] = 1/2^n$

~~$f_n(0^n) = G(K) \oplus$~~ ×

f_n maps 1^n to $\frac{1}{2^n}$ different elements

$\downarrow$

$\frac{1}{2^n}$

$f_n(0^n) \oplus f_n(1^n) = 1^n$

$y_0 \oplus y_1 = 1^n$

$y_1 = y_0 \oplus 1^n$

#4 ① $Dec_K(C) = F_K^{-1}(C) = r|m$

mins r

② Suppose F is a truly random permutation

$\tilde{\Pi} = (\tilde{Gen}, \tilde{Enc}, \tilde{Dec})$ except F_K

is a uniform function from $Auto_n$

$$Pr\left[PrivK^{CPA}_{A,\tilde{\Pi}} = 1\right] \leq \frac{1}{2} + \frac{q(n)}{2^{n/2}}$$

Case 2.

r is never used by oracle

F is chosen uniformly

Prob $m_b = \tilde{C}_1$ or $m_1 \Rightarrow \tilde{C}$

is $1/2$

Let $\tilde{C}$ be challenge ciphertext

Case 1 If r is used by oracle at least once.

- $C' = F_K(r|m') \longmapsto F_K^{-1}(C') = r|m) \mapsto r$
- r can be used to obtain m_0, m_1 in PrivK
- A makes $q(n)$ queries and r is chosen with $\frac{q(n)}{2^{n/2}}$