1) $M = \{0, \dots, 4\}$

$K \leftarrow \{0, \dots, 5\}$

$Enc_k(m) = (k + m) \bmod 5$

$Dec_k(m) = (c - k) \bmod 5$

$$Pr(C = c \mid M = m) = Pr(Enc_k(m) = c)$$

$$= \sum_{k=0}^{5} Pr(Enc_k(m) = c \mid K = k)\, Pr(K = k)$$

$$= \frac{1}{6} \sum_{k=0}^{5} Pr(Enc_k(m) = c \mid K = k)$$

for perfect secracy

$$Pr(C = c \mid M = m_0) = Pr(C = c \mid M = m_1) \quad \forall c, m_0, m_1$$

consider the case when $c = 3$, $m_0 = 0$, $m_1 = 3$

$$\therefore Pr(C = 3 \mid M = m_0) = \frac{1}{6}(0 + 0 + 0 + 1 + 0 + 0)$$

$$= 1/6 \quad \text{--- ①}$$

$$Pr(C = c \mid M = m_1) = \frac{1}{6}(1 + 0 + 0 + 0 + 0 + 1)$$

$$= 1/3 \quad \text{--- ②}$$

as ① $\neq$ ② $\Rightarrow$ encryption scheme is not perfectly secure.

2) No, this is not a perfectly secret encryption scheme as here $|K| < |M|$.

Proof: Let $M(c) = \{ m : Dec_k(c) = m \mid k \in K \}$
now as $|K| < |M|$ $\exists$ $m'$ s.t
$Dec_k(c) \neq m'$ for particular c & $\forall$ k

$$\therefore \Pr[M = m' \mid C = c] = 0 \neq \Pr[M = m']$$

(Assuming uniform distribution over $M$)

Counter example: $M = \{0,1\}^l$ (Assume uniform dist over it)
$m \leftarrow M$
let m be any $l$ bit string with even number of one's & c be a $l$ bit cipher string with odd number of ones. (assuming $m \neq c$)

$$\therefore \Pr[M = m \mid C = c] = 0 \neq P[M = m] = 1/2^l$$

same is the case when m has odd number of 1's & c has even.
$\Rightarrow$ encryption scheme not perfectly secure.

5) given any positive polynomial $q(n)$ $\exists N_1$ s.t.

$$negl_1(n) < \frac{1}{q(n)} \quad \forall n > N_1$$

as $p(n)$ is positive polynomial $\Rightarrow$ multiplying the inequality on both sides by $p(n)$

$$p(n) \cdot negl_1(n) < \frac{P(n)}{q(n)} \quad \forall n > N_2$$

$$\Rightarrow negl_2(n) < \frac{1}{r(n)} \quad \forall n > N_2$$

$r(n) = \frac{q(n)}{p(n)}$, which is a positive polynomial as $q, p$ are positive poly.

$\therefore negl_2(n)$ is negligible function

4) Assume $G_1$ is not PRG $\Rightarrow \exists$ $D_1$ distinguisher which ~~outwins~~ with non negligible probability.
constructing D for G using $D_1$ as subroutine -
for input ~~st~~ D will output similar to $D_1$ with input $t||b$ where $b \leftarrow \{0,1\}$. $\therefore$ we have $t||b = G(s)||b$ $= G_1(s||b)$ if $t = G(s)$ & t is random string

$$\Rightarrow \left| Pr[D(G(s)) = 1] - Pr[D(r) = 1] \right|$$

$$= \left| Pr[D_1(G(s)||b) = 1] - Pr[D_1(r||b) = 1] \right|$$

$$\cancel{= \left| Pr[D_1[G_1(s||b) = 1] - Pr[D_1(r||b) = 1] \right|}$$

$$= \left| Pr[D_1(G_1(s) = 1)] - Pr[D_1(r) = 1] \right|$$

$$\gg negl(n+1)$$

which is a contradiction as G is a PRG
$\Rightarrow G_1$ is also a PRG