CS435 Quiz 1

Zhaoyi Zhang 9079627627

1.(a) $2^{-k\log(n)} = \frac{1}{2^{\log(n^k)}} = \frac{1}{n^k}$

Since k is a positive integer, $\frac{1}{n^k} > \frac{1}{n^{k+1}}$

Thus $2^{-k\log(n)}$ is not negligible

1.(b) $\frac{1}{n^{50}+n^3} > \frac{1}{n^{100}+n^{50}+n^3}$, so $\frac{1}{n^{50}+n^3}$ is not negligible

Even though $2^{-\sqrt{n}}$ is negligible, overall $\frac{1}{n^{50}+n^3} - 2^{-\sqrt{n}}$ is not negligible

1.(c) $\frac{1}{2^{\sqrt[3]{n}}(n^3+n^7)} < \frac{1}{2^{\sqrt[3]{n}}} < \frac{1}{2^{\sqrt{n}}}$

Since $\frac{1}{2^{\sqrt{n}}}$ is negligible, $\frac{1}{2^{\sqrt[3]{n}}(n^3+n^7)}$ is also negligible.

2 The expansion factor of F is $l(n) = 3n$. If s is a n-bit seed, the output of G is 2n-bits, so the output of F is 3n-bits.

$$D(w) = \begin{cases} 1 & \text{if } w \text{ has a form } s \cdot G(s) \\ 0 & \text{otherwise.} \end{cases}$$

world 0

$s \leftarrow \{0,1\}^n$

$r = F(s) = s \cdot G(s)$

$Pr[D(F(s))=1] = 1$

world 1

$r \leftarrow \{0,1\}^{3n}$

$Pr[D(r)=1] = \frac{1}{2^{3n}}$

$Pr[D(F(s))=1] - Pr[D(r)=1] = 1 - \frac{1}{2^{3n}} \neq$ negligible

Thus, F(s) is not a PRG

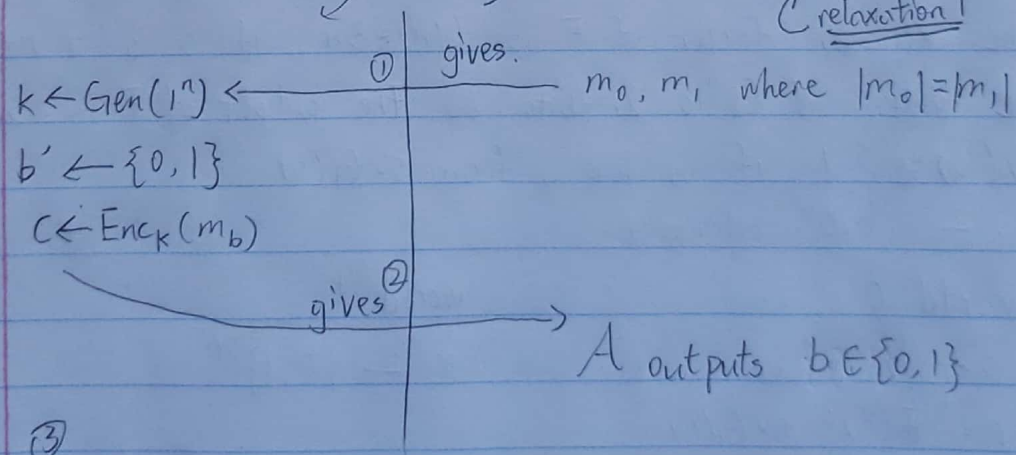
3. $P(E) = \frac{m}{2^n}$

Since we know $\frac{1}{2^n}$ is negligible, and for any positive polynomial p, negligible function negl, $p(n)\,negl$ is still negligible. m is independent of n, so $P(E) = \frac{m}{2^n}$ is still negligible.

$$P(E_1 \vee E_2 \vee \cdots \vee E_{p(n)}) \leq \sum_{i=1}^{p(n)} P(E_i) = p(n)\,P(E) = p(n)\frac{m}{2^n}$$

$p(n)$ is a positive polynomial, $m \cdot p(n)$ is still a positive polynomial. The upper bound of the probability that at least one of $p(n)$ trials the event happens is $p(n)\frac{m}{2^n}$. By the same argument used in the previous part of the answer, $p(n)\frac{m}{2^n}$ is still negligible.

4. $\Pi = (Gen, Enc, Dec)$, 1^n → A (can only run in PPT) ← relaxation 1



③

$$PrivK^{eav}_{A,\Pi}(n) = \begin{cases} 1 & \text{if } b = b' \text{ (A wins)} \\ 0 & \text{if } b \neq b' \text{ (A loses)} \end{cases}$$

$$Pr[PrivK^{eav}_{A,\Pi}(n) = 1] \leq \frac{1}{2} + negl(n)$$ relaxation 2