CS 171 HW2

Q1. a) $\exists N_f \in Z^+ \ \forall n > N_f \quad f(n) < \frac{1}{2P(n)}$
$\exists N_g \in Z^+ \ \forall n > N_g \quad g(n) < \frac{1}{2P(n)}$
$\rightarrow h(n) = f(n) + g(n) < \frac{1}{2P(n)} \quad \forall n > (\max(N_f, N_g))$

b) $\exists N_f \in Z^+ \ \forall n > N_f \quad f(n) < \frac{1}{n^c \, Poly(n)}$
$P(n) < n^c$
$\rightarrow h(n) = f(n) \cdot P(n) < \frac{1}{Poly(n)}$

c) Polynomial

$\because n^{-100}$ is Polynomial as $n^{-100} < \frac{1}{n^{101}}$ is impossible

d) Negligible

$\because$ For large enough n, $n^c < 1.01^n$, so $\frac{1}{1.01^n} < \frac{1}{P(n)}$

e) Polynomial

$\because 2^{-(\log_2 n)^2} = \frac{1}{n^2} > \frac{1}{n^3}$

f) Negligible

$\because$ Dominant term $e^{-\log n}$ is negligible since $n^c < e^{\log_2 n}$ for large enough n which means $\frac{1}{e^{\log_2 n}} < \frac{1}{n^c}$

Q2. a) When $a=0$, it is not invertible so Dec leads to error, losing the message.
$Pr[a=0] = \frac{1}{23}$.

b) $c_1 = a \cdot m_1 + b \mod 23$
$c_2 = a \cdot m_2 + b \mod 23$
$\rightarrow c_1 - c_2 = a \cdot \underbrace{(m_1 - m_2)}_{\text{non-zero}} \mod 23$

$\therefore (m_1 - m_2)$ has inverse mod 23

$\therefore$ Unique solution for a and thus b

The above is same for m_1', m_2'

$\therefore Pr[Enc(k, m_1) = c_1 \land Enc(k, m_2) = c_2] = Pr[Enc(k, m_1') = c_1 \land Enc(k, m_2') = c_2]$
$= \frac{1}{23} \times \frac{1}{22}$