SACHIN GOYAL
150020069

Q4. G_1 is a PRG. ~~There is no Discriminator D such that~~

$\Rightarrow Pr[D(r)=1] - Pr[D(G_1(s)=1)]$ ≤ negligible.
for all Discriminators D.

$G_1(s) = G(s_1 s_2 \ldots s_{|s|-1}) \| s_{|s|}$

~~* Assume $G_1(s)$ is not a~~

Now $G_1(s\|b) = G(s)\|b$ — (1) b is a random bit.

~~* Since G_1 is a~~

* Assume $G_1(s)$ is not pseudo random generator
$\Rightarrow$ There exists D_1 for G_1 such that

$Pr[D_1(r)=1] - Pr[D_1(G_1(s))=1] > (n)^{-k}$ — (2)

(assuming probabilistic polynomial time (PPT) adversaries).

Main → Let us construct a subroutine for D.

~~$D_2(r) = D_1(r\|b)$ where b is a random bit~~

Subroutine $D(r) = D_1(r\|b)$ where b is a random bit

$$\therefore \Pr[D(r)=1] - \Pr[D(G_1(s))=1]$$

$$= \Pr[D_{n+1}(r\|b)=1] - \Pr[D_{n+1}(G_1(s)\|b)]$$

$$= \Pr[D_{n+1}(r')=1] - \Pr[D_{n+1}(G_{1,n+1}(s\|b))]$$

[since $G_{1,n+1}(s\|b) = G_1(s)\|b$]

$$= \Pr[D_1(r')=1] - \Pr[D_1(G_1(s'))]$$

From our assumption of G_1 not being PRG (eqn ②)

$$\Pr[D_1(r')=1] - \Pr[D_1(G_1(s'))] > (n+1)^{-k}$$

$$\Rightarrow \Pr[D(r)=1] - \Pr[D(G_1(s))=1] \geq (n+1)^{-k}$$

not negligible.

$\Rightarrow$ CONTRADICTION

$\Rightarrow$ WRONG ASSUMPTION

$\therefore$ G_1 is a pseudo random generator

Q1

Encryption is perfectly secret if

i $Pr[C=c \mid M=m_i] = Pr[C=c \mid M=m_j]$

$\forall\ i,j \quad i \neq j$

$Enc_K(m) = (K+m) \bmod 5$

① take $m=0$

$c=0$ for $K=0$ & $K=5$

$\therefore Pr[C=0 \mid M=0] = 2/5$

② take $m=2$

$\therefore c=0$ for $K=3$

$\therefore Pr[C=0 \mid M=2] = 1/5$

$\therefore Pr[C=0 \mid M=0] \neq Pr[C=0 \mid M=2]$

NOT A PERECTLY SECURE

Q2 Again $Pr[C=c \mid M=m_i] = Pr[C=c \mid M=m_j]$

$\forall\ i,j \cdot i \neq j$

Let $l=2$ $c=11$

① $Pr[C=11 \mid M=00] = \frac{1}{4}$ $K=11$

$Pr[C = 11 \mid M = 01] = 0$ because $K = 10$ Not Valid

$\therefore$ Not perfectly secure

Q3 negl₁ is negligible

$\Rightarrow$ $negl_1(n) < \frac{1}{K(n)}$ $\forall$ $n > N$ where $K(n)$ is some polynomial

let $negl_1(n) < \frac{1}{h(n)\,q(n)}$ $\forall\, n > N$

where $q(n)$ is some positive polynomial.

$\rightarrow negl_2 = h(n)\, negl_1(n)$

$\rightarrow negl_2(n) < \frac{h(n)}{h(n)\,q(n)} = \frac{1}{q(n)}$ $\forall n > N$

$\Rightarrow$ $negl_2(n)$ is also negligible